Internal Pentest

Fix Actions

Sample Internal Pentest
H3 Sample Account
May 24, 2024

HORIZON3.ai
~~TRUST BUT~~ VERIFY

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

Note: This document may contain information that is potentially sensitive in nature, including personally identifiable information. Use discretion when sharing this document with any other parties. The information contained herein is protected and is considered proprietary information for the exclusive use of **Horizon 3 AI** and **H3 Sample Account** for this report.

Table of Contents

CRITICAL Severity

Windows SMB Remote Code Execution Vulnerability 1

Windows Print Spooler Remote Code Execution Vulnerability 6

Active Directory Domain Services Elevation of Privilege Vulnerability 7

Microsoft Windows Active Directory Certificate Services (ADCS) Privilege Escalation via User Specified Machine Account DNSHostName 8

Unauthenticated Access to the Jenkins Script Console 9

Insecure Java JMX Configuration 10

Weak or Default Credentials - Cracked Credentials 12

SMB Signing Not Required 14

LLMNR Poisoning Possible 15

NBT-NS Poisoning Possible 18

Kerberoasting 23

Credential Dumping - Security Account Manager (SAM) Database 24

Credential Dumping - Local Security Authority Subsystem Service (LSASS) Memory 25

Active Directory Certificate Services Misconfiguration Privilege Escalation - Subject Alternative Name 26

Active Directory Certificate Services Misconfigured Enrollment Agent Template 27

Active Directory Certificate Services Misconfigured Template Access Controls 28

Credential Reuse - Shared Windows Local User and Domain User Accounts 29

Credential Dumping - Data Protection API (DPAPI) Secrets 30

Password in Active Directory User Attribute 31

Netlogon Elevation of Privilege Vulnerability 32

GitLab ExifTool Remote Code Execution Vulnerability 33

Credential Dumping - Local Security Authority (LSA) Secrets 34

Microsoft Entra (AzureAD) Connect Credential Dumping 35

Microsoft Entra (AzureAD) - Over-Privileged Service Principal 36

Microsoft Entra (AzureAD) - Service Principal Takeover 37

Credential Reuse - Windows Local Administrator Accounts 38

UnrealIRCd Remote Code Execution Vulnerability 39

Apache Struts 2 Prefixed Parameters OGNL Remote Code Execution Vulnerability 40

Apache ActiveMQ Remote Code Execution Vulnerability 41

Apache Shiro RememberME Cookie Deserialization Remote Code Execution Vulnerability 42

Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability Bypass 43

Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability 44

Apache Struts2 Content Header Remote Code Execution Vulnerability 45
Apache Struts2 S2-048 Remote Code Execution Vulnerability 46
Vulnerable Cisco Smart Install 47
Apache Solr Velocity Remote Code Execution Vulnerability 48
SaltStack Salt Remote Code Execution Vulnerability 49
Apache Airflow Experimental API Authentication Bypass Vulnerability 50
Oracle WebLogic Java Deserialization Vulnerability - Console Component 51
Apache Airflow Authorization Bypass Vulnerability 52
VMware vCenter Server Access Control Vulnerability 53
VMware vCenter vROPS Plugin Remote Code Execution Vulnerability 54
VMware vRealize Operations Manager Server-Side Request Forgery Vulnerability 58
VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability 59
Apache mod_proxy Server-Side Request Forgery Vulnerability 63
Apache Log4j2 Remote Code Execution Vulnerability 64
Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability 65
Redis Lua Sandbox Escape 66
F5 BIG-IP iControl REST Remote Command Execution Vulnerability 67
Apache CouchDB Unauthenticated Remote Code Execution Vulnerability 68
Atlassian Confluence Namespace OGNL Injection Vulnerability 69
Zoho ManageEngine ADAudit Plus Remote Code Execution Vulnerability 70
Fortinet FortiOS / FortiProxy / FortiSwitchManager Authentication Bypass Vulnerability 71
VMware vRealize Network Insight Remote Code Execution Vulnerability 72
Atlassian Confluence Server - Improper Authorization 73
Adobe ColdFusion Unauthenticated File Read Vulnerability 74
Adobe ColdFusion Remote Code Execution Vulnerability 75
Adobe ColdFusion Deserialization of Untrusted Data Remote Code Execution Vulnerability 76
Citrix Gateway Unauthenticated Remote Code Execution 77
Adobe ColdFusion JNDI Remote Code Execution Vulnerability 78
Apache ActiveMQ OpenWire Transport Remote Code Execution Vulnerability 79
F5 BIG-IP Unauthenticated Remote Code Execution via AJP Smuggling 80
Fortinet FortiClient EMS SQL Injection Vulnerability 81
Unauthenticated Kubelet API Remote Code Execution Vulnerability 82
Weak or Default Credentials - Web Applications 83
AWS Instance Metadata Service v1 Exposed 84
JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability 85

Azure Multi-Factor Authentication Disabled 86
AWS Assume Role Access 87
PaperCut File Upload Remote Code Execution Vulnerability 88
Weak NFS Export Permissions 89
VMware vCenter Server-Side Request Forgery Vulnerability 91
Microsoft Exchange Remote Code Execution Vulnerability 92
Citrix Bleed - Leaking Session Tokens 93
Jenkins Arbitrary File Leak Vulnerability 94
Unauthenticated Access to Sensitive Kubelet API Endpoints 95
Unauthenticated Kubernetes API Server Access 96
Weak or Default Credentials - SSH 97
Apache Solr Arbitrary File Read Vulnerability 99
Weak or Default Credentials - Microsoft SQL Server 100
Apache Solr DataImportHandler Remote Code Execution Vulnerability 101
Drupal Core Remote Code Execution Vulnerability 102
Microsoft Windows Machine Account NTLM Coercion via LSARPC Spoofing Vulnerability 103
PolKit PkExec Local Privilege Escalation Vulnerability 104
Anonymous FTP Enabled 105
IPMI Cipher Zero Vulnerability 106
FTP Directory Traversal Vulnerability 107
Weak or Default Credentials - FTP 108
Weak or Default Credentials - Telnet 109
Unrestricted Sudo Privileges 110
Credential Dumping - /etc/shadow File 111
Active Directory Certificate Services Misconfiguration: NTLM Relay to AD CS HTTP Endpoint 112
Microsoft Windows Machine Account NTLM Coercion via Authenticated LSARPC Spoofing 113
Authenticated Microsoft Windows Machine Account NTLM Coercion via Distributed File System Namespace Management Protocol Manipulation 114
NFS UID/GID Manipulation Possible 115
Zoho ManageEngine ServiceDesk Plus Unauthenticated Remote Code Execution Vulnerability 116

HIGH Severity

Group Policy Preferences Password Elevation of Privilege Vulnerability 117
Weak or Default Credentials - MySQL 120
Weak or Default Credentials - Postgres 121
Weak or Default Credentials - MongoDB 122

Anonymous MongoDB Access 123
HTTP.sys Denial of Service and Remote Code Execution Vulnerability 124
Weak or Default Credentials - Cracked Credentials from Active Directory Services Database (NTDS) 125
Password Reuse Found in Active Directory Services Database (NTDS) 126
Active Directory User has Entra Administrator Role 127
Remote Desktop Services Remote Code Execution Vulnerability 128
SaltStack Authorization Bypass Vulnerability 129
Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability 130
OpenSSL Heartbleed Vulnerability 131
Apache JServ Protocol (AJP) Vulnerability 132
Grafana Directory Traversal Vulnerability 133
Adobe ColdFusion Improper Access Control Vulnerability 134
Adobe ColdFusion Improper Access Control Vulnerability - Patch Bypass 135
Gradio Windows Credentials Leak Vulnerability 136
Insecure IPMI Implementation 137
Kerberos Pre-Authentication Disabled 140
Public Access to Git Repository 141
Credential Reuse 142
Active Directory Certificate Services Misconfigured Template Requires Enrollment Agent Signature 143
Shell History File Exposure 144
Domain User with Local Administrator Privileges 145
Gradio Arbitrary File Read Vulnerability 146
Credential Dumping - Active Directory Services Database (NTDS) 147
Kerberos Unconstrained Delegation 148
Apache Druid Server-Side Request Forgery Vulnerability 149

MEDIUM Severity

Redis Unauthenticated Access Vulnerability 150
Unauthenticated Access to Elasticsearch 151
Active Directory Certificate Services Misconfiguration Privilege Escalation - Any Purpose or No (aka SubCA) EKU Misconfiguration 152
Unauthenticated Docker Registry API Access 153
Keycloak 12.0.1 - request_uri Blind Server-Side Request Forgery (SSRF) 154
Jetty Limited Path Traversal Vulnerability - Second Variation 155
Adobe ColdFusion WDDX Deserialization Info Leak Vulnerability 156
Authenticated Microsoft Windows Machine Account NTLM Coercion via Print Spooler Protocol Manipulation 157

Anonymous Access to ZooKeeper API 158
Anonymous Access to Printer using PJL or PS 159
Kubernetes Service Account Token Exposure 160
Unauthenticated Access to Apache Solr 161
Unauthenticated Access to Jenkins People Directory 162
Jenkins Self-Signup Enabled 163
Unauthenticated Gitlab User Enumeration 164
Unauthenticated Jenkins Dashboard Exposure 165
Zone Transfer Allowed to Any Server 166
Ruby on Rails Debug Mode Enabled 167
Golang pprof Debugging Endpoint Enabled 168
Public Access to Amazon EC2 AMI 169
Public Access to Amazon EBS Snapshot 170
Public Access to Amazon RDS Snapshot 171
Active Directory - User Password Not Required 172

LOW Severity

Public Access to Amazon S3 Bucket 173
Guest Account Enabled 174
Weak or Default Credentials - SNMP 176
Web Directory Listing 177
Exposed Kubernetes Version 178
Weak Password Strength Requirements 179
SMB Null Session Allowed 180
Expired SSL/TLS Certificate 181

Windows SMB Remote Code Execution Vulnerability

CRITICAL 10

CVE-2017-0144

Affected Hosts

- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- 10.0.229.11 (fs.smoke.net)
- 10.0.4.135 (win8)
- 10.0.220.54 (winxp.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.0.229.6 (app4.smoke.net)
- 10.0.220.6 (app2.smoke.net)
- Domain Controller 10.0.229.2 (dc2.smoke.net)

Table of Contents

- **Option 1: Apply Patch to Host**
- **Option 2: Disable SMBv1 via Group Policy**
- **Option 3: Disable SMBv1 Server via Group Policy**
- **Option 4: Block Access to SMB from Untrusted Hosts**

Option 1: Apply Patch to Host

Microsoft released a patch, KB4012598, addressing this group of vulnerabilities. To install it, download the patch from the Microsoft Update Catalog for the corresponding host operating system.

NOTE: See **here** for more details.

Option 2: Disable SMBv1 via Group Policy

To disable the SMBv1 client, the services registry key needs to be updated to disable the start of **MRxSMB10** and then the dependency on **MRxSMB10** needs to be removed from the entry for **LanmanWorkstation** so that it can start normally without requiring **MRxSMB10** to first start.

This guidance updates and replaces the default values in the following two items in the registry:

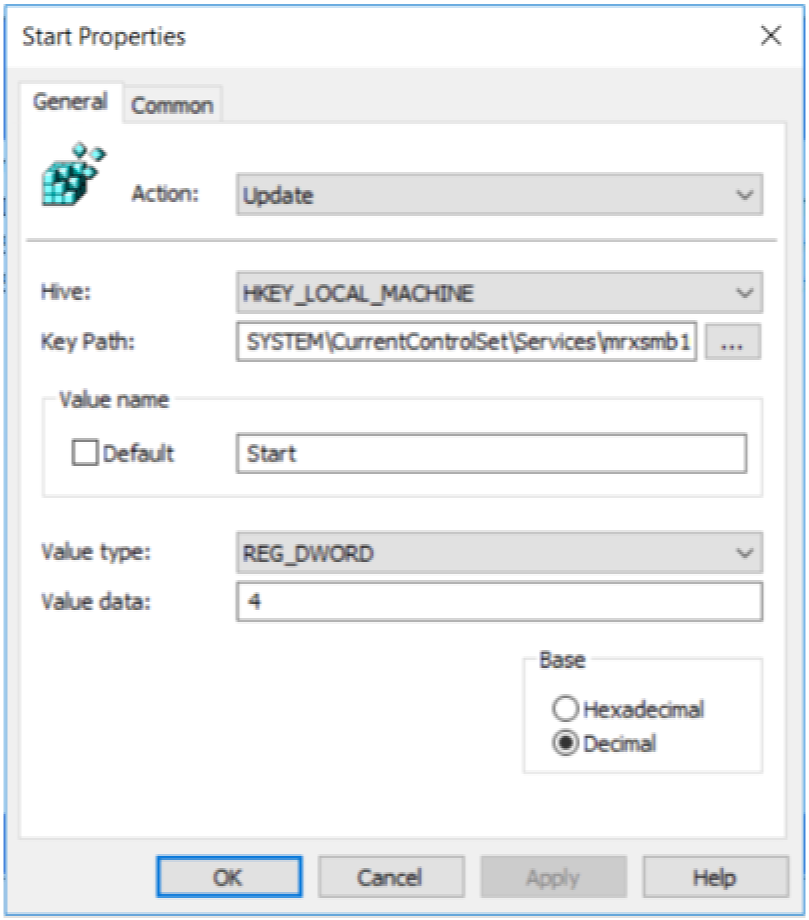
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mrxsmb10`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation`

To configure this by using Group Policy, follow these steps:

1. Open the **Group Policy Management Console**. Right-click the GPO that should contain the new preference item, and then click **Edit**.
2. In the console tree under **Computer Configuration**, expand the **Preferences** folder, and then expand the **Windows Settings** folder.
3. Right-click the **Registry** node, point to **New**, and select **Registry Item**.
4. In the **New Registry Properties** dialog box, select the following:
   - **Action**: Update
   - **Hive**: HKEY_LOCAL_MACHINE
   - **Key Path**: SYSTEM\CurrentControlSet\services\mrxsmb10
   - **Value name**: Start
   - **Value type**: REG_DWORD

- **Value data**: 4

NOTE: The default value includes **MRxSMB10** in many versions of Windows, so by replacing them with this multi-value string, it is in effect removing **MRxSMB10** as a dependency for **LanmanServer** and going from four default values down to just these three values above.



Start Properties

Action: Update

Hive: HKEY_LOCAL_MACHINE

Key Path: SYSTEM\CurrentControlSet\Services\mrxsmb1

Value name

□ Default Start

Value type: REG_DWORD

Value data: 4

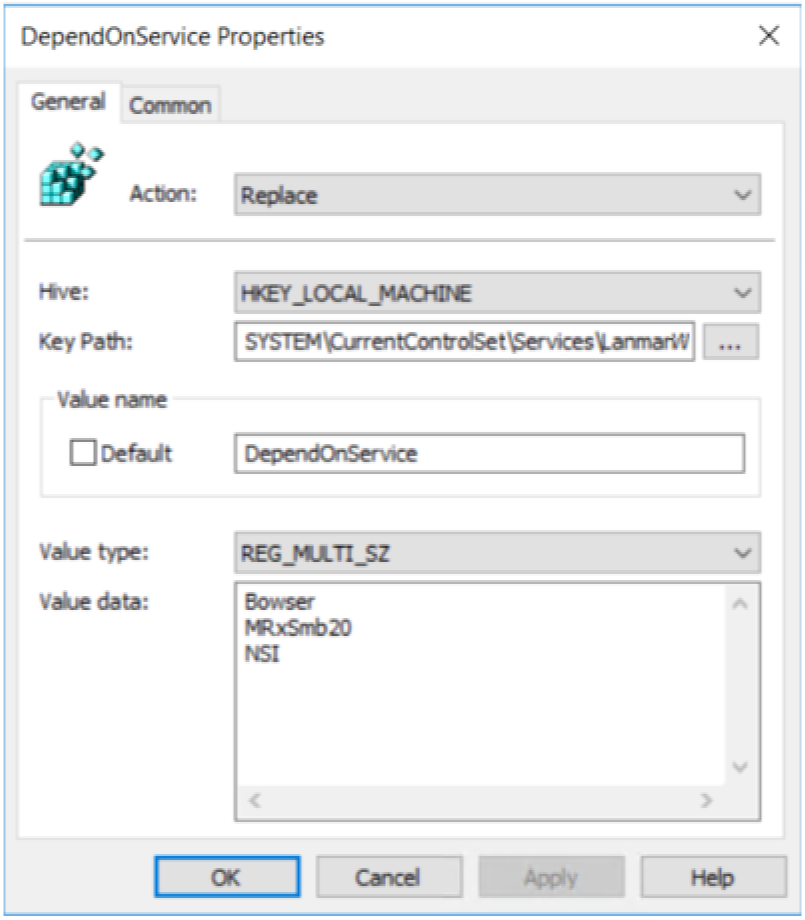
Base

○ Hexadecimal

● Decimal

5. Then remove the dependency on the **MRxSMB10** that was disabled. In the **New Registry Properties** dialog box, select the following:
   - **Action**: Replace
   - **Hive**: HKEY_LOCAL_MACHINE
   - **Key Path**: SYSTEM\CurrentControlSet\Services\LanmanWorkstation
   - **Value name**: DependOnService
   - **Value type**: REG_MULTI_SZ
   - **Value data**:
     - Bowser
     - MRxSmb20
     - NSI

   NOTE: These three strings will not have bullets (see the following screenshot).



Action: Replace

Hive: HKEY_LOCAL_MACHINE

Key Path: SYSTEM\CurrentControlSet\Services\LanmanW

Value name

□ Default DependOnService

Value type: REG_MULTI_SZ

Value data:

```
Bowser
MRxSmb20
NSI
```

NOTE: When you use Group Policy Management Console, you don't have to use quotation marks or commas. Just type each entry on individual lines.

6. Restart the targeted systems to finish disabling SMB v1.

Option 3: Disable SMBv1 Server via Group Policy

This procedure configures the following new item in the registry:

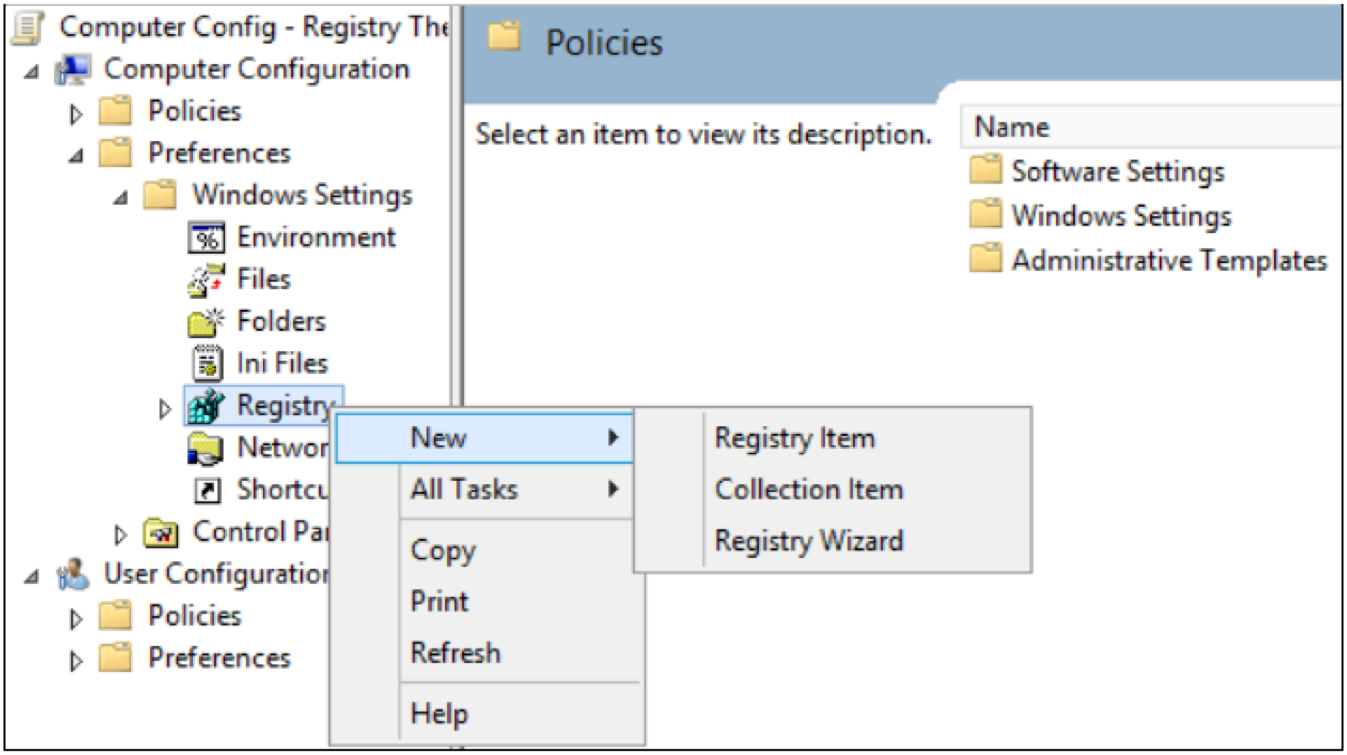
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters`

Configured with:

- Registry entry: **SMB1**
- REG_DWORD: **0** = Disabled

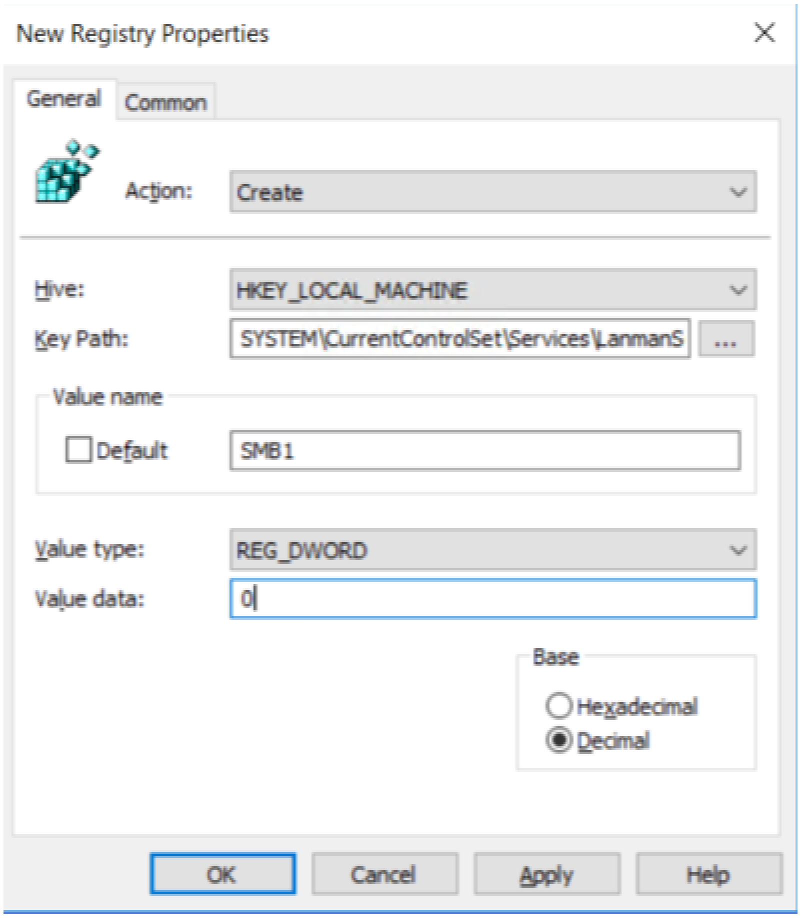
To use Group Policy to configure this, follow these steps:

1. Open the **Group Policy Management Console**. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click **Edit**.
2. In the console tree under **Computer Configuration**, expand the **Preferences** folder, and then expand the **Windows Settings** folder.
3. Right-click the **Registry** node, point to **New**, and select **Registry Item**



4. In the **New Registry Properties** dialog box, select the following:

- **Action**: Create
- **Hive**: HKEY_LOCAL_MACHINE
- **Key Path**: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
- **Value name**: SMB1
- **Value type**: REG_DWORD
- **Value data**: 0



Action: Create

Hive: HKEY_LOCAL_MACHINE

Key Path: SYSTEM\CurrentControlSet\Services\LanmanS

Value name

□ Default SMB1

Value type: REG_DWORD

Value data: 0

Base

○ Hexadecimal

● Decimal

This procedure disables the SMBv1 Server components. This Group Policy must be applied to all necessary workstations, servers, and domain controllers in the domain.

Option 4: Block Access to SMB from Untrusted Hosts

Microsoft recommends restricting the use of SMB in general to hosts that do not host SMB shares. To restrict the use of SMB, follow the official Microsoft guide for disabling “Inbound connections to a computer”. See **Prevent SMB Traffic from Lateral Connections** for more details.

Mitigations

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

References

- **MS17-010**
- **CVE-2017-0144**

Windows Print Spooler Remote Code Execution Vulnerability

CRITICAL 10

CVE-2021-34527

Affected Hosts

- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- 10.0.220.6 (app2.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.0.229.11 (fs.smoke.net)
- 10.0.229.6 (app4.smoke.net)
- 10.0.4.3 (ex01.pod04.example.internal)

Mitigations

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

References

- **Microsoft Security Advisory for CVE-2021-34527**
- **CVE-2021-34527**

Active Directory Domain Services Elevation of Privilege Vulnerability

CRITICAL 10

CVE-2021-42278

Affected Hosts

- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.229.1 (dc.smoke.net)

Mitigations

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

References

- **Microsoft Security Advisory for CVE-2021-42287**
- **Microsoft Security Advisory for CVE-2021-42278**
- **How to Exploit noPAC**
- **CVE-2021-42287**
- **CVE-2021-42278**

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

CRITICAL 10

CVE-2022-26923

Affected Hosts

- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)

Mitigations

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

References

- **Active Directory Domain Services Elevation of Privilege Vulnerability**
- **Certifried: Active Directory Domain Privilege Escalation (CVE-2022-26923)**
- **CVE-2022-26923**

Unauthenticated Access to the Jenkins Script Console

CRITICAL 10

H3-2020-0021

Affected Hosts

- 10.0.40.102 (airflow-target.smoke.net)
- 10.0.229.4 (ex2.smoke.net)
- 10.2.51.103

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**
- **Jenkins - Script-Console Java Execution (Metasploit)**

Insecure Java JMX Configuration

CRITICAL 10

H3-2020-0022

Affected Hosts

- 10.0.4.129 (win7.pod04.example.internal)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- 10.0.40.89
- 10.0.4.134
- 10.0.4.16
- 10.0.229.11 (fs.smoke.net)
- 10.0.4.15
- 10.0.229.4 (ex2.smoke.net)
- 10.0.4.8
- 10.0.4.4 (svr01.pod04.example.internal)
- 10.0.40.84
- 10.0.4.9
- 10.0.4.133

Table of Contents

- **Option 1: Disable JMX**
- **Option 2: Configure a Whitelist Firewall**
- **Option 3: Configure User Authentication on the JMX Server**

Option 1: Disable JMX

JMX is only required if you need remote management and monitoring of a Java-based application or the Java Virtual Machine (JVM) running the application. If this isn't required, disable it in your start-up options of the JVM or in the configuration of the application exposing the JMX port.

Option 2: Configure a Whitelist Firewall

Look for an option similar to `-Dcom.sun.management.jmxremote.port=9999` in your application configuration or JVM command line arguments.

In this instance, port 9999 is the port JMX is utilizing. Restrict access to your local machine on port 9999 to hosts you trust and need access to the JMX port for remote management and monitoring.

Option 3: Configure User Authentication on the JMX Server

This will help prevent unauthorized users from accessing the JMX port and installing their own exploit payloads.

1. Create a password file jmxremote.password which should look similar to the following:NOTE: File name can be anything you want, but must match the argument provided in step 2 and 3). Use strong passwords.

```
##Defining two "roles", each with its own password
monitorRole  YourStrongPassword1
controlRole  YourStrongPassword2
```

1. The security of the password file relies on your file system's access control mechanisms. The file must be readable by the user running the Java application exposing JMX. To do this on Windows, use a command like the following:

   `cacls jmxremote.password /P username:R`

2. When starting up your JVM, ensure the option below is added to the startup command:
   ```
   -Dcom.sun.management.jmxremote.password.file=jmxremote.password
   ```

Configure SSL on the JMX server. This will help prevent possible leakage of usernames and passwords in clear text over your network.

- Add the following to configure SSL for your JMX instance. Ensure your keystore password used when you created your certificate matches the appropriate options below.

```
-Dcom.sun.management.jmxremote.ssl=true
-Djavax.net.ssl.keyStore=/home/user/.keystore
-Djavax.net.ssl.keyStorePassword=myKeyStorePassword
-Dcom.sun.management.jmxremote.ssl.need.client.auth=true
-Djavax.net.ssl.trustStore=/home/user/.truststore
-Djavax.net.ssl.trustStorePassword=myTrustStorePassword
-Dcom.sun.management.jmxremote.registry.ssl=true
```

Mitigations

- Configure user authentication and SSL on the JMX endpoint.

References

- **Attacking RMI based JMX Services**
- **Java JMX Server Insecure Configuration Java Code Execution (Metasploit)**

Weak or Default Credentials - Cracked Credentials

CRITICAL 10

H3-2021-0020

Affected Assets

- Cleartext Password for a-jsmith
- Cleartext Password for it_support
- Cleartext Password for svc_sync
- Cleartext Password for boba_fett
- Cleartext Password for user
- Cleartext Password for a-jsmith
- Cleartext Password for user
- Cleartext Password for root
- Cleartext Password for xadmin
- Cleartext Password for vagrant
- Cleartext Password for xadmin
- Cleartext Password for postgres
- Cleartext Password for xadmin
- Cleartext Password for it_support
- Cleartext Password for xadmin
- Cleartext Password for a-jsmith
- Cleartext Password for user
- Cleartext Password for a-jsmith
- Cleartext Password for a-jsmith
- Cleartext Password for admin

Table of Contents

- **Option 1: Implement a Strong Password Policy**
- **Option 2: Implement a Configuration Management Process**

Option 1: Implement a Strong Password Policy

Change the credential’s password and ensure a strong password policy is in place and users are properly trained on best practices. The National Institute of Standards and Technology (NIST) commonly releases guidance on password best practices which include:

- A minimum length of 8 characters
- Blacklisting passwords that contain dictionary words, repetitive or sequential characters, and the company name
- Implement Multi-Factor Authentication when available

NOTE: See full NIST publication here **NIST 800-63-3**

Option 2: Implement a Configuration Management Process

Often, systems and applications will be installed without the default credentials being changed. Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.

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**
- **T1110: Brute Force**

SMB Signing Not Required

CRITICAL 10

H3-2021-0030

Affected Hosts

- 10.0.229.6 (app4.smoke.net)
- 10.0.229.11 (fs.smoke.net)
- 10.0.220.6 (app2.smoke.net)
- 10.0.220.52 (win7.smoke.net)
- 10.0.4.130 (win10.pod04.example.internal)
- 10.0.4.129 (win7.pod04.example.internal)
- 10.0.220.54 (winxp.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.0.4.24 (irc.testirc.net)
- 10.0.4.136 (win7-32)
- 10.0.40.53 (sambacry)
- 10.0.4.14 (win2008)
- 10.0.40.95
- 10.0.4.31 (openmediavault.pod04.example.internal)
- 10.0.4.23 (obwa.pod04.example.internal)
- 10.0.4.4 (svr01.pod04.example.internal)
- 10.0.40.72
- 10.0.4.8
- 10.0.4.22 (zoho.pod04.example.internal)
- 10.0.40.76

Mitigations

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

References

- **Microsoft network server: Digitally sign communications (always)**
- **Microsoft network client: Digitally sign communications (always)**
- **Overview of Server Message Block Signing**
- **Samba Configuration**
- **The Basics of SMB Signing (Covering Both SMB1 and SMB2)**

LLMNR Poisoning Possible

CRITICAL 10

H3-2021-0034

Affected Host

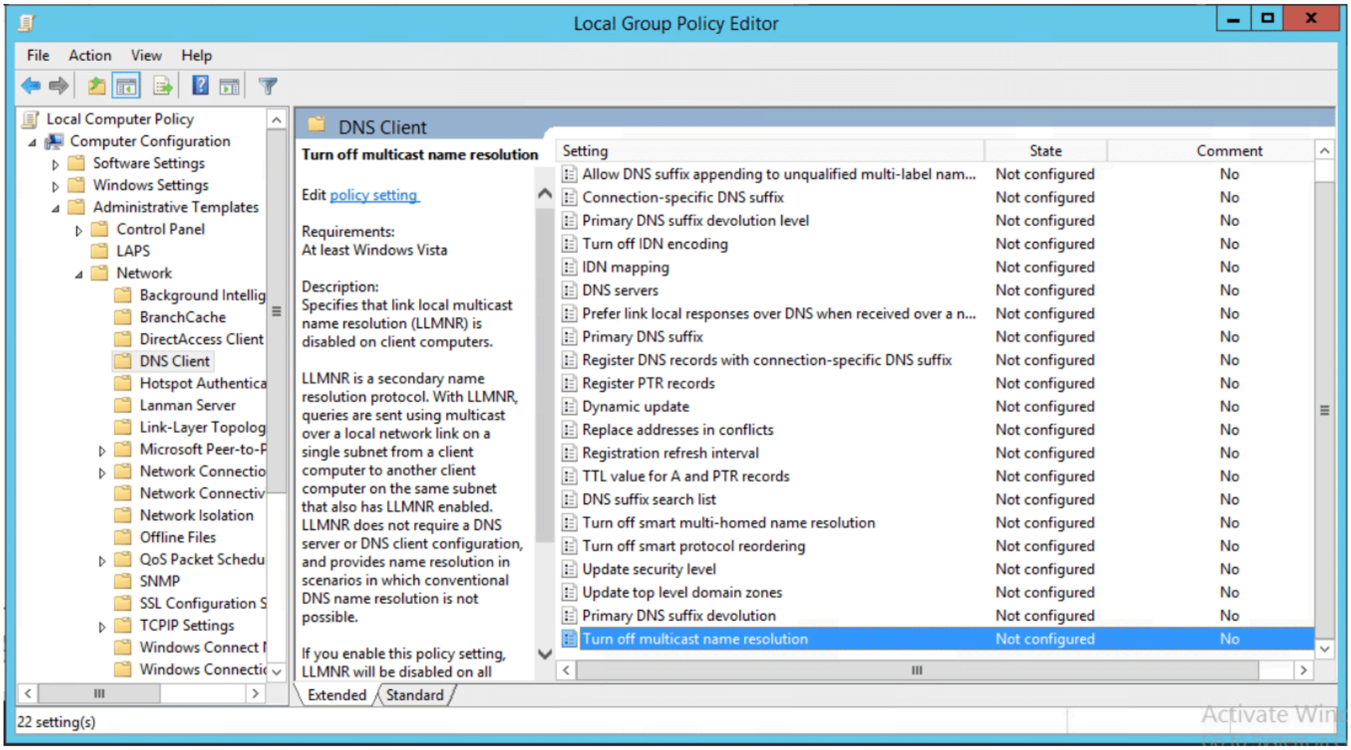
- 10.0.227.51

Table of Contents

- **Option 1: Disable via Group Policy**
- **Option 2: Disable on Selected Hosts**

Option 1: Disable via Group Policy.

1. Open the “Local Group Policy Editor” on the Domain Controller.
2. Navigate to Computer Configuration > Administrative Templates > Network > DNS Client and then selecting “Turn Off Multicast Name Resolution”



Turn off multicast name resolution

Edit policy setting

Requirements:
At least Windows Vista

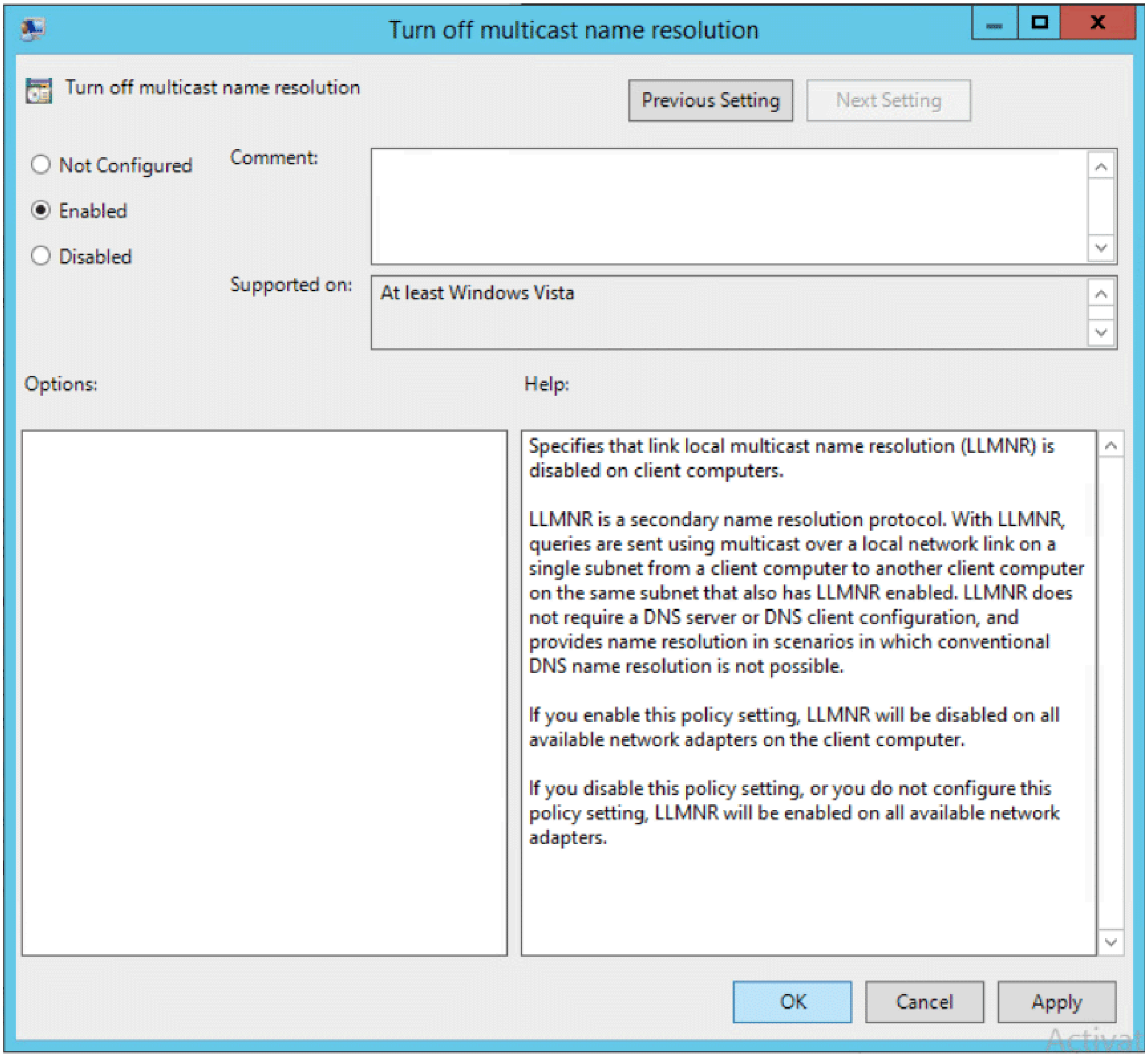
Description:
Specifies that link local multicast name resolution (LLMNR) is disabled on client computers.

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

If you enable this policy setting, LLMNR will be disabled on all

Setting	State	Comment
Allow DNS suffix appending to unqualified multi-label nam...	Not configured	No
Connection-specific DNS suffix	Not configured	No
Primary DNS suffix devolution level	Not configured	No
Turn off IDN encoding	Not configured	No
IDN mapping	Not configured	No
DNS servers	Not configured	No
Prefer link local responses over DNS when received over a n...	Not configured	No
Primary DNS suffix	Not configured	No
Register DNS records with connection-specific DNS suffix	Not configured	No
Register PTR records	Not configured	No
Dynamic update	Not configured	No
Replace addresses in conflicts	Not configured	No
Registration refresh interval	Not configured	No
TTL value for A and PTR records	Not configured	No
DNS suffix search list	Not configured	No
Turn off smart multi-homed name resolution	Not configured	No
Turn off smart protocol reordering	Not configured	No
Update security level	Not configured	No
Update top level domain zones	Not configured	No
Primary DNS suffix devolution	Not configured	No
Turn off multicast name resolution	Not configured	No

3. Click “Enabled” and select “Ok”



Turn off multicast name resolution

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Help:

Specifies that link local multicast name resolution (LLMNR) is disabled on client computers.

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

If you enable this policy setting, LLMNR will be disabled on all available network adapters on the client computer.

If you disable this policy setting, or you do not configure this policy setting, LLMNR will be enabled on all available network adapters.

Option 2: Disable on Selected Hosts

1. Log onto the host and open an Administrative Command Prompt
2. Disable LLMNR by disabling the “EnableMulticast” registry key with the following commands:

```
REG ADD "HKLM\Software\policies\Microsoft\Windows NT\DNSClient"
REG ADD "HKLM\Software\policies\Microsoft\Windows NT\DNSClient" /v " EnableMulticast" /t
REG_DWORD /d "0" /f
```

Mitigations

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

References

- **T1171 - LLMNR/NBT-NS Poisoning and Relay**
- **Local Network Vulnerabilities - LLMNR and NTB-NS Poisoning**
- **How to Disable LLMNR and Why You Want To**

NBT-NS Poisoning Possible

CRITICAL 10

H3-2021-0035

Affected Host

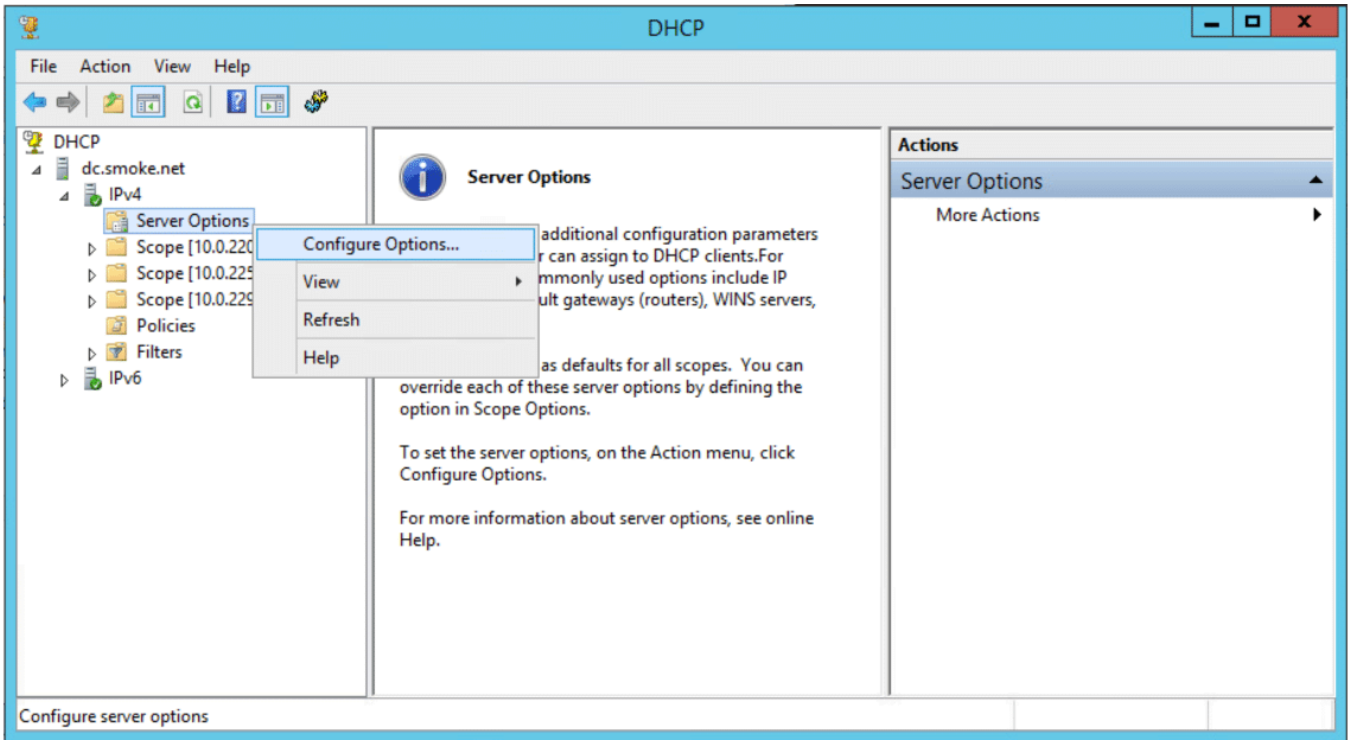
- 10.0.227.51

Table of Contents

- Option 1: Disable via DHCP
- Option 2: Disable via Specific Host

Option 1: Disable via DHCP

1. Log on to the server providing DHCP to the environment and open the DHCP Management interface by running “dhcpmgmt.msc”
2. Navigate to the “Server Options” within your domain and right click and select “Configure Options...”



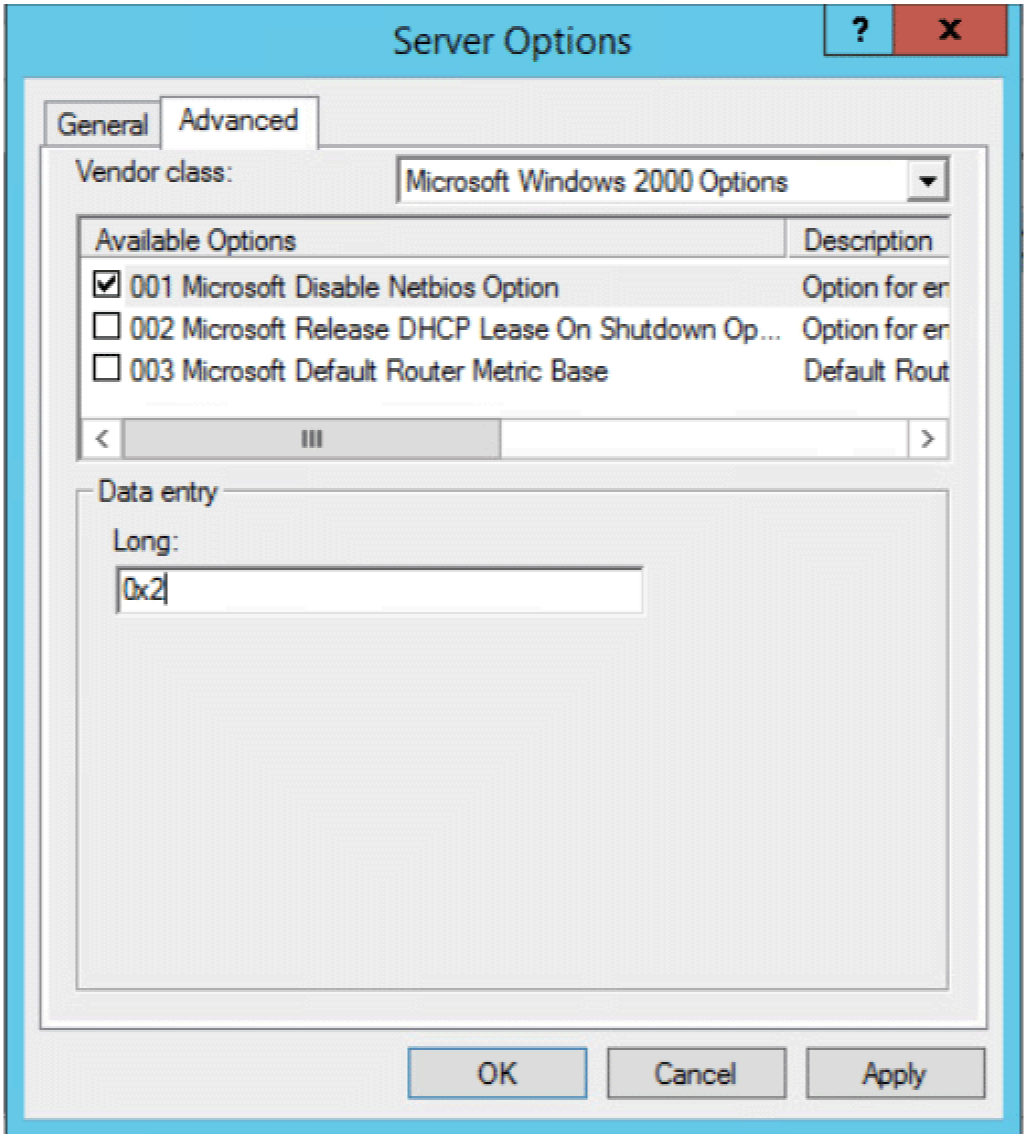
additional configuration parameters
r can assign to DHCP clients.For
mmonly used options include IP
ult gateways (routers), WINS servers,

as defaults for all scopes. You can override each of these server options by defining the option in Scope Options.

To set the server options, on the Action menu, click Configure Options.

For more information about server options, see online Help.

3. Select the “Advanced” tab, select the “Microsoft Windows 2000 Options”, select “001 Microsoft Disable Netbios Option”, change the value to “0x2”, and select “Ok”.



Vendor class: Microsoft Windows 2000 Options

Available Options	Description
☑ 001 Microsoft Disable Netbios Option	Option for en
□ 002 Microsoft Release DHCP Lease On Shutdown Op...	Option for en
□ 003 Microsoft Default Router Metric Base	Default Rout

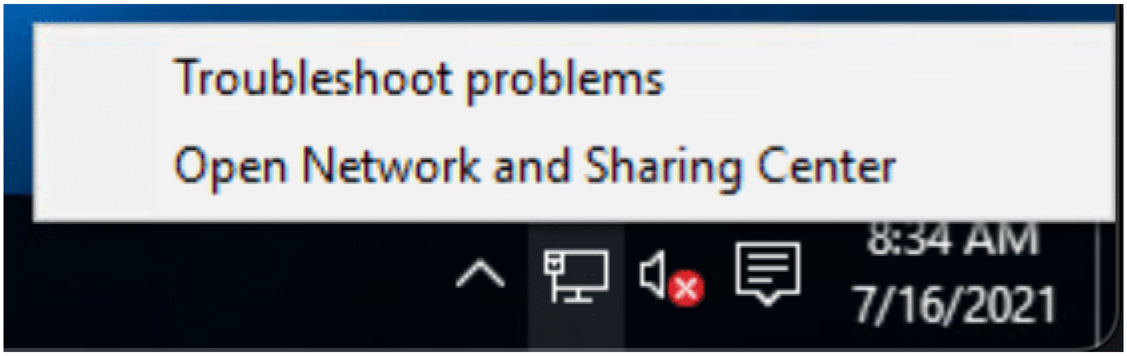
Data entry

Long:

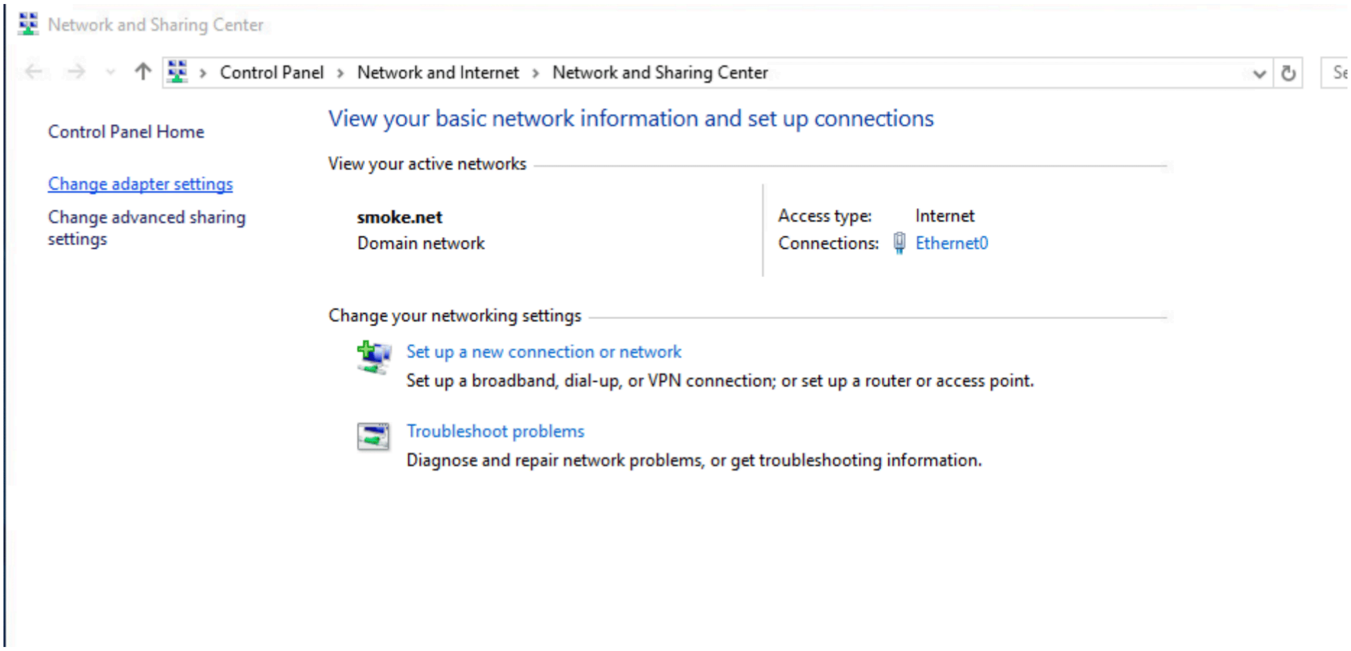
0x2

Option 2: Disable on Specific Host

1. Log on to the host and open the “Network and Sharing Center” by searching or right clicking the Network icon in the bottom right and selecting “Open Network and Sharing Center”.



2. Click “Change adapter settings”.


Network and Sharing Center
Control Panel › Network and Internet › Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
Set up a new connection or network
Troubleshoot problems

View your basic network information and set up connections

View your active networks

smoke.net
Domain network

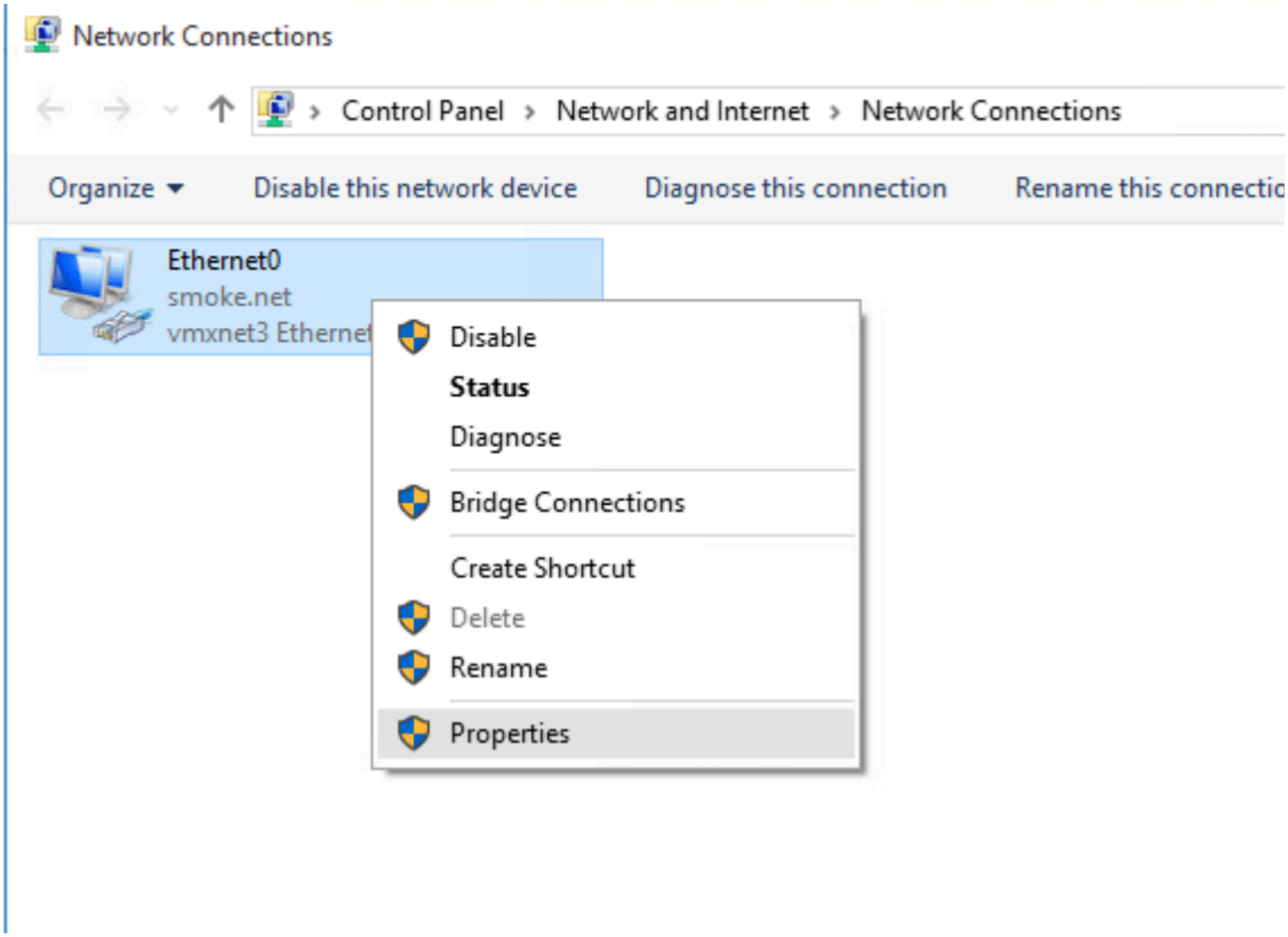
Access type: Internet
Connections: Ethernet0

Change your networking settings

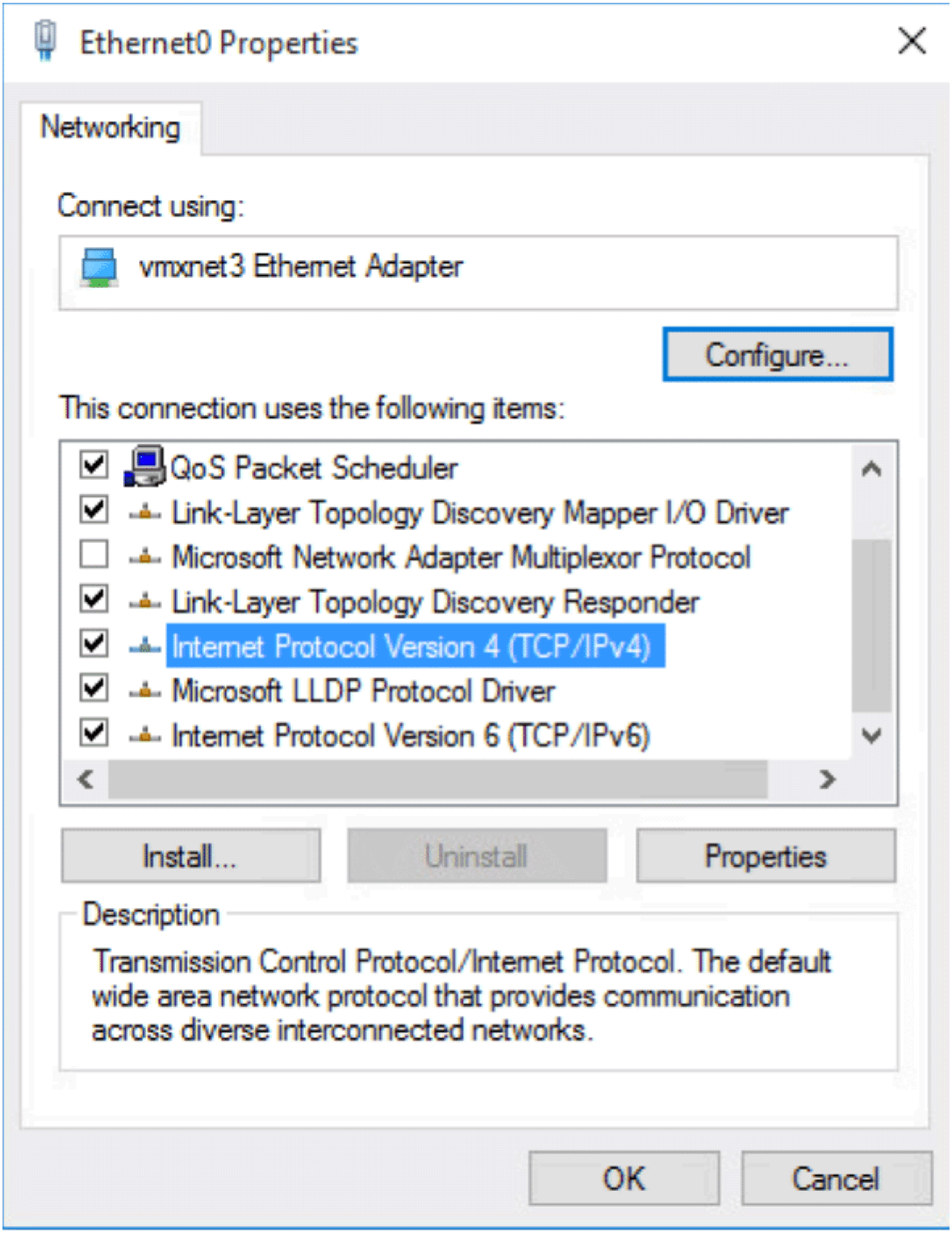
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

3. Right click on the interface and select “Properties”.



4. Select “Internet Protocol Version 4 (TCP/IPv4)” and click on “Properties”.



Ethernet0 Properties

Networking

Connect using:

vmxnet3 Ethernet Adapter

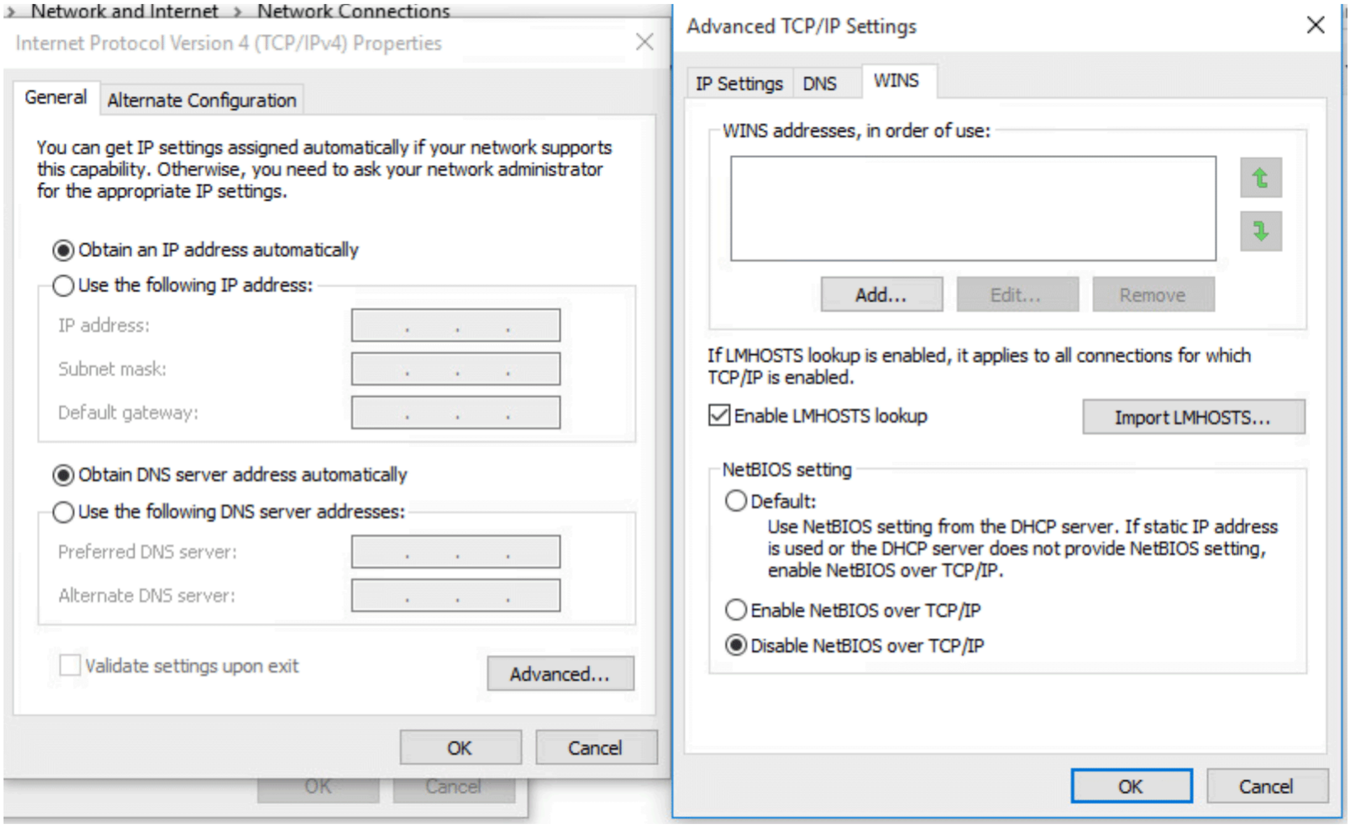
This connection uses the following items:

☑ QoS Packet Scheduler
☑ Link-Layer Topology Discovery Mapper I/O Driver
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Link-Layer Topology Discovery Responder
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. On the “General” tab click “Advanced” and navigate to the WINS tab, then select “Disable NetBIOS over TCP/IP” and select “Ok”.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

WINS addresses, in order of use:

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

NetBIOS setting

○ Default:

Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

Mitigations

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

References

- **T1171 - LLMNR/NBT-NS Poisoning and Relay**
- **Local Network Vulnerabilities - LLMNR and NTB-NS Poisoning**
- **How to Disable LLMNR and Why You Want To**

Kerberoasting

CRITICAL 10

H3-2021-0038

Affected Assets

- Kerb Tgs 23 Hash for svc_sync
- Kerb Tgs 23 Hash for svc_okta_sso
- Kerb Tgs 23 Hash for svc_mssql
- Kerb Tgs 23 Hash for svc_solarwinds

Mitigations

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

References

- **MITRE ATT&CK Technique: Kerberoasting**
- **Group Managed Service Accounts Overview**

Credential Dumping - Security Account Manager (SAM) Database

CRITICAL 10

H3-2021-0042

Affected Hosts

- 10.0.4.129 (win7.pod04.example.internal)
- 10.0.4.14 (win2008)
- 10.0.220.54 (winxp.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- 10.2.4.5 (horizon.pod04.example.internal)
- 10.0.4.4 (svr01.pod04.example.internal)
- 10.0.229.3 (ex.smoke.net)
- 10.0.40.89
- 10.0.229.6 (app4.smoke.net)
- 10.0.40.72
- 10.0.4.133
- 10.0.220.52 (win7.smoke.net)
- 10.0.220.6 (app2.smoke.net)
- 10.0.40.70
- 10.0.4.9
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- 10.0.40.76
- 10.0.4.136 (win7-32)
- 10.0.4.8
- 10.0.229.11 (fs.smoke.net)

Mitigations

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

References

- **MITRE ATT&CK Technique: OS Credential Dumping: Security Account Manager**
- **Local Administrator Password Solution (LAPS)**

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

CRITICAL 10

H3-2021-0044

Affected Hosts

- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- 10.0.40.89
- 10.2.4.5 (horizon.pod04.example.internal)
- 10.0.220.52 (win7.smoke.net)
- 10.0.220.6 (app2.smoke.net)
- 10.0.4.4 (svr01.pod04.example.internal)
- 10.0.4.129 (win7.pod04.example.internal)
- 10.0.229.6 (app4.smoke.net)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- 10.0.4.8
- 10.0.4.135 (win8)
- 10.0.40.72
- 10.0.229.11 (fs.smoke.net)
- 10.0.40.76
- 10.0.4.9
- 10.0.229.3 (ex.smoke.net)

Mitigations

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

References

- **MITRE ATT&CK Technique: OS Credential Dumping: LSASS Memory**
- **Local Administrator Password Solution (LAPS)**
- **Manage Windows Defender Credential Guard**
- **Attack Surface Reduction**

Active Directory Certificate Services Misconfiguration Privilege Escalation - Subject Alternative Name

CRITICAL 10

H3-2022-0016

Affected Hosts

- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)

Mitigations

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

References

- **Certified Pre-Owned: Abusing Active Directory Certificate Services**
- **SpectreOps - Certified Pre-Owned**
- **Hidden Dangers: Certificate Subject Alternative Names (SANs)**

Active Directory Certificate Services Misconfigured Enrollment Agent Template

CRITICAL 10

H3-2022-0018

Affected Hosts

- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)

Mitigations

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

References

- **Certified Pre-Owned: Abusing Active Directory Certificate Services**
- **SpectreOps - Certified Pre-Owned**

Active Directory Certificate Services Misconfigured Template Access Controls

CRITICAL 10

H3-2022-0020

Affected Hosts

- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)

Mitigations

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

References

- **Certified Pre-Owned: Abusing Active Directory Certificate Services**
- **SpectreOps - Certified Pre-Owned**
- **Certipy**

Credential Reuse - Shared Windows Local User and Domain User Accounts

CRITICAL 10

H3-2022-0085

Affected Hosts

- 10.2.4.5 (horizon.pod04.example.internal)
- 10.2.4.5 (horizon.pod04.example.internal)
- 10.0.220.53 (win10.smoke.net)
- 10.2.4.5 (horizon.pod04.example.internal)

Mitigations

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

References

- **NIST Password Guidelines**

Credential Dumping - Data Protection API (DPAPI) Secrets

CRITICAL 10

H3-2023-0019

Affected Hosts

- 10.0.220.52 (win7.smoke.net)
- 10.0.4.6 (az01.pod04.example.internal)
- 10.0.40.84
- 10.0.4.129 (win7.pod04.example.internal)
- 10.0.229.11 (fs.smoke.net)
- 10.0.229.3 (ex.smoke.net)

Mitigations

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

References

- **MITRE ATT&CK Technique: OS Credential Dumping**

Password in Active Directory User Attribute

CRITICAL 10

H3-2023-0029

Affected Assets

- Cleartext Password for bhuser
- Cleartext Password for enc_bhuser

Mitigations

- If the user is not being utilized, consider removing the affected user from Active Directory.
- Remove the Attribute from the Active Directory User, using the Active Directory Users and Computers utility.
- Determine if any third-party software is utilizing the passwords stored in the 'userPassword', 'unicodePwd', 'UnixUserPassword', or 'sfupassword' fields for the affected user. If so, determine if updates are available to the software to allow for the attribute to be removed.

References

- **Bloodhound - ReadTheDocs - User Node, Extra Properties**
- **Microsoft Open Specifications - Active Directory Schema, Attribute userPassword**

Netlogon Elevation of Privilege Vulnerability

CRITICAL 10

CVE-2020-1472

Affected Hosts

- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)

Apply the February 9, 2021 Security Patch to the Host

Microsoft released a patch on February 9, 2021 addressing this vulnerability. To install it, apply the latest security updates on every Domain Controller. For more information, see **CVE-2020-1472 Security Bulletin**

Mitigations

- Apply the updates referenced in Microsoft Security Bulletin CVE-2020-1472 and configure the registry key that will enable Enforcement Mode.
- On February 9, 2021 a Windows Update will automatically enable Enforcement Mode on all Domain Controllers regardless of the registry key value.

References

- **CVE-2020-1472**
- **Microsoft Security Bulletin CVE-2020-1472**
- **Microsoft Registry Key for Enforcement Mode**

GitLab ExifTool Remote Code Execution Vulnerability

CRITICAL 10

CVE-2021-22205

Affected Host

- 10.2.51.107

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**
- **Gitlab Hotpatch Instructions for CVE-2021-22205**
- **Gitlab issue 327121**
- **CVE-2021-22205**

Credential Dumping - Local Security Authority (LSA) Secrets

CRITICAL 10

H3-2021-0043

Affected Hosts

- 10.0.4.6 (az01.pod04.example.internal)
- 10.0.229.11 (fs.smoke.net)
- 10.0.220.54 (winxp.smoke.net)
- 10.0.229.3 (ex.smoke.net)
- 10.0.40.89
- 10.0.220.52 (win7.smoke.net)
- 10.0.229.6 (app4.smoke.net)
- 10.0.40.70
- 10.0.220.6 (app2.smoke.net)
- 10.2.4.5 (horizon.pod04.example.internal)
- 10.0.40.76
- 10.0.4.129 (win7.pod04.example.internal)
- 10.0.4.4 (svr01.pod04.example.internal)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)

Mitigations

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

References

- **MITRE ATT&CK Technique: OS Credential Dumping: LSA Secrets**
- **MITRE ATT&CK Technique: OS Credential Dumping: Cached Domain Credentials**

Microsoft Entra (AzureAD) Connect Credential Dumping

CRITICAL 10

H3-2024-0010

Affected Host

- 10.0.4.6 (az01.pod04.example.internal)

Mitigations

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

References

- **MITRE ATT&CK Technique: OS Credential Dumping**
- **Dirk-jan Mollema: Updating adconnectdump - a journey into DPAPI**

Microsoft Entra (AzureAD) - Over-Privileged Service Principal

CRITICAL 10

H3-2024-0011

Affected Assets

- Entra Service Principal CBR-CICD-SP-STAGE
- Entra Service Principal atk-dev-pod-app

Mitigations

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

References

- **SpectreOps - Service Principal Abuse**
- **Dirk-jan Mollema: Azure AD privilege escalation - Taking over default application permissions as Application Admin**
- **Microsoft - Using role-based access control for applications**
- **Microsoft - What is Conditional Access?**

Microsoft Entra (AzureAD) - Service Principal Takeover

CRITICAL 10

H3-2024-0012

Affected Assets

- Microsoft Entra User sync_az01_97d10b16b452
- Entra Global Admin a-jsmith

Mitigations

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

References

- **Dirk-jan Mollema: Azure AD privilege escalation - Taking over default application permissions as Application Admin**
- **Fabian Bader - From on-prem to Global Admin without password reset**
- **Microsoft - Entra Built-In Roles**
- **Microsoft - What is Conditional Access?**

Credential Reuse - Windows Local Administrator Accounts

CRITICAL 9.9

H3-2022-0084

Affected Hosts

- 10.0.220.53 (win10.smoke.net)
- 10.0.4.4 (svr01.pod04.example.internal)
- 10.0.40.71
- 10.0.4.4 (svr01.pod04.example.internal)
- 10.0.4.22 (zoho.pod04.example.internal)
- 10.0.40.75
- 10.0.4.22 (zoho.pod04.example.internal)
- 10.0.4.130 (win10.pod04.example.internal)
- 10.0.4.14 (win2008)
- 10.0.4.3 (ex01.pod04.example.internal)
- 10.0.40.64
- 10.0.4.6 (az01.pod04.example.internal)
- 10.0.40.95
- 10.0.4.136 (win7-32)
- 10.0.4.9
- 10.0.4.6 (az01.pod04.example.internal)
- 10.0.4.8
- 10.0.4.134
- 10.0.229.3 (ex.smoke.net)
- 10.0.4.3 (ex01.pod04.example.internal)

Mitigations

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

References

- **Local Administrator Password Solution (LAPS)**
- **NIST Password Guidelines**

UnrealIRCd Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2010-2075

Affected Host

- 10.0.4.24 (irc.testirc.net)

Mitigations

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

References

- **CVE-2010-2075**

Apache Struts 2 Prefixed Parameters OGNL Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2013-2251

Affected Host

- 10.2.51.105

Mitigations

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

References

- **Apache Advisory and Patches**
- **CVE-2013-2251**

Apache ActiveMQ Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2016-3088

Affected Host

- 10.0.229.4 (ex2.smoke.net)

Mitigations

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

References

- **Apache ActiveMQ Advisory**
- **Red Hat Guidance**
- **CVE-2016-3088**

Apache Shiro RememberME Cookie Deserialization Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2016-4437

Affected Host

- 10.2.51.105

Mitigations

- Upgrade to Apache Shiro 1.2.5 or later.

References

- **Vendor Acknowledgement**
- **CVE-2016-4437**

Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability Bypass

CRITICAL 9.8

CVE-2017-10271

Affected Host

- 10.2.51.105

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**
- **CVE-2017-10271**

Oracle Weblogic wls-wsat Component XML Deserialization Vulnerability CRITICAL 9.8

CVE-2017-3506

Affected Host

- 10.2.51.105

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**
- **Oracle Critical Patch Update Advisory**
- **Remote OS Command Execution on Oracle Weblogic server via [CVE-2017-3506]**
- **8220 Gang Exploiting Oracle WebLogic Flaw to Hijack Servers and Mine Cryptocurrency**

Apache Struts2 Content Header Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2017-5638

Affected Host

- 10.2.51.105

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**
- **Apache Struts Security Advisory S2-046**
- **CVE-2017-5638 Detail**

Apache Struts2 S2-048 Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2017-9791

Affected Host

- 10.2.51.105

Mitigations

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

References

- **S2-048**
- **CVE-2017-9791 Detail**

Vulnerable Cisco Smart Install

CRITICAL 9.8

CVE-2018-0171

Affected Host

- 10.0.100.253

Table of Contents

- **Option 1: Upgrade IOS to a Secure Version**
- **Option 2: Disable the Smart Install Service**
- **Option 3: Apply Firewall Whitelist Rules**

Option 1: Upgrade IOS to a Secure Version

If the hardware and licensing supports upgrading to a newer IOS version, follow the official “Software Installation and Upgrade Procedures” from Cisco **here**. Otherwise follow Option 2 for disabling the Smart Install service.

Option 2: Disable the Smart Install Service

It is recommended, that if the Smart Install service is not in use, to completely disable the service by issuing the following command from an elevated Cisco prompt:

```
no vstack
```

Option 3: Apply Firewall Whitelist Rules

It is recommended that if the Smart Install service is not in use to apply firewall rules limiting access to the service on port 4876/tcp. The following command from an elevated Cisco prompt will limit all access to that port:

```
ip access-list extended CFC_DISABLE_ALL_SMI deny tcp any any eq 4786 permit ip any any
```

Mitigations

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

References

- **CVE-2018-0171**

Apache Solr Velocity Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2019-17558

Affected Host

- 10.2.51.108

Mitigations

- Upgrade to Apache Solr 8.4 or greater.

References

- **CVE-2019-17558**
- **Vendor Advisory**
- **Proof of Concept and Writeup**

SaltStack Salt Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2020-11651

Affected Host

- 10.0.220.50

Mitigations

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

References

- **CVE-2020-11651**
- **SALT 2019.2.4 RELEASE NOTES**
- **Salt 3000.2 Release Notes**

Apache Airflow Experimental API Authentication Bypass Vulnerability

CRITICAL 9.8

CVE-2020-13927

Affected Host

- 10.2.51.102

Mitigations

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

References

- **CVE-2020-13927**
- **Vendor Advisory**

Oracle WebLogic Java Deserialization Vulnerability - Console Component

CRITICAL 9.8

CVE-2020-14882

Affected Host

- 10.2.51.105

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**
- **Oracle Security Advisory for CVE-2020-14882**
- **Oracle Security Advisory for CVE-2020-14750**

Apache Airflow Authorization Bypass Vulnerability

CRITICAL 9.8

CVE-2020-17526

Affected Host

- 10.2.51.102

Mitigations

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

References

- **CVE-2020-17526**
- **Vendor Advisory**

VMware vCenter Server Access Control Vulnerability

CRITICAL 9.8

CVE-2020-3952

Affected Hosts

- 10.0.40.99 (vcsa.smoke.net)
- 10.0.4.29 (vcsa.pod04.example.internal)

Mitigations

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

References

- **CVE-2020-3952**
- **VMware Security Advisories**

VMware vCenter vROPS Plugin Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2021-21972

Affected Hosts

- 10.0.4.29 (vcsa.pod04.example.internal)
- 10.0.40.99 (vcsa.smoke.net)

Table of Contents

- Option 1: Upgrade vCenter Instance
- Option 2: Disable Plugins on Virtual Server Appliance Deployments
- Option 3: Disable Plugins on Windows-based vCenter Server Deployments
- Validation

Option 1: Upgrade your vCenter Instance

Upgrade the major release version to a version at or above as indicated below:

- Version 7.0 – Patched 7.0 U1c or later
- Version 6.7 – Patched 6.7 U3l or later
- Version 6.5 – Patched 6.5 U3n or later

Option 2: Disable Plugins on Virtual Server Appliance Deployments

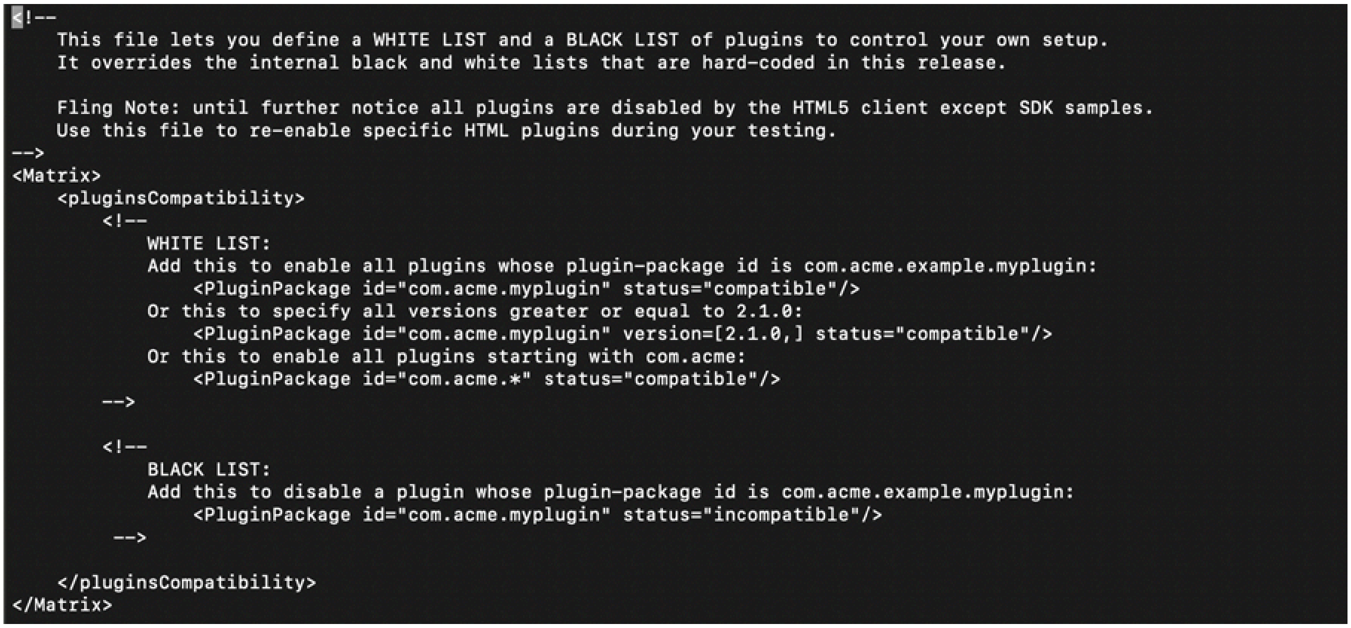
Important: Plugins must be set to "incompatible." Disabling a plugin from within the UI does not prevent exploitation. The following actions must be performed on both the active and passive nodes in environments running vCenter High Availability (VCHA).

1. Connect to the vCSA using an SSH session and root credentials.
2. Backup the /etc/vmware/vsphere-ui/compatibility-matrix.xml file:

```
cp -v /etc/vmware/vsphere-ui/compatibility-matrix.xml /etc/vmware/vsphere-ui/compatibility-matrix.xml.backup
```

1. Open the compatibility-matrix.xml file in a text editor.

- NOTE: Contents of this file looks like below:

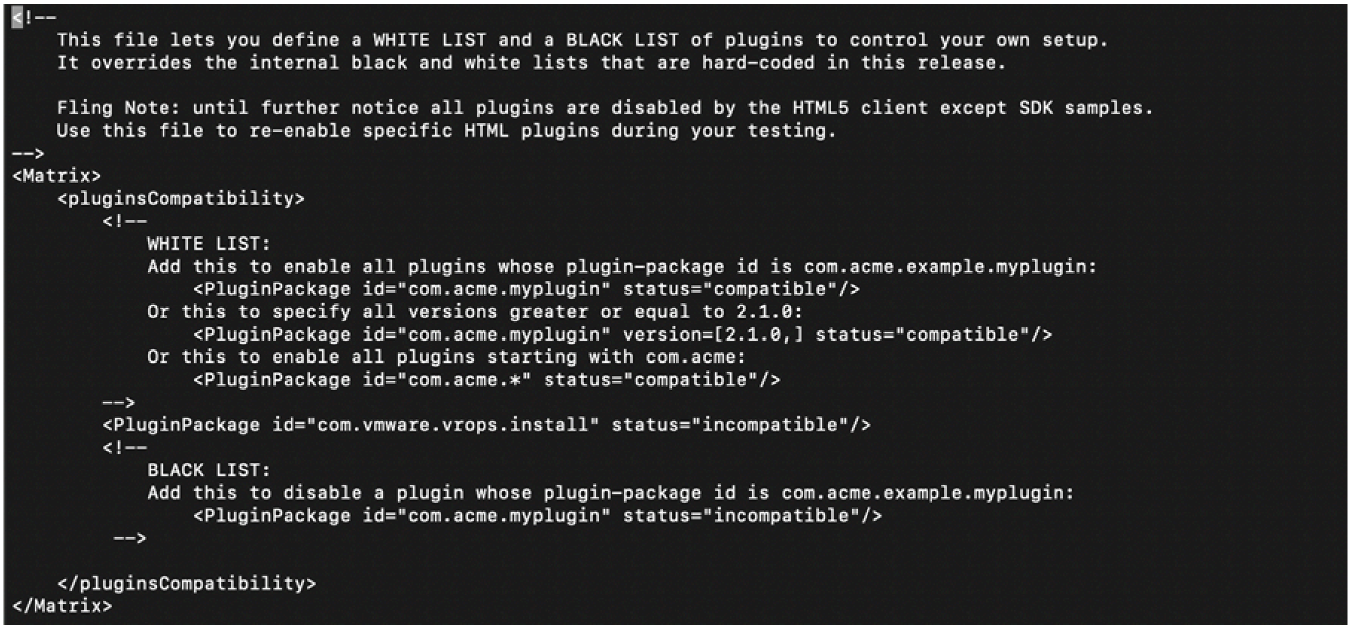


```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    It overrides the internal black and white lists that are hard-coded in this release.

    Fling Note: until further notice all plugins are disabled by the HTML5 client except SDK samples.
    Use this file to re-enable specific HTML plugins during your testing.
-->
<Matrix>
    <pluginsCompatibility>
        <!--
            WHITE LIST:
            Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="compatible"/>
            Or this to specify all versions greater or equal to 2.1.0:
                <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
            Or this to enable all plugins starting with com.acme:
                <PluginPackage id="com.acme.*" status="compatible"/>
        -->

        <!--
            BLACK LIST:
            Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="incompatible"/>
         -->

    </pluginsCompatibility>
</Matrix>
```

1. Add the following line in between the WHITE LIST and BLACK LIST blocks:

```
<PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
```

- NOTE: The file should like below:



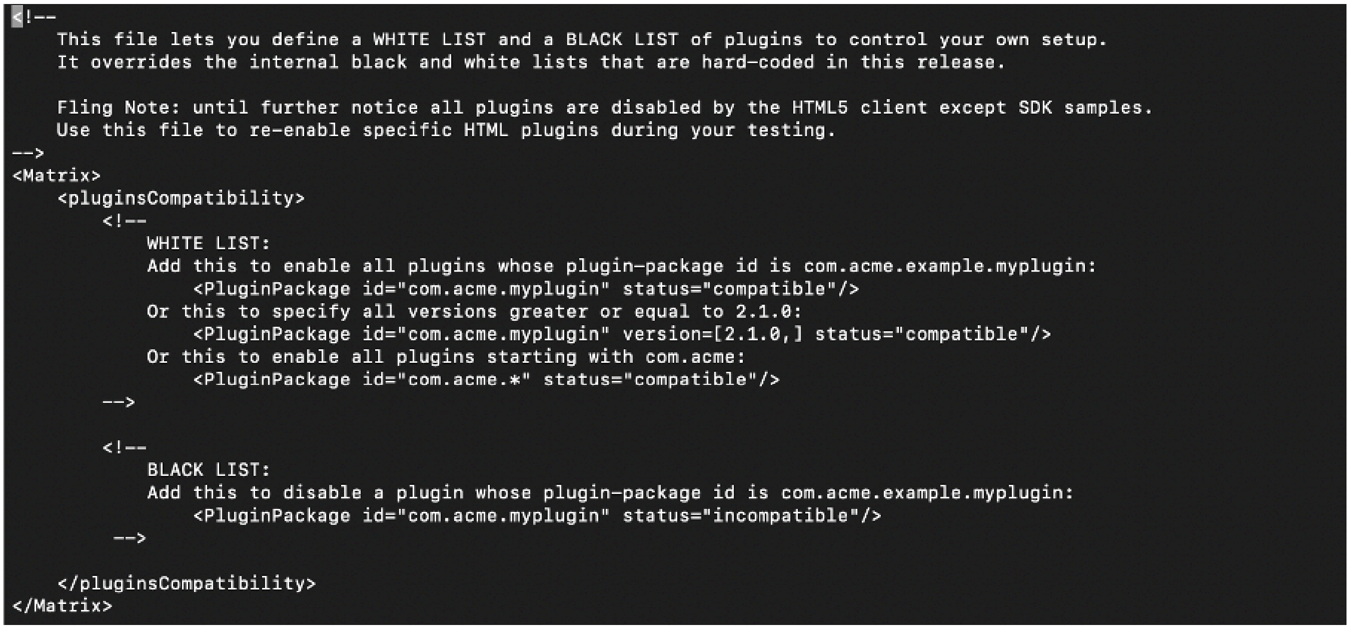
```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    It overrides the internal black and white lists that are hard-coded in this release.

    Fling Note: until further notice all plugins are disabled by the HTML5 client except SDK samples.
    Use this file to re-enable specific HTML plugins during your testing.
-->
<Matrix>
    <pluginsCompatibility>
        <!--
            WHITE LIST:
            Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="compatible"/>
            Or this to specify all versions greater or equal to 2.1.0:
                <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
            Or this to enable all plugins starting with com.acme:
                <PluginPackage id="com.acme.*" status="compatible"/>
        -->
        <PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
        <!--
            BLACK LIST:
            Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="incompatible"/>
         -->

    </pluginsCompatibility>
</Matrix>
```

1. Save and close the compatibility-matrix.xml file.
2. Stop and restart the vsphere-ui service using the commands:

```
service-control --stop vsphere-ui.
service-control --start vsphere-ui.
```

Option 3: Disable Plugins on Windows-based vCenter Server Deployments

1. Use Remote Desktop to access the Windows based vCenter Server.
2. Take a backup of the C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\compatibility-matrix.xml file.
3. Content of this file looks like below:

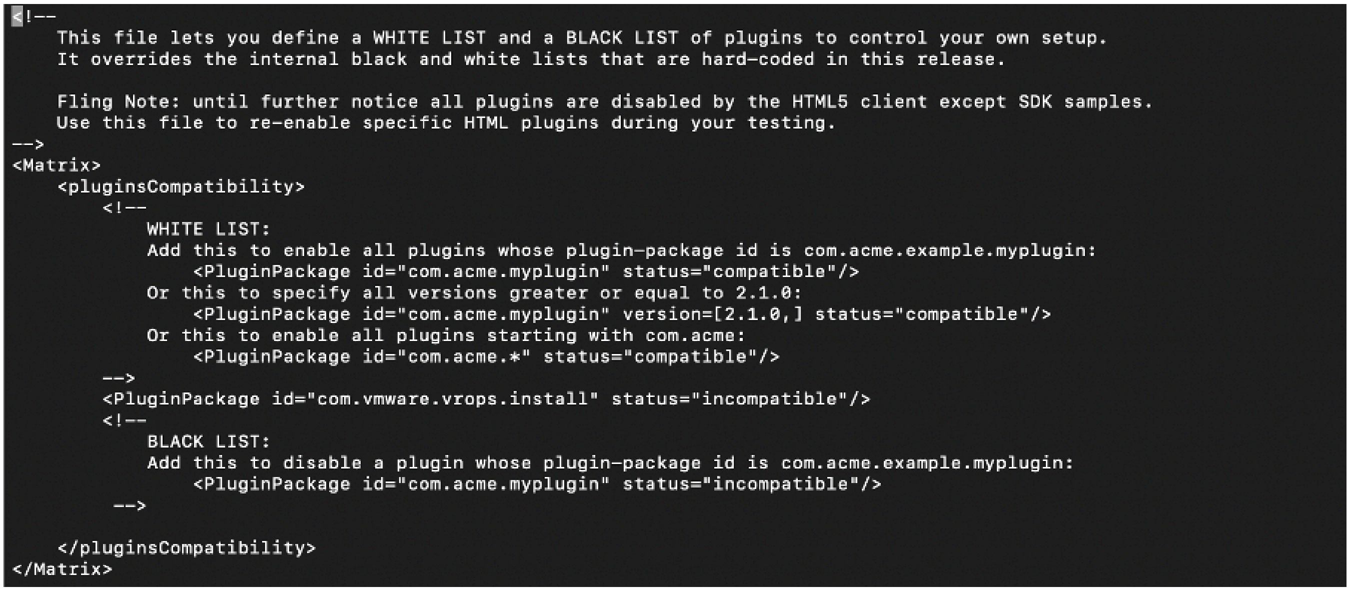


```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    It overrides the internal black and white lists that are hard-coded in this release.

    Fling Note: until further notice all plugins are disabled by the HTML5 client except SDK samples.
    Use this file to re-enable specific HTML plugins during your testing.
-->
<Matrix>
    <pluginsCompatibility>
        <!--
            WHITE LIST:
            Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="compatible"/>
            Or this to specify all versions greater or equal to 2.1.0:
                <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
            Or this to enable all plugins starting with com.acme:
                <PluginPackage id="com.acme.*" status="compatible"/>
        -->

        <!--
            BLACK LIST:
            Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="incompatible"/>
         -->

    </pluginsCompatibility>
</Matrix>
```

4. Add the following line in between the WHITE LIST and BLACK LIST blocks:

```
<PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
```

- NOTE: The file should look like below:



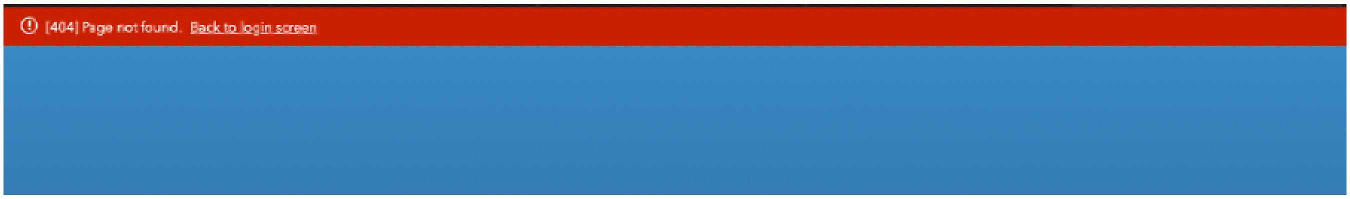
```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    It overrides the internal black and white lists that are hard-coded in this release.

    Fling Note: until further notice all plugins are disabled by the HTML5 client except SDK samples.
    Use this file to re-enable specific HTML plugins during your testing.
-->
<Matrix>
    <pluginsCompatibility>
        <!--
            WHITE LIST:
            Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="compatible"/>
            Or this to specify all versions greater or equal to 2.1.0:
                <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
            Or this to enable all plugins starting with com.acme:
                <PluginPackage id="com.acme.*" status="compatible"/>
         -->
        <PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
        <!--
            BLACK LIST:
            Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="incompatible"/>
         -->

    </pluginsCompatibility>
</Matrix>
```

1. Stop and restart the vsphere-ui service using the commands:

```
C:\Program Files\VMware\vCenter Server\bin> service-control --stop vsphere-ui
C:\Program Files\VMware\vCenter Server\bin> service-control --start vsphere-ui
```

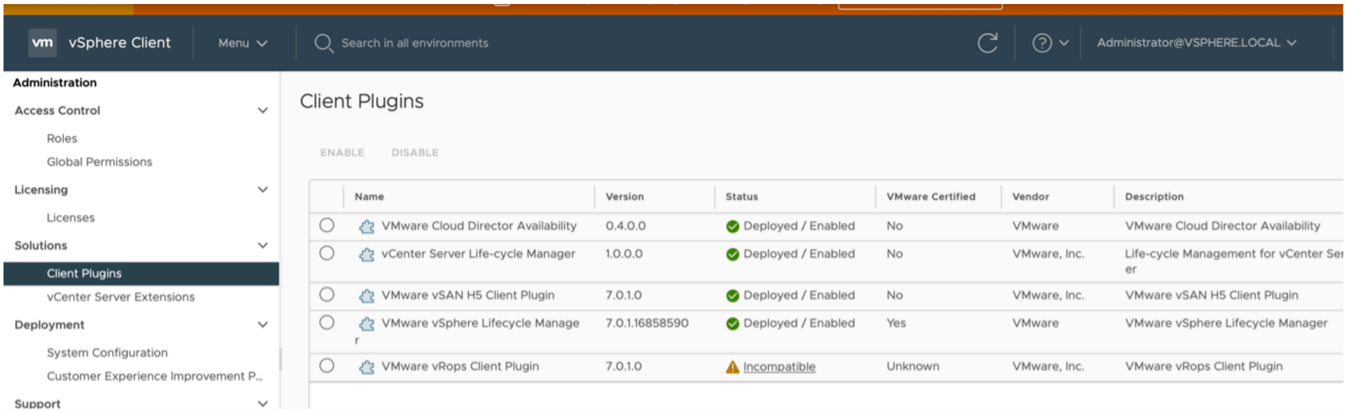
Validation

1. Navigate to the https://{your-vcenter-hostname}/ui/vropspluginui/rest/services/checkmobregister. This page should display a 404/Not Found error, as shown below:



ⓘ [404] Page not found. Back to login screen

2. From the vSphere Client (HTML 5), the VMware vROPS Client plugin can be seen as “incompatible” under `Administration > Solutions > Client Plugins` as shown below:



Client Plugins

	Name	Version	Status	VMware Certified	Vendor	Description
○	VMware Cloud Director Availability	0.4.0.0	✓ Deployed / Enabled	No	VMware	VMware Cloud Director Availability
○	vCenter Server Life-cycle Manager	1.0.0.0	✓ Deployed / Enabled	No	VMware, Inc.	Life-cycle Management for vCenter Server
○	VMware vSAN H5 Client Plugin	7.0.1.0	✓ Deployed / Enabled	No	VMware, Inc.	VMware vSAN H5 Client Plugin
○	VMware vSphere Lifecycle Manager	7.0.1.16858590	✓ Deployed / Enabled	Yes	VMware	VMware vSphere Lifecycle Manager
○	VMware vRops Client Plugin	7.0.1.0	⚠ Incompatible	Unknown	VMware, Inc.	VMware vRops Client Plugin

3. This confirms that the vRops Client Plugin is set to “Incompatible”.

Mitigations

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

References

- **CVE-2021-21972**
- **Proof of Concept for CVE-2021-21972**
- **VMware Advisory VMSA-2021-0002**
- **VMware KB82374**

VMware vRealize Operations Manager Server-Side Request Forgery Vulnerability

CRITICAL 9.8

CVE-2021-21975

Affected Hosts

- 10.0.4.27
- 10.0.40.87

Mitigations

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

References

- **VMware Security Bulletin**
- **Metasploit Exploit**

VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2021-21985

Affected Hosts

- 10.0.40.99 (vcsa.smoke.net)
- 10.0.4.29 (vcsa.pod04.example.internal)

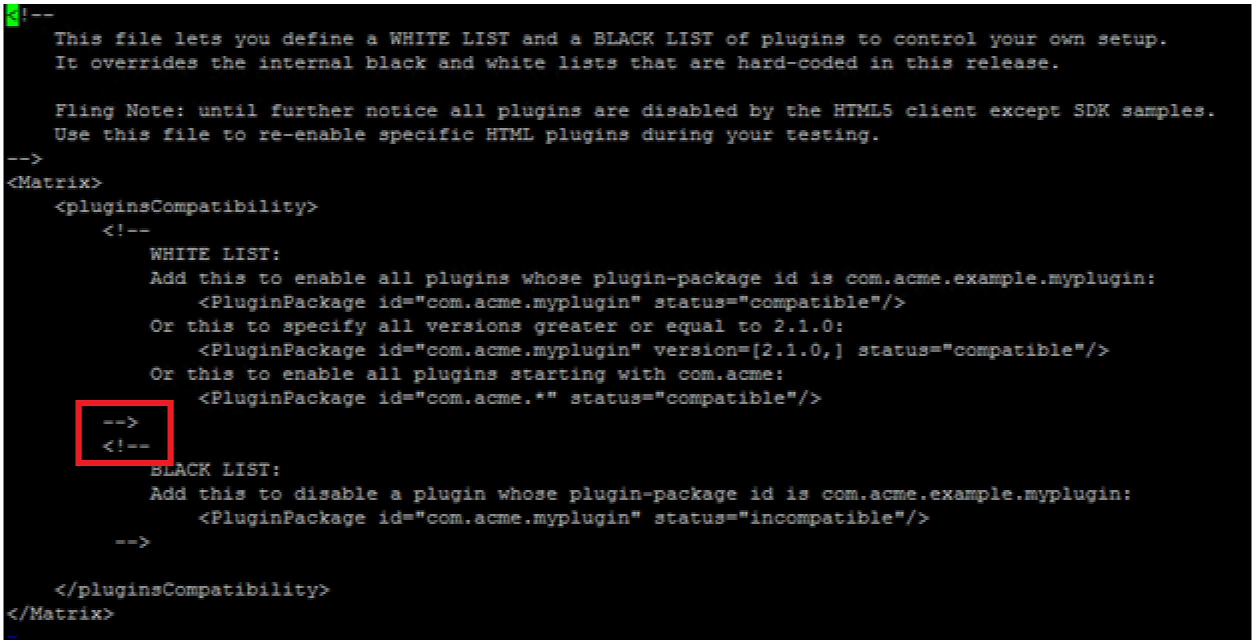
Table of Contents

- **Option 1: For vCenter Server Appliances**
- **Option 2: For Windows-based vCenter Servers**

Option 1: For vCenter Server Appliances

1. Connect to the vCSA using an SSH session and root credentials.
2. Backup the /etc/vmware/vsphere-ui/compatibility-matrix.xml file.
3. Open the compatibility-matrix.xml file in a text editor:

- Note: Content of an unedited file should look similar to the following:



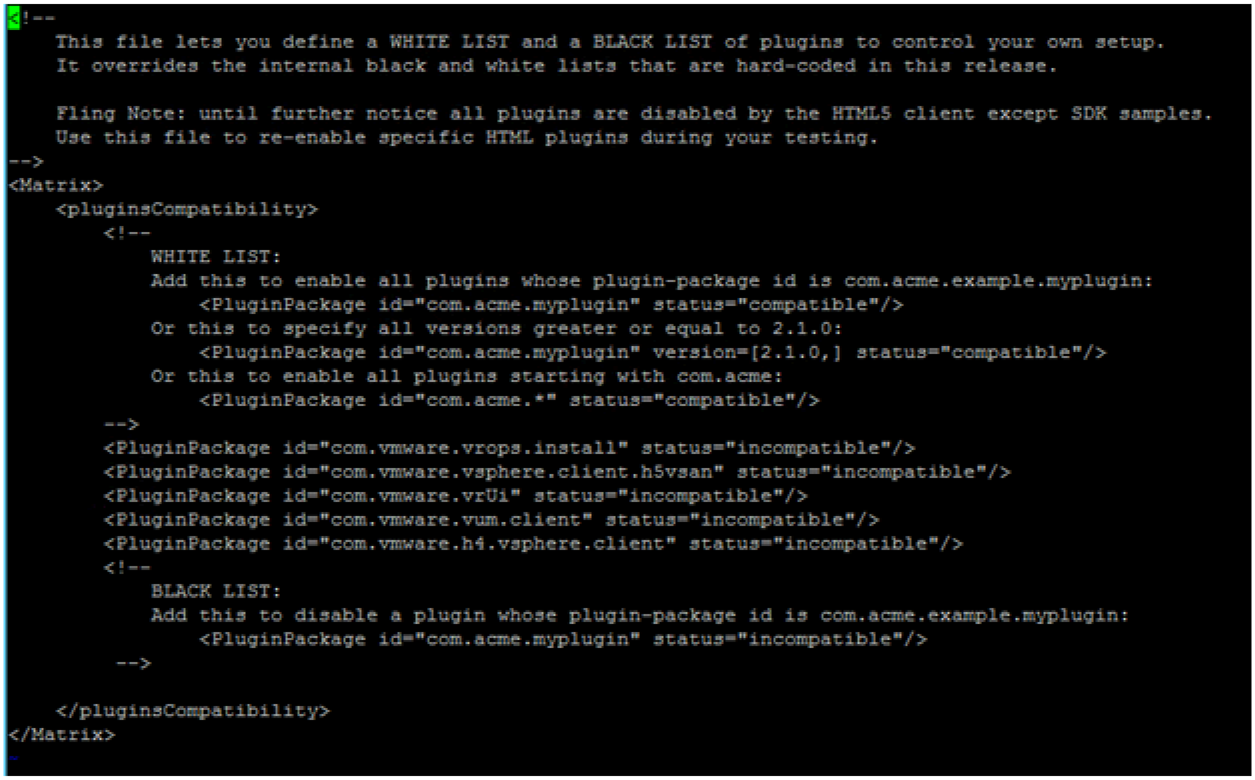
```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    It overrides the internal black and white lists that are hard-coded in this release.

    Fling Note: until further notice all plugins are disabled by the HTML5 client except SDK samples.
    Use this file to re-enable specific HTML plugins during your testing.
-->
<Matrix>
    <pluginsCompatibility>
        <!--
            WHITE LIST:
            Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="compatible"/>
            Or this to specify all versions greater or equal to 2.1.0:
                <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
            Or this to enable all plugins starting with com.acme:
                <PluginPackage id="com.acme.*" status="compatible"/>
        -->
        <!--
            BLACK LIST:
            Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="incompatible"/>
         -->

    </pluginsCompatibility>
</Matrix>
```

1. To disable all plugins with disclosed vulnerabilities, add the following lines as shown below:

- Note: These entries should be added between the -> and <!— entries highlighted above.

```
<PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
<PluginPackage id="com.vmware.vsphere.client.h5vsan" status="incompatible"/>
<PluginPackage id="com.vmware.vrUi" status="incompatible"/>
<PluginPackage id="com.vmware.vum.client" status="incompatible"/>
<PluginPackage id="com.vmware.h4.vsphere.client" status="incompatible"/>
```

1. The file should look like the following image:



```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    It overrides the internal black and white lists that are hard-coded in this release.

    Fling Note: until further notice all plugins are disabled by the HTML5 client except SDK samples.
    Use this file to re-enable specific HTML plugins during your testing.
-->
<Matrix>
    <pluginsCompatibility>
        <!--
            WHITE LIST:
            Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="compatible"/>
            Or this to specify all versions greater or equal to 2.1.0:
                <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
            Or this to enable all plugins starting with com.acme:
                <PluginPackage id="com.acme.*" status="compatible"/>
        -->
        <PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
        <PluginPackage id="com.vmware.vsphere.client.h5vsan" status="incompatible"/>
        <PluginPackage id="com.vmware.vrUi" status="incompatible"/>
        <PluginPackage id="com.vmware.vum.client" status="incompatible"/>
        <PluginPackage id="com.vmware.h4.vsphere.client" status="incompatible"/>
        <!--
            BLACK LIST:
            Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="incompatible"/>
         -->

    </pluginsCompatibility>
</Matrix>
```

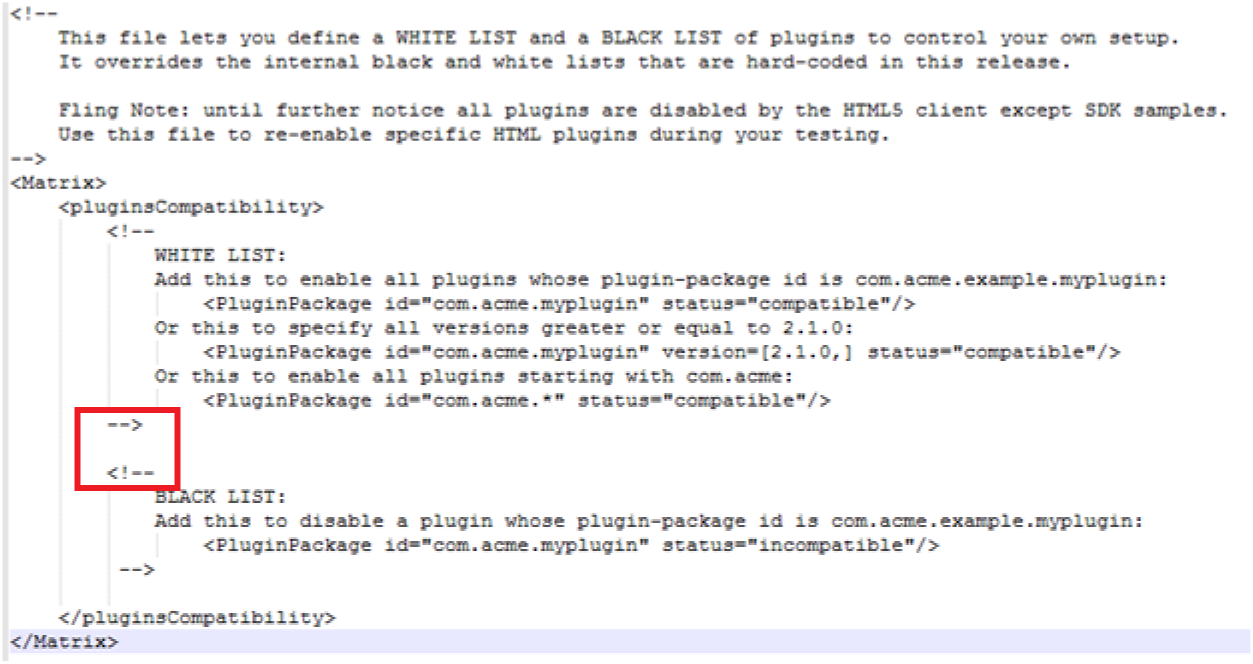
2. Save and close the compatibility-matrix.xml file.
3. Stop and restart the vsphere-ui service using these commands:

```
service-control --stop vsphere-ui
service-control --start vsphere-ui
```

Option 2: For Windows-based vCenter Servers

1. Use Remote Desktop to access the Windows-based vCenter Server.
2. Take a backup of the C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\compatibility-matrix.xml file.

3. Open the compatibility-matrix.xml file in a text editor:



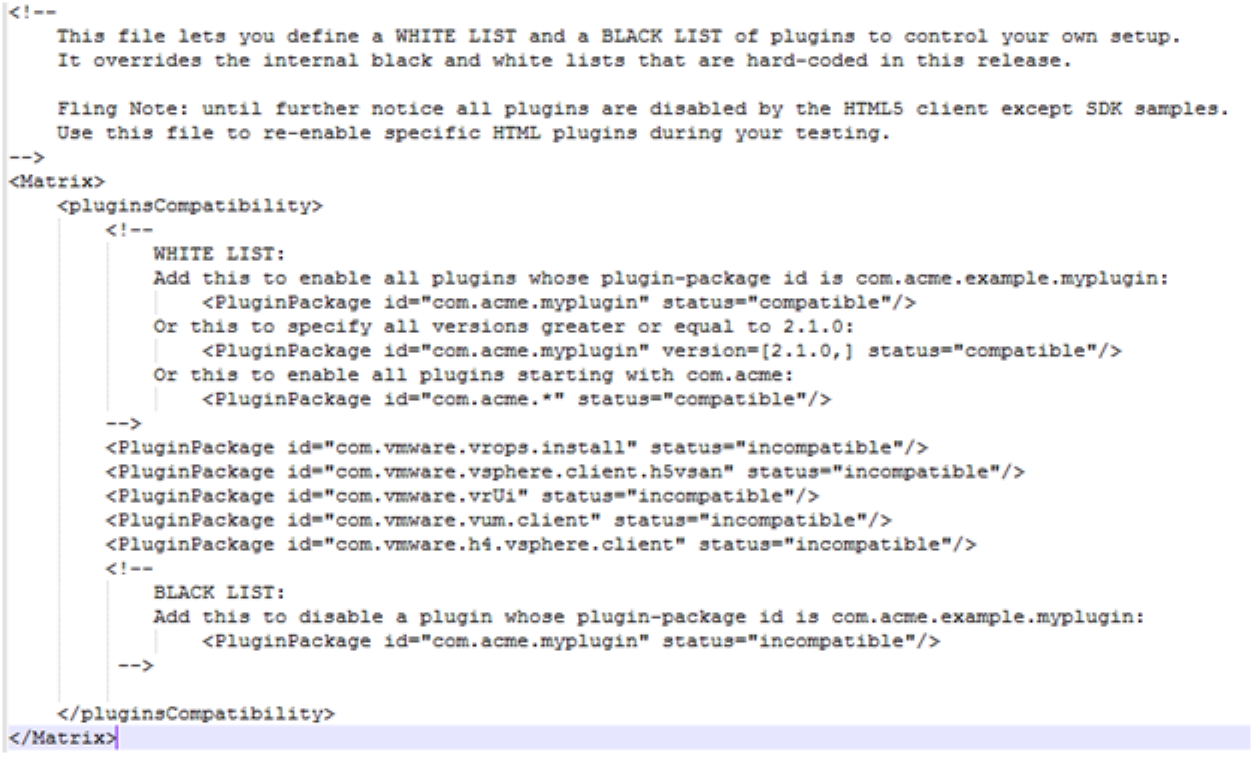
```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    It overrides the internal black and white lists that are hard-coded in this release.

    Fling Note: until further notice all plugins are disabled by the HTML5 client except SDK samples.
    Use this file to re-enable specific HTML plugins during your testing.
-->
<Matrix>
    <pluginsCompatibility>
        <!--
            WHITE LIST:
            Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="compatible"/>
            Or this to specify all versions greater or equal to 2.1.0:
                <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
            Or this to enable all plugins starting with com.acme:
                <PluginPackage id="com.acme.*" status="compatible"/>
        -->

        <!--
            BLACK LIST:
            Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="incompatible"/>
         -->

    </pluginsCompatibility>
</Matrix>
```

4. To disable all plugins with disclosed vulnerabilities, add the following lines as shown below:

- Note: These entries should be added between the -> and <!— entries highlighted above

```
<PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
<PluginPackage id="com.vmware.vsphere.client.h5vsan" status="incompatible"/>
<PluginPackage id="com.vmware.vrUi" status="incompatible"/>
<PluginPackage id="com.vmware.vum.client" status="incompatible"/>
<PluginPackage id="com.vmware.h4.vsphere.client" status="incompatible"/>
```

1. The file should look like the photo below:



```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    It overrides the internal black and white lists that are hard-coded in this release.

    Fling Note: until further notice all plugins are disabled by the HTML5 client except SDK samples.
    Use this file to re-enable specific HTML plugins during your testing.
-->
<Matrix>
    <pluginsCompatibility>
        <!--
            WHITE LIST:
            Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="compatible"/>
            Or this to specify all versions greater or equal to 2.1.0:
                <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
            Or this to enable all plugins starting with com.acme:
                <PluginPackage id="com.acme.*" status="compatible"/>
        -->
        <PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
        <PluginPackage id="com.vmware.vsphere.client.h5vsan" status="incompatible"/>
        <PluginPackage id="com.vmware.vrUi" status="incompatible"/>
        <PluginPackage id="com.vmware.vum.client" status="incompatible"/>
        <PluginPackage id="com.vmware.h4.vsphere.client" status="incompatible"/>
        <!--
            BLACK LIST:
            Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin:
                <PluginPackage id="com.acme.myplugin" status="incompatible"/>
         -->

    </pluginsCompatibility>
</Matrix>
```

2. Save and close the file.

3. In a Windows command prompt, stop and restart the vsphere-ui service using these commands:

```
C:\Program Files\VMware\vCenter Server\bin> service-control --stop vsphere-ui
C:\Program Files\VMware\vCenter Server\bin> service-control --start vsphere-ui
```

Mitigations

- Apply all updates and patch to the latest vendor-supported version.
- Apply workarounds described in VMware KB83829.

References

- **CVE-2021-21985**
- **Metasploit Module**
- **VMware Advisory VMSA-2021-0010**
- **VMware KB83829**

Apache mod_proxy Server-Side Request Forgery Vulnerability

CRITICAL 9.8

CVE-2021-40438

Affected Hosts

- 10.2.4.132 (coldfusion18.pod04.example.internal)
- 10.2.13.132 (docker.pod13.example.internal)

Mitigations

- This vulnerability affects Apache HTTP Server 2.4.48 and earlier. Upgrade the product to the latest version.

References

- **What is SSRF?**
- **Apache 2.4 Vulnerabilities**
- **CVE-2021-40438**

Apache Log4j2 Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2021-44228

Affected Hosts

- 10.2.4.132 (coldfusion18.pod04.example.internal)
- 10.0.40.79
- 10.0.220.200 (coldfusion18.smoke.net)
- 10.0.4.28
- 10.2.51.108
- 10.2.13.132 (docker.pod13.example.internal)
- 10.2.51.104
- 10.0.40.114
- 10.2.51.106
- 10.2.51.104
- 10.2.51.107

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**
- **Compilation of Vendor Advisories**
- **Cheat Sheet Reference Guide**
- **Horizon3.ai: The Long Tail of Log4Shell Exploitation**
- **Understanding Log4Shell: the Apache log4j2 Remote Code Execution Vulnerability**
- **Apache Log4j2 Release Notes**
- **CVE-2021-44228**

Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability

CRITICAL 9.8

CVE-2021-44515

Affected Hosts

- 10.0.4.22 (zoho.pod04.example.internal)
- 10.0.4.22 (zoho.pod04.example.internal)
- 10.0.4.22 (zoho.pod04.example.internal)
- 10.0.4.22 (zoho.pod04.example.internal)

Mitigations

- Use the exploit detection tool provided in the vendor's Security Advisory to check for signs of compromise.
- Apply all updates and patch to the latest vendor-supported version as described in the Security Advisory.

References

- **CVE-2021-44515: Security Advisory**
- **CVE-2021-44515 Detail**
- **ZohOwned: A Critical Authentication Bypass on Zoho ManageEngine Desktop Central**

Redis Lua Sandbox Escape

CRITICAL 9.8

CVE-2022-0543

Affected Host

- 10.0.220.50

Mitigations

- This vulnerability affects Debian-specific redis. Refer to the Debian Security Advisory to update the redis package using the package manager on the affected system.

References

- **Debian Security Advisory: DSA-5081**
- **Researcher Blog Post**
- **Metasploit Module**
- **CVE-2022-0543 Redis Vulnerability in NetApp Products | NetApp Product Security**
- **CVE-2022-0543**

F5 BIG-IP iControl REST Remote Command Execution Vulnerability

CRITICAL 9.8

CVE-2022-1388

Affected Hosts

- 10.0.4.7
- 10.2.4.98
- 10.0.40.80 (f5.smoke.net)

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**
- **Horizon3.ai: Deep Dive on CVE-2022-1388**
- **CVE-2022-1388**

Apache CouchDB Unauthenticated Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2022-24706

Affected Host

- 10.0.220.50

Mitigations

- Upgrade installation beyond 3.2.2.

References

- **CVE-2022-24706 Detail**
- **CVE-2022-24706: Apache CouchDB Remote Privilege Escalation**
- **Cluster setup**

Atlassian Confluence Namespace OGNL Injection Vulnerability

CRITICAL 9.8

CVE-2022-26134

Affected Host

- 10.0.40.54

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**
- **Zero-Day Exploitation of Atlassian Confluence**
- **CVE-2022-26134**

Zoho ManageEngine ADAudit Plus Remote Code Execution Vulnerability CRITICAL 9.8

CVE-2022-28219

Affected Hosts

- 10.0.4.22 (zoho.pod04.example.internal)
- 10.0.4.22 (zoho.pod04.example.internal)

Mitigations

- Update to ManageEngine ADAudit Plus build 7060 or later.

References

- **ManageEngine Advisory**
- **Horizon3.ai Blog Post**
- **CVE-2022-28219**

Fortinet FortiOS / FortiProxy / FortiSwitchManager Authentication Bypass Vulnerability

CRITICAL 9.8

CVE-2022-40684

Affected Hosts

- 10.0.40.67
- 10.0.4.25
- 10.0.40.67
- 10.0.4.25

Mitigations

- Apply all updates and patch to the latest vendor-supported version. This issue is fixed in FortiOS 7.2.2, FortiOS 7.0.7, FortiProxy 7.2.1, FortiProxy 7.0.7, and FortiSwitchManager 7.2.1.
- If updating is not possible, follow the mitigations in the Fortinet Security Advisory.

References

- **Fortinet Advisory**
- **Horizon3.ai Technical Deep Dive on CVE-2022-40684**
- **Horizon3.ai Indicators of Compromise for CVE-2022-40684**
- **CVE-2022-40684**

VMware vRealize Network Insight Remote Code Execution Vulnerability CRITICAL 9.8

CVE-2023-20887

Affected Host

- 10.0.4.26

Mitigations

- Apply the patches for VMSA-2023-0012 to the affected vRealize Network Insight device.

References

- **Vendor Advisory and Patches**
- **CISA Advisory**
- **CVE-2023-20887**

Atlassian Confluence Server - Improper Authorization

CRITICAL 9.8

CVE-2023-22518

Affected Host

- 10.0.40.54

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**
- **Vendor Advisory**

Adobe ColdFusion Unauthenticated File Read Vulnerability

CRITICAL 9.8

CVE-2023-26359

Affected Host

- 10.2.4.132 (coldfusion18.pod04.example.internal)

Mitigations

- Update to Adobe ColdFusion 2021 Update 6 or later if running ColdFusion 2021. Update to Adobe ColdFusion 2018 Update 16 or later if running ColdFusion 2018.

References

- **Adobe Security Advisory**
- **CVE-2023-26359**

Adobe ColdFusion Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2023-26360

Affected Host

- 10.2.4.132 (coldfusion18.pod04.example.internal)

Mitigations

- Update to Adobe ColdFusion 2021 Update 6 or later if running ColdFusion 2021. Update to Adobe ColdFusion 2018 Update 16 or later if running ColdFusion 2018.

References

- **Adobe Security Advisory**
- **CVE-2023-26360**
- **Original Proof Of Concept and Writeup**
- **Metasploit Proof of Concept**

Adobe ColdFusion Deserialization of Untrusted Data Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2023-29300

Affected Host

- 10.2.4.132 (coldfusion18.pod04.example.internal)

Mitigations

- Upgrade to ColdFusion 2018 Update 17 or later, ColdFusion 2021 Update 7 or later, or ColdFusion 2023 Update 1 or later.

References

- **CVE-2023-29300**
- **Adobe Advisory**

Citrix Gateway Unauthenticated Remote Code Execution

CRITICAL 9.8

CVE-2023-3519

Affected Host

- 10.0.40.218

Mitigations

- Upgrade to the latest version as indicated in the security advisory.

References

- **Citrix ADC and Citrix Gateway Security Bulletin**
- **Technical Summary of Observed Citrix CVE-2023-3519 Incidents**
- **Indicators of Compromise Scanner for Citrix ADC Zero-Day (CVE-2023-3519)**
- **CVE-2023-3519**

Adobe ColdFusion JNDI Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2023-38204

Affected Host

- 10.2.4.132 (coldfusion18.pod04.example.internal)

Mitigations

- Update to Adobe ColdFusion 2023 Update 2 or later if running ColdFusion 2023. Update to Adobe ColdFusion 2021 Update 9 or later if running ColdFusion 2021. Update to ColdFusion 2018 Update 19 or later if running ColdFusion 2018.

References

- **Adobe Security Advisory**
- **Original Proof Of Concept and Writeup For CVE-2023-38204**
- **Additional Analysis by GobySec on CVE-2023-38204**
- **CVE-2023-38205 Analysis and Writeup**

Apache ActiveMQ OpenWire Transport Remote Code Execution Vulnerability

CRITICAL 9.8

CVE-2023-46604

Affected Hosts

- 10.2.51.101
- 10.0.229.4 (ex2.smoke.net)
- 10.0.220.6 (app2.smoke.net)

Mitigations

- The vulnerability is fixed in Apache ActiveMQ versions 5.15.16, 5.16.7, 5.17.6, and 5.18.3. Update to these versions or a later version.

References

- **Vendor Advisory**
- **CVE-2023-46604**

F5 BIG-IP Unauthenticated Remote Code Execution via AJP Smuggling CRITICAL 9.8

CVE-2023-46747

Affected Hosts

- 10.2.4.98
- 10.0.4.7
- 10.0.40.80 (f5.smoke.net)

Mitigations

- Follow the instructions referenced in the vendor advisory. There is a provided script to patch the vulnerability. Additionally, restrict access to the Traffic Management User Interface (TMUI) portal entirely on the public internet.

References

- **CVE-2023-46747**
- **Vendor Advisory**

Fortinet FortiClient EMS SQL Injection Vulnerability

CRITICAL 9.8

CVE-2023-48788

Affected Hosts

- 10.0.40.71
- 10.0.40.63

Mitigations

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

References

- **Fortinet Security Advisory**
- **Horizon3.ai Technical Deep Dive on CVE-2023-48788**
- **CVE-2023-48788**

Unauthenticated Kubelet API Remote Code Execution Vulnerability

CRITICAL 9.8

H3-2021-0005

Affected Hosts

- 10.2.13.29
- 10.2.4.10

Mitigations

- Disable --enable-debugging-handlers kubelet flag to prevent exposing the /run, /exec, /portForward, and /attach endpoints.
- Ensure kubelet is protected using --anonymous-auth=false kubelet flag.
- Allow only legitimate users using --client-ca-file or --authentication-token-webhook kubelet flags.

References

- **Kubelet options**
- **CIS Benchmarks: Securing Kubernetes**

Weak or Default Credentials - Web Applications

CRITICAL 9.8

H3-2021-0021

Affected Hosts

- 10.0.229.4 (ex2.smoke.net)
- 10.2.51.108
- 10.0.40.1 (pfsense.smoke.net)
- 10.2.51.102
- 10.2.51.108
- 10.0.40.102 (airflow-target.smoke.net)
- 10.0.4.23 (obwa.pod04.example.internal)
- 10.2.51.105
- 10.0.4.23 (obwa.pod04.example.internal)
- 10.2.51.105
- 10.2.51.101
- 10.0.40.19 (www.app-a.com)
- 10.0.4.23 (obwa.pod04.example.internal)
- 10.0.4.31 (openmediavault.pod04.example.internal)
- 10.0.229.4 (ex2.smoke.net)
- 10.2.51.101

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**
- **T1110: Brute Force**

AWS Instance Metadata Service v1 Exposed

CRITICAL 9.8

H3-2021-0040

Affected Hosts

- 10.2.4.132 (coldfusion18.pod04.example.internal)
- 10.2.13.132 (docker.pod13.example.internal)
- 3.19.142.123

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**

JBoss Application Server HTTP Invoker Remote Code Execution Vulnerability

CRITICAL 9.8

H3-2021-0047

Affected Host

- 10.2.51.105

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**
- **CISA Analysis Report (AR18-312A): JexBoss – JBoss Verify and EXploitation Tool**
- **FoxGlove Security: What Do WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and Your Application Have in Common?**
- **SAS Guidance: Removing the JMX Console and the EJBInvokerServlet and JMXInvokerServlet applications from the JBoss application server**
- **IBM: JBoss Security Remediation Guidance**

Azure Multi-Factor Authentication Disabled

CRITICAL 9.8

H3-2022-0002

Affected Assets

- Microsoft Entra User sync_az01_97d10b16b452
- Microsoft Entra User xhh0p6mzrs
- Microsoft Entra User a-jsmith
- Microsoft Entra User jsmith
- Microsoft Entra User xhh0p6mzrs
- Microsoft Entra User jsmith
- Microsoft Entra User jsmith
- Entra Global Admin nodezero_92250
- Microsoft Entra User a-jsmith
- Entra Global Admin a-jsmith
- Microsoft Entra User xhh0p6mzrs
- Microsoft Entra User xhh0p6mzrs

Mitigations

- Enable multi-factor authentication for all users to access Azure resources.

References

- **How to Enable Multi-Factor Authentication in Azure**

AWS Assume Role Access

CRITICAL 9.8

H3-2022-0074

Affected Assets

- AWS Role read-role
- AWS Role list-role
- AWS Role write-role
- AWS Role assuming-role
- AWS Role audit
- AWS Role hard-to-guess-305199

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**

PaperCut File Upload Remote Code Execution Vulnerability

CRITICAL 9.8

H3-2023-0020

Affected Hosts

- 10.0.229.11 (fs.smoke.net)
- 10.0.229.11 (fs.smoke.net)

Mitigations

- Update to PaperCut NG/MF version 22.1.3 or later.
- Configure an allowlist of device IP addresses that can communicate with the PaperCut server.

References

- **PaperCut NG/MF Security Bulletin (July 2023)**
- **Horizon3.ai Research Advisory**
- **Horizon3.ai Technical Deep Dive**
- **CVE-2023-39143**
- **PaperCut NG Release History**
- **PaperCut Common Security Questions**
- **Securing your PaperCut NG/MF Server**

Weak NFS Export Permissions

CRITICAL 9.5

H3-2020-0009

Affected Hosts

- 10.0.4.4 (svr01.pod04.example.internal)
- 10.0.40.53 (sambacry)
- 10.0.220.200 (coldfusion18.smoke.net)

Table of Contents

- **Option 1: Disable the NFS Service**
- **Option 2: Restrict Access to the NFS Service**

Option 1: Disable the NFS Service

Debian/Ubuntu

- From within a terminal:

```
sudo service nfs-kernel-server stop
sudo apt-get --purge remove nfs-kernel-server nfs-common portmap
```

CentOS 6/RHEL 6

- From within a terminal:

```
chkconfig rpcgssd off
chkconfig rpcidmapd off
chkconfig portmap off
chkconfig nfs off
yum remove portmap nfs-utils
```

CentOS 7+/RHEL 7+

- From within a terminal:

```
systemctl disable nfs-lock
systemctl stop nfs
systemctl disable nfs
yum remove nfs-utils portmap
```

Option 2: Restrict Access to the NFS service

Different systems allow restriction of which clients can connect to the NFS service.

- On Linux systems, the /etc/exports file can be configured to whitelist clients that access the NFS service:

```
[root@server ~]# cat /etc/exports/root/nfs
192.168.0.100(rw,async)
```

NOTE: On other systems, the solution may be to implement firewall rules to disallow access to the service from untrusted clients.

Mitigations

- Implement appropriate controls to restrict access to authorized systems only.
- Review the permissions of the exported NFS share to confirm secure best practices are being used.

References

- **CWE-284: Improper Access Control**
- **Security and NFS**

VMware vCenter Server-Side Request Forgery Vulnerability

CRITICAL 9.5

CVE-2021-21973

Affected Hosts

- 10.0.4.29 (vcsa.pod04.example.internal)
- 10.0.40.99 (vcsa.smoke.net)

Mitigations

- Upgrade to VMWare vCenter 7.0 U1cv, 6.7 U3l, or 6.5 U3n or greater. If the server is Cloud Foundation Server then upgrade to 4.2 or 3.10.1.2 or greater.

References

- **CVE-2021-21973**
- **Vendor Advisory**

Microsoft Exchange Remote Code Execution Vulnerability

CRITICAL 9.5

CVE-2021-26855

Affected Host

- 10.0.4.3 (ex01.pod04.example.internal)

Mitigations

- This vulnerability is part of an attack chain with three other vulnerabilities which lead to Remote Code Execution. Apply all updates and patch to the latest vendor-supported version.

References

- **CVE-2021-26855**
- **Microsoft Security Advisory for CVE-2021-26855**
- **March 2021 Microsoft Exchange Security Updates**

Citrix Bleed - Leaking Session Tokens

CRITICAL 9.5

CVE-2023-4966

Affected Host

- 10.0.40.218

Mitigations

- Citrix customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible.

References

- **CVE-2023-4966**
- **Vendor Advisory**
- **Technical blogpost from Assetnote**

Jenkins Arbitrary File Leak Vulnerability

CRITICAL 9.5

CVE-2024-23897

Affected Hosts

- 10.0.229.3 (ex.smoke.net)
- 10.0.229.4 (ex2.smoke.net)
- 10.0.40.82
- 10.0.40.102 (airflow-target.smoke.net)

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**
- **Jenkins Patch Workaround**
- **SonarSource Researcher Writeup**
- **Horizon3: Assessing the Impact of the Jenkins Arbitrary File Leak Vulnerability**
- **CVE-2024-23897**

Unauthenticated Access to Sensitive Kubelet API Endpoints

CRITICAL 9.5

H3-2021-0003

Affected Hosts

- 10.2.4.10
- 10.2.13.29

Mitigations

- Unless otherwise required, disable the read-only port entirely by using --read-only-port=0 kubelet flags.
- Unless otherwise required, ensure kubelet is protected using --anonymous-auth=false kubelet flag.
- If possible, allow only legitimate users using --client-ca-file or --authentication-token-webhook kubelet flags.
- Unless otherwise required, disable --enable-debugging-handlers kubelet flag to prevent leaking logs, pod, health and command line flag information.

References

- **Kubelet Authentication/Authorization**
- **CIS Benchmarks: Securing Kubernetes**

Unauthenticated Kubernetes API Server Access

CRITICAL 9.5

H3-2021-0006

Affected Hosts

- 10.2.4.12
- 10.2.4.10
- 10.2.13.29
- 10.2.13.31

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**
- **Using RBAC Authorization**
- **CIS Benchmarks: Securing Kubernetes**

Weak or Default Credentials - SSH

CRITICAL 9.5

H3-2021-0014

Affected Hosts

- 10.0.4.31 (openmediavault.pod04.example.internal)
- 10.0.4.24 (irc.testirc.net)
- 10.0.229.4 (ex2.smoke.net)
- 10.0.40.83
- 10.0.40.121
- 10.0.40.18
- 10.0.40.114
- 10.0.40.17 (cacti.example.com)
- 10.0.220.200 (coldfusion18.smoke.net)
- 10.0.40.134
- 10.2.51.106
- 10.0.40.92
- 10.0.40.170
- 10.0.40.54
- 10.0.40.88
- 10.0.40.6
- 10.0.40.19 (www.app-a.com)
- 10.0.100.102
- 10.2.51.108
- 10.0.40.74

Table of Contents

- **Option 1: Implement a Strong Password Policy**
- **Option 2: Implement a Configuration Management Policy**

Option 1: Implement a Strong Password Policy

Change the credential's password and ensure a strong password policy is in place and users are properly trained on best practices. The National Institute of Standards and Technology (NIST) commonly releases guidance on password best practices which include:

- A minimum length of 8 characters
- Blacklisting passwords that contain dictionary words, repetitive or sequential characters, and the company name
- Implement Multi-Factor Authentication when available

NOTE: See full NIST publication here **NIST 800-63-3**

Option 2: Implement a Configuration Management Process

Often, systems and applications will be installed without the default credentials being changed. Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.

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**
- **T1110: Brute Force**

Apache Solr Arbitrary File Read Vulnerability

CRITICAL 9.4

H3-2023-0023

Affected Hosts

- 10.2.51.108
- 10.2.51.107

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**
- **Apache Solr Security Advisory**
- **Apache Solr Arbitrary File Read and SSRF Vulnerability Threat Alert**
- **Apache Solr Security News**

Weak or Default Credentials - Microsoft SQL Server

CRITICAL 9.4

H3-2021-0016

Affected Host

- 10.2.51.101

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**
- **T1110: Brute Force**

Apache Solr DataImportHandler Remote Code Execution Vulnerability

CRITICAL 9.2

CVE-2019-0193

Affected Host

- 10.2.51.108

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**
- **CVE-2019-0193**

Drupal Core Remote Code Execution Vulnerability

CRITICAL 9.2

CVE-2019-6340

Affected Host

- 10.2.51.103

Mitigations

- If you are using Drupal 8.6.x, upgrade to Drupal 8.6.10
- If you are using Drupal 8.5.x or earlier, upgrade to Drupal 8.5.11

References

- **Drupal core - Highly critical - Remote Code Execution - SA-CORE-2019-003**
- **Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution**
- **CVE-2019-6340**

Microsoft Windows Machine Account NTLM Coercion via LSARPC Spoofing Vulnerability

CRITICAL 9.2

CVE-2021-36942

Affected Hosts

- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)

Mitigations

- Apply all updates and patch to the latest vendor-supported version. Specifically, install Microsoft patches KB5005106 (CVE-2021-3692) and KB5013952 (CVE-2022-26925)

References

- **CERT/CC Vulnerability Note**
- **CVE-2021-36942: Microsoft Windows LSA Spoofing Vulnerability Advisory**
- **CVE-2022-26925: Microsoft Windows LSA Spoofing Vulnerability Advisory**
- **CVE-2021-36942**
- **CVE-2022-26925**
- **PetitPotam**
- **August 10, 2021-KB5005106 (Security-only update)**
- **Microsoft May 10, 2022-KB5013952 (OS Build 14393.5125)**

PolKit PkExec Local Privilege Escalation Vulnerability

CRITICAL 9.2

CVE-2021-4034

Affected Hosts

- 10.0.40.83
- 10.0.4.24 (irc.testirc.net)
- 10.0.40.80 (f5.smoke.net)

Mitigations

- Update the PolKit version to the latest supported version. Follow guidance specific to the host's Linux distribution.

References

- **CVE-2021-4034**
- **RedHat CVE-2021-4034 Update Guidance**
- **Debian CVE-2021-4034 Update Guidance**
- **Ubuntu CVE-2021-4034 Update Guidance**
- **Qualys CVE-2021-4034 Vulnerability Details**

Anonymous FTP Enabled

CRITICAL 9.2

H3-2020-0005

Affected Hosts

- 10.2.51.107
- 10.0.229.4 (ex2.smoke.net)
- 10.0.4.4 (svr01.pod04.example.internal)
- 10.0.40.72
- 10.0.40.72

Mitigations

- Disable anonymous login or disable the FTP service if not needed.

References

- **CWE-284: Improper Access Control**

IPMI Cipher Zero Vulnerability

CRITICAL 9.2

H3-2020-0017

Affected Host

- 10.0.100.102

Mitigations

- Disable the IPMI service if not needed.
- Disable cipher suite zero authentication method.
- If IPMI service is required and unable to disable cipher suite zero authentication, implement access controls to limit access via whitelisted addresses.

References

- **CWE-287: Improper Authentication**
- **CVE-2013-4782**
- **CVE-2013-4783**
- **CVE-2013-4784**
- **CVE-2013-4785**

FTP Directory Traversal Vulnerability

CRITICAL 9.2

H3-2020-0028

Affected Host

- 10.2.51.107

Mitigations

- Apply the updates referenced by the vendor of the product.
- If possible, use chrooted jails to run the software if no patch is available. This will help restrict where the files can be obtained and not leak sensitive data from the host
- Implement access control lists to limit access to specific hosts that need access to the resource

References

- **CWE Path Traversal**

Weak or Default Credentials - FTP

CRITICAL 9.2

H3-2021-0012

Affected Hosts

- 10.2.51.107
- 10.0.229.4 (ex2.smoke.net)
- 10.0.229.4 (ex2.smoke.net)
- 10.0.229.4 (ex2.smoke.net)
- 10.0.229.4 (ex2.smoke.net)
- 10.0.40.74
- 10.0.40.72
- 10.2.51.107
- 10.0.40.72
- 10.0.4.4 (svr01.pod04.example.internal)
- 10.0.40.72
- 10.0.40.72
- 10.2.51.107
- 10.0.4.4 (svr01.pod04.example.internal)

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**
- **T1110: Brute Force**

Weak or Default Credentials - Telnet

CRITICAL 9.2

H3-2021-0013

Affected Hosts

- 10.0.40.74
- 10.2.51.101

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**
- **T1110: Brute Force**

Unrestricted Sudo Privileges

CRITICAL 9.2

H3-2021-0039

Affected Hosts

- 10.0.229.4 (ex2.smoke.net)
- 10.0.40.6
- 10.0.40.170
- 10.2.51.106
- 10.0.40.18
- 10.0.40.134
- 10.0.40.114
- 10.0.40.88
- 10.0.40.17 (cacti.example.com)
- 10.0.40.92
- 10.0.40.19 (www.app-a.com)
- 10.0.40.121
- 10.0.40.54
- 10.0.4.24 (irc.testirc.net)
- 10.0.220.200 (coldfusion18.smoke.net)

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**

Credential Dumping - /etc/shadow File

CRITICAL 9.2

H3-2021-0045

Affected Hosts

- 10.0.40.83
- 10.0.4.24 (irc.testirc.net)
- 10.0.229.4 (ex2.smoke.net)
- 10.0.40.80 (f5.smoke.net)
- 10.2.4.98
- 10.0.220.200 (coldfusion18.smoke.net)
- 10.0.40.17 (cacti.example.com)
- 10.0.40.134
- 10.2.51.102
- 10.0.4.7
- 10.0.4.31 (openmediavault.pod04.example.internal)
- 10.0.40.170
- 10.0.40.19 (www.app-a.com)
- 10.2.51.106
- 10.0.40.114
- 10.0.40.121
- 10.0.40.18
- 10.0.40.53 (sambacry)

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**
- **Red Hat: How to monitor permission, ownership or any other change to a particular directory or file**

Active Directory Certificate Services Misconfiguration: NTLM Relay to AD CS HTTP Endpoint

CRITICAL 9.2

H3-2022-0024

Affected Hosts

- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)

Mitigations

- Harden AD HTTP Endpoints. Remove AD CS HTTP endpoints if they are not required. See 'Certified Pre-Owned: Abusing Active Directory Certificate Services, Harden AD CS HTTP Endpoints - PREVENT8'
- Disable NTLM Authentication at the host Level. On AD CS servers, configure GPOs to set Computer Configuration Windows Settings -> Security Settings -> Local Policies -> Security Options ->“Network security: Restrict NTLM: Incoming NTLM traffic” to “Deny All Accounts” and add exceptions as necessary using the setting “Network security: Restrict NTLM: Add server exceptions in this domain.” The other “Restrict NTLM settings” value can also be enabled to better audit NTLM usage in an environment. See 'Certified Pre-Owned: Harden AD CS HTTP Endpoints - PREVENT8' for additional details.
- Disable NTLM Authentication at the IIS level. Disable authentication providers for each IIS application associated with an AD CS HTTP endpoint. See 'Certified Pre-Owned: Harden AD CS HTTP Endpoints - PREVENT8' for additional details.
- If disabling NTLM is infeasible, enforce HTTPS and enable Extended Protection for Authentication. See Microsoft Security Response Center reference.

References

- **Certified Pre-Owned: Abusing Active Directory Certificate Services, Harden AD CS HTTP Endpoints - PREVENT8**
- **SpectreOps - Certified Pre-Owned**
- **Microsoft Security Response Center - Extended Protection for Authentication.**

Microsoft Windows Machine Account NTLM Coercion via Authenticated LSARPC Spoofing

CRITICAL 9.2

H3-2022-0073

Affected Hosts

- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)

Block remote EFSRPC functionality with RPC Filters

If Microsoft Encrypted File System Remote Protocol (MS-EFSRPC) is not required, administrators should block the remote EFSRPC functionality on the vulnerable host using RPC filters.

1. Create a text file with the following content:

```
rpc

filter

add rule layer=um actiontype=block

add condition field=if_uuid matchtype=equal data=c681d488-d850-11d0-8c52-00c04fd90f7e

add filter

add rule layer=um actiontype=block

add condition field=if_uuid matchtype=equal data=df1941c5-fe89-4e79-bf10-463657acf44d

add filter

quit
```

2. Use the netsh command line utility to import the RPC filter from an elevated administrator prompt:

```
netsh -f <FILTER_FILE_NAME>
```

3. To confirm the filters are in place, you can view the current RPC filters using the following command:

```
netsh rpc filter show filter
```

See **CERT Coordination Center Vulnerability Note VU:#405600** for additional details.

Mitigations

- If not required, administrators should block the remote EFSRPC functionality on the vulnerable host using RPC filters. See CERT Coordination Center Vulnerability Note VU:#405600 for details.

References

- **CERT Coordination Center Vulnerability Note VU:#405600 -- Microsoft Windows Active Directory Certificate Services can allow for AD compromise via PetitPotam NTLM relay attacks**
- **[MS-EFSR]: Encrypting File System Remote (EFSRPC) Protocol**

Authenticated Microsoft Windows Machine Account NTLM Coercion via Distributed File System Namespace Management Protocol Manipulation

CRITICAL 9.2

H3-2023-0014

Affected Hosts

- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)

Mitigations

- If not required, administrators should block the remote MS-DFSNM functionality on the vulnerable host using RPC filters. This can be done by blocking the RPC interface UUIDs for MS-DFSNM.
- Enable Extended Protection for Authentication (EPA), disable HTTP on servers running Active Directory Certificate Services (AD CS), disable NTLM authentication on where possible, and enforce SMB signing to mitigate NTLM relay attacks that could result from hosts vulnerable to MS-DFSNM coercion.

References

- **[MS-DFSNM]: Distributed File System (DFS): Namespace Management Protocol**
- **MS-DFSNM Abuse (DFSCoerce)**

NFS UID/GID Manipulation Possible

CRITICAL 9

H3-2020-0010

Affected Host

- 10.0.220.200 (coldfusion18.smoke.net)

Mitigations

- Implement the use of NFSv4 over older versions such as NFSv2 or NFSv3 to take advantage of Kerberos authentication.
- Avoid using options such as 'no_root_squash' if not needed. Furthermore, restrict share access to only authorized hosts.

References

- **CWE-284: Improper Access Control**
- **Security and NFS**

Zoho ManageEngine ServiceDesk Plus Unauthenticated Remote Code Execution Vulnerability

CRITICAL 9

CVE-2021-44077

Affected Host

- 10.0.4.22 (zoho.pod04.example.internal)

Mitigations

- Update to ServiceDesk Plus build 11306 or higher.

References

- **Vendor Advisory**
- **CISA Alert (AA21-336A)**
- **Horizon3.ai Proof of Concept**
- **CVE-2021-44077**

Group Policy Preferences Password Elevation of Privilege Vulnerability

HIGH 8.8

CVE-2014-1812

Affected Hosts

- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- 10.0.4.130 (win10.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- 10.0.220.53 (win10.smoke.net)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- 10.0.4.130 (win10.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- 10.0.229.11 (fs.smoke.net)
- 10.0.4.130 (win10.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- 10.0.4.130 (win10.pod04.example.internal)
- 10.0.220.53 (win10.smoke.net)
- 10.0.229.6 (app4.smoke.net)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)

Table of Contents:

- **Option 1: Patch the Host**
- **Option 2: Remove Old or Unused Policies**

Option 1: Patch the Host

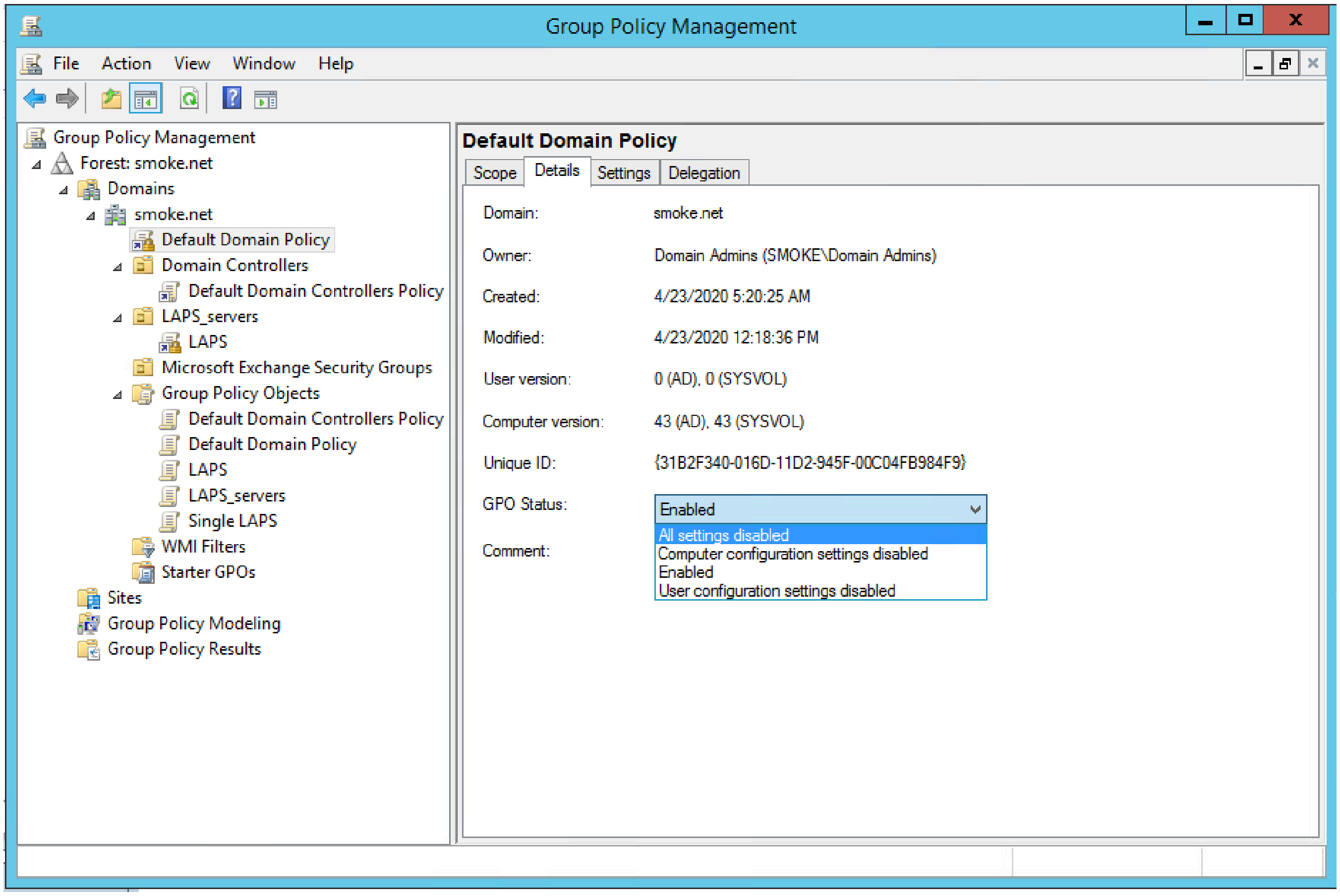
Microsoft released a patch, KB2928120, addressing this vulnerability. To install it, download the patch from the **MS14-025 Security Bulletin** for the corresponding host operating system.

Option 2: Remove Old or Unused Policies

Even if the correct patch has been applied, old policies that contained passwords will still need to be removed. To remove the policies identified in the weakness:

1. In Group Policy Management console, open the policy that contains CPassword data.

2. Change the action to **Delete** or **Disable**, as applicable to the preference.



Default Domain Policy

Domain: smoke.net

Owner: Domain Admins (SMOKE\Domain Admins)

Created: 4/23/2020 5:20:25 AM

Modified: 4/23/2020 12:18:36 PM

User version: 0 (AD), 0 (SYSVOL)

Computer version: 43 (AD), 43 (SYSVOL)

Unique ID: {31B2F340-016D-11D2-945F-00C04FB984F9}

GPO Status: Enabled

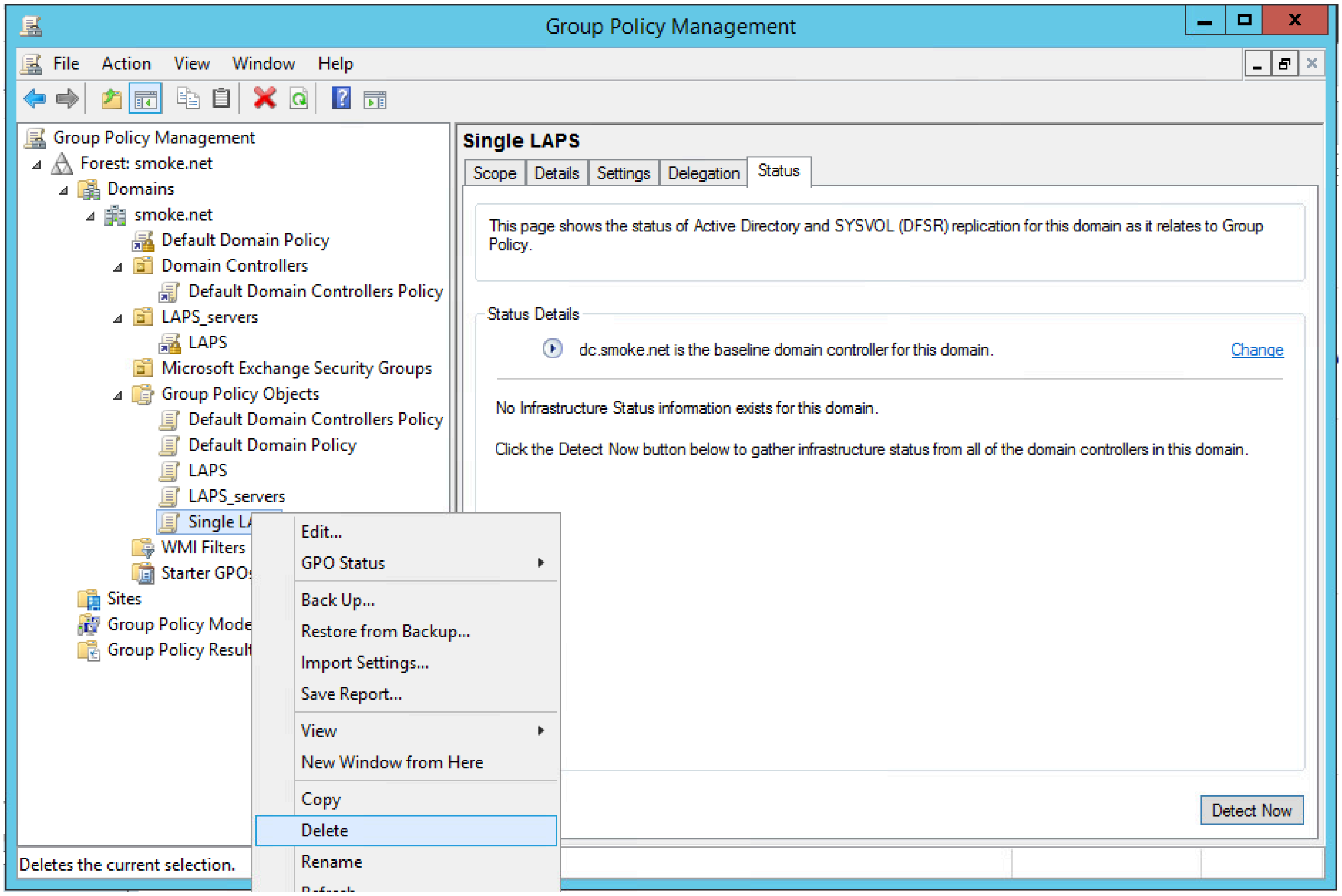
- All settings disabled
- Computer configuration settings disabled
- Enabled
- User configuration settings disabled

Comment:

3. Click **OK** to save your changes.

4. Wait for one or two Group Policy refresh cycles to allow changes to propagate to clients.

5. After changes are applied on all clients, delete the preference.



This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.

dc.smoke.net is the baseline domain controller for this domain.

No Infrastructure Status information exists for this domain.

Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.

Deletes the current selection.

6. Repeat steps 1 through 5 as needed to clean your whole environment. When the detection script returns zero results, you are finished.

References:

- **Vulnerability in Group Policy Preferences Could Allow Privilege Escalation**

Mitigations

- Apply the updates referenced in Microsoft Security Bulletin MS14-025 below.
- Those that had existing group policies that used the Group Policy preferences before this patch was applied will need to take additional action to remove those policies. Follow the steps outlined in the "Removing CPassword preferences" at the very bottom of the Knowledge Base article linked below.

References

- **CVE-2014-1812**
- **Microsoft Security Bulletin MS14-025**
- **Knowledge Base Article 2962486**

Weak or Default Credentials - MySQL

HIGH 8.6

H3-2021-0017

Affected Host

- 10.2.51.101

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**
- **T1110: Brute Force**

Weak or Default Credentials - Postgres

HIGH 8.6

H3-2021-0018

Affected Assets

- Service User postgres
- Service User postgres

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**
- **T1110: Brute Force**

Weak or Default Credentials - MongoDB

HIGH 8.6

H3-2022-0067

Affected Hosts

- 10.2.51.101
- 10.2.51.101

Mitigations

- Ensure a strong password policy is in place that requires long, random, and unique passwords for service accounts that access the MongoDB database.
- Ensure a least-privilege policy is implemented for service accounts that access the MongoDB database to minimize the impact of a compromised account.
- Consider use of Kerberos, LDAP, or certificate-based authentication as a stronger alternative to password-based authentication.
- Identify a configuration management process that ensures authentication and access control are enabled and default credentials are changed before MongoDB servers are deployed in a production environment.

References

- **CWE-521: Weak Password Requirements**
- **CWE-309: Use of Password System for Primary Authentication**
- **T1110: Brute Force**
- **Security Checklist — MongoDB Manual**

Anonymous MongoDB Access

HIGH 8.6

H3-2022-0070

Affected Hosts

- 10.0.40.114
- 10.2.51.101

Mitigations

- Identify a configuration management process that ensures authentication and access control are enabled before MongoDB servers are deployed in a production environment.

References

- **CWE-284: Improper Access Control**
- **Enable Access Control - MongoDB Manual**
- **Security Checklist — MongoDB Manual**

HTTP.sys Denial of Service and Remote Code Execution Vulnerability

HIGH 8.1

CVE-2015-1635

Affected Hosts

- Domain Controller 10.0.229.1 (dc.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)

Mitigations

- Apply the patches as described in the Microsoft advisory.

References

- **Vendor Advisory**
- **CVE-2015-1635**

Weak or Default Credentials - Cracked Credentials from Active Directory Services Database (NTDS)

HIGH 8

H3-2022-0093

Affected Hosts

- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)

Mitigations

- Ensure a strong password policy is in place in accordance with the latest NIST guidance. In particular, ensure users aren't setting passwords that are known to have been part of prior breaches or are easily guessed based on contextual terms such as your company's name. Consider removing any policy requirements for password complexity and password rotation, as these requirements have been shown to result in users setting predictable passwords.
- Configure your password policy to set a high minimum password length of 12 characters or more.
- Reset the passwords for any accounts whose password hashes were cracked, especially for highly privileged accounts and easily guessable passwords. Easily guessable passwords are ones marked as being among the top 10000 known bad passwords, or ones that were cracked with the following methods: Empty password, Based on username, Credential stuffing, Credential tweaking, Based on contextual term, and Based off common breach term for your company.
- Deactivate any accounts that are no longer needed.
- Consider the use of a password manager to store complex, unique passwords where possible.

References

- **NIST Special Publication 800-63B: Digital Identity Guidelines**

Password Reuse Found in Active Directory Services Database (NTDS)

HIGH 8

H3-2022-0095

Affected Hosts

- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)

Mitigations

- Reset the passwords for any accounts found to be sharing passwords, especially for highly privileged accounts.
- Deactivate any accounts that are no longer needed.
- Consider the use of a password manager to store complex, unique passwords where possible.

References

- **NIST Password Guidelines**

Active Directory User has Entra Administrator Role

HIGH 8

H3-2024-0029

Affected Asset

- Domain Admin a-jsmith

Mitigations

- Avoid using on-premises synced accounts for Microsoft Entra role assignments. Use separate and unique Entra ID administrator accounts that do not synchronize with on-premises Domains using Entra Connect.
- Utilize a Least Privilege security policy and limit the administrative access provided to users. Entra has several built in administrator roles - choose the one that best fits the privileges a given administrator account requires.
- Limit the number of Global Administrators to less than 5. Limit the number of total privileged role assignments to less than 10.

References

- **Microsoft - Best Practices for Microsoft Entra Roles**

Remote Desktop Services Remote Code Execution Vulnerability

HIGH 7.8

CVE-2019-0708

Affected Host

- 10.0.220.54 (winxp.smoke.net)

Table of Contents

- **Option 1: Patch the Host**
- **Option 2: Enable NLA on the Host**

Option 1: Patch the Host

Microsoft released patches, KB4493471 and KB4493472, addressing this vulnerability. Install one of the patches from the Microsoft Update Catalog for the corresponding host operating system. See Microsoft's update guide **here**

Option 2: Enable NLA on the Host

Enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2

You can enable Network Level Authentication to block unauthenticated attackers from exploiting this vulnerability. With NLA turned on, an attacker would first need to authenticate to Remote Desktop Services using a valid account on the target system before attempting to exploit the vulnerability.

Steps to Enable NLA:

- On the vulnerable host, from the Start Menu, access Control Panel > System and Security > System > Remote settings > Remote tab > Remote Desktop
- Check these options:
  - `Allow remote connections to this computer`
  - `Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)`

Mitigations

- Apply the patches released on May 19, 2019 by Microsoft.
- Disable remote desktop services if not required. Enable Network Level Authentication (NLA).

References

- **CVE-2019-0708**
- **Microsoft Updates: CVE-2019-0708**
- **Customer guidance for CVE-2019-0708**

SaltStack Authorization Bypass Vulnerability

HIGH 7.8

CVE-2021-25281

Affected Hosts

- 10.0.220.50
- 10.0.220.50

Mitigations

- Update to SaltStack version 3002.5, 3001.6, 3000.8 or later.

References

- **SaltStack Security Advisory**
- **CVE-2021-25281**

Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability

HIGH 7.8

CVE-2021-40539

Affected Host

- 10.0.4.22 (zoho.pod04.example.internal)

Mitigations

- ADSelfService Plus builds up to 6113 are affected. Update to build 6114 or later, as described in the Vendor Advisory.

References

- **ManageEngine Advisory**
- **CVE-2021-40539**

OpenSSL Heartbleed Vulnerability

HIGH 7.5

CVE-2014-0160

Affected Host

- 10.2.51.101

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**
- **Heartbleed**
- **FOX-IT Blog Writeup**

Apache JServ Protocol (AJP) Vulnerability

HIGH 7.5

CVE-2020-1938

Affected Hosts

- 10.0.40.102 (airflow-target.smoke.net)
- 10.2.51.102

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**

Grafana Directory Traversal Vulnerability

HIGH 7.5

CVE-2021-43798

Affected Host

- 10.2.51.105

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**
- **CVE-2021-43798**

Adobe ColdFusion Improper Access Control Vulnerability

HIGH 7.5

CVE-2023-29298

Affected Host

- 10.0.40.170

Mitigations

- Upgrade to ColdFusion 2018 Update 17, ColdFusion 2021 Update 7, or ColdFusion 2023 Update 1 or later.

References

- **CVE-2023-29298**
- **Vendor Advisory**

Adobe ColdFusion Improper Access Control Vulnerability - Patch Bypass

HIGH 7.5

CVE-2023-38205

Affected Host

- 10.0.40.170

Mitigations

- Upgrade affected servers to ColdFusion 2023 Update 3, ColdFusion 2021 Update 9, or ColdFusion 2018 Update 19 or later and apply all technical mitigation solutions.

References

- **CVE-2023-38205**
- **Writeup On Vulnerability**
- **Vendor Advisory**
- **Adobe ColdFusion 2023 Mitigations**
- **Adobe ColdFusion 2021 Mitigations**
- **Adobe ColdFusion 2019 Mitigations**

Gradio Windows Credentials Leak Vulnerability

HIGH 7.5

CVE-2024-34510

Affected Hosts

- 10.0.220.6 (app2.smoke.net)
- 10.0.220.53 (win10.smoke.net)

Mitigations

- Upgrade to Gradio 4.20 or later.

References

- **Gradio Changelog**
- **CVE-2024-34510**

Insecure IPMI Implementation

HIGH 7.5

H3-2020-0016

Affected Host

- 10.0.100.102

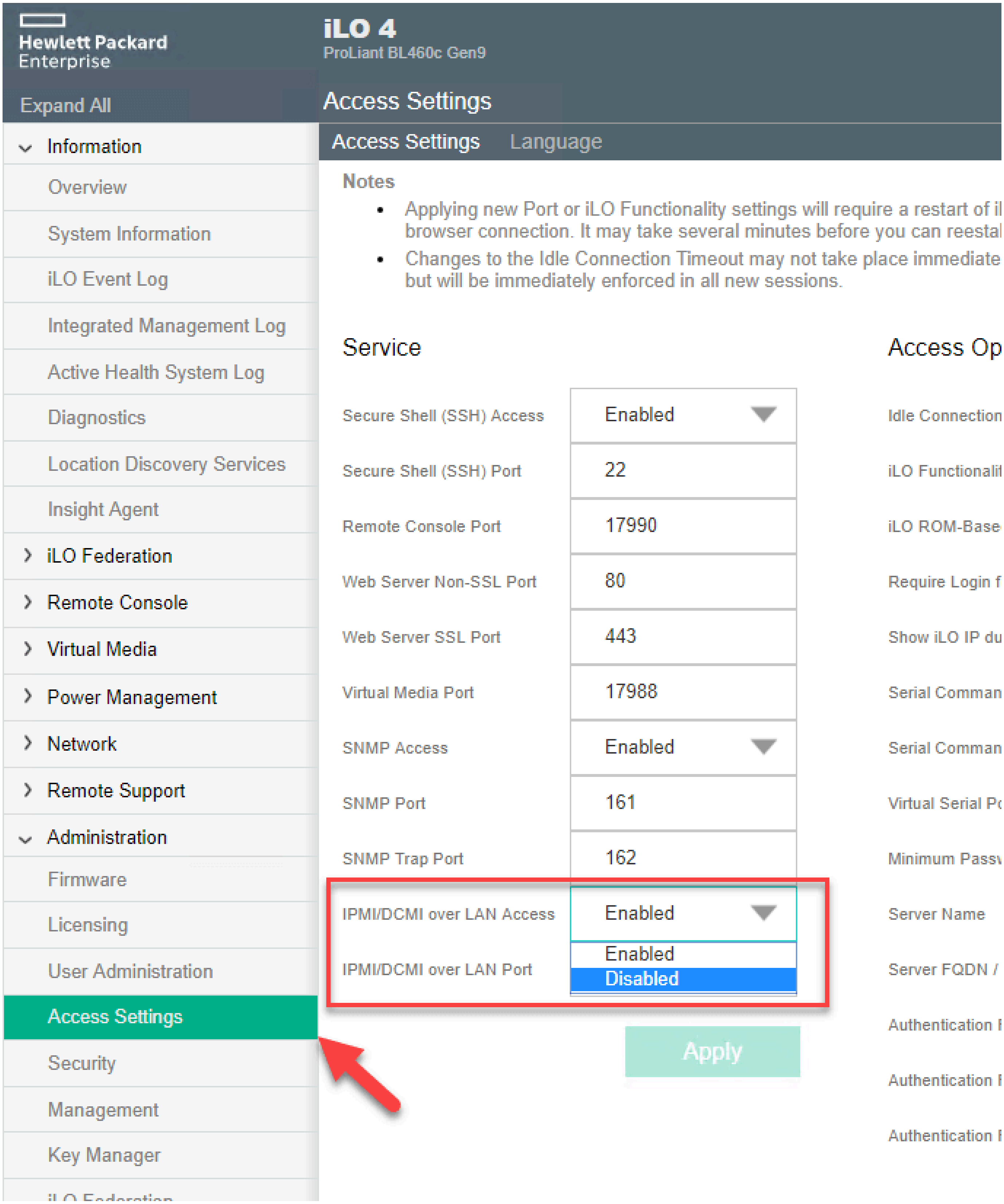
Table of Contents

- **Option 1: Disable the IPMI Service**
- **Option 2: Implement a Strong Password**
- **Option 3: Implement a Strong Password Policy**
- **Option 4: Implement a Configuration Management Policy**

This weakness is the result of a flaw in the protocol design. As a result, there is not a software patch or fix action that can completely remove the weakness without disabling the service (option 1). However, the weakness can be mitigated using options 2-4. These options do NOT prevent an attacker from obtaining password hashes, but can increase the complexity of offline password cracking attacks. These fix actions may reduce the likelihood of an attacker obtaining a cleartext password, but **NodeZero will continue to report the weakness**.

Option 1: Disable the IPMI Service

The IPMI service settings can typically be managed via the web page in the Administration section. Specifically, on the HP iLO, navigate to the Administration->Access Settings page and set the “IPMI over LAN Access” to “Disabled”.



iLO 4
ProLiant BL460c Gen9

Access Settings

Notes

- Applying new Port or iLO Functionality settings will require a restart of il browser connection. It may take several minutes before you can reestal
- Changes to the Idle Connection Timeout may not take place immediate but will be immediately enforced in all new sessions.

Service

Secure Shell (SSH) Access	Enabled
Secure Shell (SSH) Port	22
Remote Console Port	17990
Web Server Non-SSL Port	80
Web Server SSL Port	443
Virtual Media Port	17988
SNMP Access	Enabled
SNMP Port	161
SNMP Trap Port	162
IPMI/DCMI over LAN Access	Enabled Enabled Disabled
IPMI/DCMI over LAN Port	

Option 2: Implement a Strong Password

If disabling the service is not an option, updating the password to be much stronger will prevent attackers from cracking the hash obtainable from this vulnerability. Change the credential's password and consider implementing additionally security policies. Typically to update passwords on these systems, log in via the web page, access the account settings, and update the password.

Option 3: Implement a Strong Password Policy

Ensure a strong password policy is in place and users are properly trained on best practices. The National Institute of Standards and Technology (NIST) commonly releases guidance on password best practices which include:

- A minimum length of 8 characters
- Blacklisting passwords that contain dictionary words, repetitive or sequential characters, and the company name
- Implement Multi-Factor Authentication when available
- For more detail see **NIST 800-63-3**

Option 4: Implement a Configuration Management Policy

Often, systems and applications will be installed without the default credentials being changed. Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.

Mitigations

- Disable the IPMI service if not needed. If required, implement access controls to limit access via whitelisted addresses.

References

- **CWE-287: Improper Authentication**
- **CVE-2013-4786**

Kerberos Pre-Authentication Disabled

HIGH 7.5

H3-2021-0011

Affected Assets

- Kerberos AS-REP Hash for nsunkavally
- Kerberos AS-REP Hash for nsunkavally

Mitigations

- Re-enable Kerberos pre-authentication for the user. Find the User within Active Directory, and under the Account tab within the Account options uncheck 'Do not require Kerberos preauthentication'.

References

- **Kerberos Pre-Authentication: Why It Should Not Be Disabled**
- **AS-REP Toasting Attack Example**

Public Access to Git Repository

HIGH 7.5

H3-2021-0031

Affected Asset

- Git Repo fakegit

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**
- **Security Best Practices for Git Users**
- **10 GitHub Security Best Practices**
- **Removing sensitive data from a repository**

Credential Reuse

HIGH 7.5

H3-2021-0032

Affected Hosts

- 10.0.220.6 (app2.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.0.220.52 (win7.smoke.net)
- 10.0.40.72

Mitigations

- Update the password to be unique and ensure it follows current password guidelines.

References

- **NIST Password Guidelines**

Active Directory Certificate Services Misconfigured Template Requires Enrollment Agent Signature

HIGH 7.5

H3-2022-0019

Affected Hosts

- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)

Mitigations

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

References

- **Certified Pre-Owned: Abusing Active Directory Certificate Services**
- **SpectreOps - Certified Pre-Owned**

Shell History File Exposure

HIGH 7.5

H3-2022-0044

Affected Hosts

- 10.0.4.23 (obwa.pod04.example.internal)
- 10.0.4.23 (obwa.pod04.example.internal)

Mitigations

- Check your DocumentRoot regularly to see if any of those files exist and are exposed to the public.
- There are multiple methods of preventing a user's command history from being flushed to their .bash_history file, including use of the following commands:set +o history and set -o history to start logging again;unset HISTFILE being added to a user's .bash_rc file; andln -s /dev/null ~/.bash_history to write commands to /dev/nullinstead.

References

- **Unsecured Credentials: Bash History**
- **How to Manage Your Linux Command History**

Domain User with Local Administrator Privileges

HIGH 7.5

H3-2022-0086

Affected Hosts

- 10.2.4.5 (horizon.pod04.example.internal)
- 10.0.220.53 (win10.smoke.net)

Mitigations

- Unless absolutely required, regular domain users should not have local administrator privileges. Restrict privileges so that regular domain users are not part of the local Administrators group on workstations.

References

- **Implementing Least-Privilege Administrative Models**

Gradio Arbitrary File Read Vulnerability

HIGH 7.5

H3-2024-0031

Affected Hosts

- 10.0.220.200 (coldfusion18.smoke.net)
- 10.0.220.200 (coldfusion18.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.0.220.6 (app2.smoke.net)

Mitigations

- Update the target application to the latest version of Gradio, at least version 4.20.0.
- Enable user authentication to access the Gradio application.

References

- **Gradio Changelog**
- **Enabling Gradio Authentication**
- **GitHub Advisory for CVE-2023-51449**
- **GitHub Advisory for CVE-2023-34239**
- **CVE-2024-1561**
- **CVE-2023-51449**
- **CVE-2023-34239**

Credential Dumping - Active Directory Services Database (NTDS)

HIGH 7.2

H3-2021-0046

Affected Hosts

- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)

Mitigations

- Deploy and tune endpoint detection and response tools to monitor and prevent common attacker methods such as Volume Shadow Copy and DCSync.
- Limit the number of privileged accounts in groups like Domain Admins, Enterprise Admins, Account Operators, Server Operators, and Print Operators.
- Ensure all privileged accounts have complex, unique passwords.
- Limit accounts with the "Replicating Directory Changes" permission needed to perform a DCSync.
- Encrypt and secure domain controller backups.

References

- **MITRE ATT&CK Technique: OS Credential Dumping: NTDS**
- **MITRE ATT&CK Technique: OS Credential Dumping: DCSync**

Kerberos Unconstrained Delegation

HIGH 7.1

H3-2023-0009

Affected Assets

- Domain User APP4$
- Domain User FS$

Mitigations

- Privileged domain accounts should have the "Account is sensitive and cannot be delegated" setting enabled within the Active Directory and/or be added to the Protected User group.
- Limit/constrain accounts that require delegation authority to the specific services they require. A domain administrator should check the "Trust this user for delegation to specified services only" radio button in the "Delegation" tab in the account's Properties panel from the Active Directory GUI. and then use the Add button to select the specific services for delegation
- Audit domain accounts that are allowed to delegate users, ensuring only those Principals that truly require this setting have it enabled. To disable an account's delegation authority, a domain administrator can check the "Do not trust this user for delegation" radio button in the "Delegation" tab in the account's Properties panel from the Active Directory GUI.

References

- **Microsoft - Security assessment: Insecure Kerberos delegation**
- **Microsoft - Configuring Kerberos delegation for group Managed Service Accounts**
- **SpecterOps Blog - Another Word on Delegation**

Apache Druid Server-Side Request Forgery Vulnerability

HIGH 7

H3-2021-0041

Affected Hosts

- 10.2.51.104
- 10.2.51.104

Mitigations

- Implement authentication on the server.

References

- **Security Best Practices for Apache Druid**

Redis Unauthenticated Access Vulnerability

MEDIUM 6.5

H3-2024-0018

Affected Host

- 10.0.220.50

Mitigations

- Reconfigure the Redis server to require all connections to be authenticated by enabling the requirepass option in redis.conf.

References

- **CVE-2022-20821**
- **Technical Demonstration of How This Could Be Abused**
- **Vendor Patch Instructions**

Unauthenticated Access to Elasticsearch

MEDIUM 6

H3-2021-0036

Affected Host

- 10.0.40.114

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**

Active Directory Certificate Services Misconfiguration Privilege Escalation - Any Purpose or No (aka SubCA) EKU Misconfiguration

MEDIUM 6

H3-2022-0017

Affected Hosts

- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.229.2 (dc2.smoke.net)

Mitigations

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

References

- **Certified Pre-Owned: Abusing Active Directory Certificate Services**
- **SpectreOps - Certified Pre-Owned**

Unauthenticated Docker Registry API Access

MEDIUM 5.5

H3-2021-0009

Affected Host

- 10.0.229.4 (ex2.smoke.net)

Mitigations

- Ensure the Docker Registry API implements TLS certificates from a trusted CA.
- Enable authentication to the Docker Registry API by configuring basic authentication or token based authentication.

References

- **Docker Registry**
- **Configuring a registry**

Keycloak 12.0.1 - request_uri Blind Server-Side Request Forgery (SSRF)

MEDIUM 5.3

CVE-2020-10770

Affected Hosts

- 10.2.51.106
- 10.2.51.106

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**
- **CVE-2020-10770 keycloak: Default Client configuration is vulnerable to SSRF using the "request_uri" parameter**

Jetty Limited Path Traversal Vulnerability - Second Variation

MEDIUM 5.3

CVE-2021-34429

Affected Host

- 10.2.51.103

Mitigations

- Update to Jetty version 9.4.43, 10.0.6, 11.0.6 or later.

References

- **CVE-2021-34429**
- **Encoded URIs can access WEB-INF**

Adobe ColdFusion WDDX Deserialization Info Leak Vulnerability

MEDIUM 5.3

CVE-2023-44353

Affected Hosts

- 10.2.4.132 (coldfusion18.pod04.example.internal)
- 10.0.40.170

Mitigations

- Follow the instructions referenced in the vendor advisory.

References

- **CVE-2023-44353**
- **Vendor Advisory**

Authenticated Microsoft Windows Machine Account NTLM Coercion via Print Spooler Protocol Manipulation

MEDIUM 5.3

H3-2023-0016

Affected Hosts

- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.229.1 (dc.smoke.net)

Mitigations

- If not required, administrators should block the remote MS-RPRN functionality on the vulnerable host using RPC filters. This can be done by blocking the RPC interface UUIDs for MS-RPRN. Turn off Spooler Service if possible, and disable it from starting back up on boot. Disable kerberos delegation where possible, disable Spooler from accepting client connections (GPO setting), and enable account is sensitive and cannot be delegated for high privileged accounts.
- Enable Extended Protection for Authentication (EPA), disable HTTP on servers running Active Directory Certificate Services (AD CS), disable NTLM authentication on where possible, and enforce SMB signing to mitigate NTLM relay attacks that could result from hosts vulnerable to MS-DFSNM coercion.

References

- **[MS-RPRN]: Print System Remote Protocol**
- **MS-RPRN Abuse (PrinterBug)**

Anonymous Access to ZooKeeper API

MEDIUM 5

H3-2020-0002

Affected Hosts

- 10.2.51.101
- 10.2.51.104

Mitigations

- Configure authentication if possible or at least configure ACLs on the ZooKeeper API if authentication is not possible.

References

- **CWE-284: Improper Access Control**
- **ZooKeeper Security**
- **Configuring ZooKeeper**

Anonymous Access to Printer using PJL or PS

MEDIUM 5

H3-2020-0003

Affected Host

- 10.2.51.101

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**
- **Printer Exploitation Toolkit**

Kubernetes Service Account Token Exposure

MEDIUM 5

H3-2021-0007

Affected Hosts

- 10.2.13.31
- 10.2.4.10
- 10.2.13.29
- 10.2.4.12

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**
- **Using RBAC Authorization**
- **CIS Benchmarks: Securing Kubernetes**

Unauthenticated Access to Apache Solr

MEDIUM 5

H3-2022-0028

Affected Hosts

- 10.2.51.107
- 10.2.51.108

Mitigations

- Disable anonymous access. Administrators should configure their deployments following guides listed in references.

References

- **Basic Authentication Plugin**
- **Securing Solr With Basic Authentication**

Unauthenticated Access to Jenkins People Directory

MEDIUM 5

H3-2022-0033

Affected Hosts

- 10.0.229.4 (ex2.smoke.net)
- 10.0.40.102 (airflow-target.smoke.net)
- 10.2.51.103

Mitigations

- Disable anonymous access. Administrators should configure their deployments following guides listed in references.

References

- **Managing Security**
- **Access granted with Overall/Read**

Jenkins Self-Signup Enabled

MEDIUM 5

H3-2022-0071

Affected Host

- 10.2.51.103

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**

Unauthenticated Gitlab User Enumeration

MEDIUM 5

H3-2022-0078

Affected Host

- 10.2.51.107

Mitigations

- Disable 'Public' access. Administrators should configure their deployments following guides listed in references.

References

- **Project and group visibility**

Unauthenticated Jenkins Dashboard Exposure

MEDIUM 5

H3-2023-0026

Affected Hosts

- 10.0.229.4 (ex2.smoke.net)
- 10.2.51.103
- 10.0.40.102 (airflow-target.smoke.net)

Mitigations

- Enable security through authentication using the guide provided by Jenkins.

References

- **Securing Jenkins**

Zone Transfer Allowed to Any Server

MEDIUM 4.8

H3-2020-0004

Affected Host

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

Mitigations

- Only allow zone transfers to servers that require the information.

References

- **CAPEC-291: DNS Zone Transfers**
- **AXFR Requests May Leak Domain Information**

Ruby on Rails Debug Mode Enabled

MEDIUM 4.5

H3-2022-0038

Affected Host

- 10.0.4.24 (irc.testirc.net)

Mitigations

- Configure rails application to run in production mode.

References

- **RailsGuides**

Golang pprof Debugging Endpoint Enabled

MEDIUM 4.5

H3-2022-0039

Affected Hosts

- 10.2.4.12
- 10.2.13.31

Mitigations

- Ensure that net/http/pprof endpoints are not exposed to the internet.

References

- **Your pprof is showing**
- **GO Documentation**

Public Access to Amazon EC2 AMI

MEDIUM 4.5

H3-2022-0088

Affected Asset

- AWS EC2 Resource arn:aws:ec2:us-east-2:209109850873:image/ami-03fbf714e4910ff68

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**

Public Access to Amazon EBS Snapshot

MEDIUM 4.5

H3-2022-0089

Affected Asset

- AWS EC2 Resource arn:aws:ec2:us-east-2:209109850873:snapshot/snap-06a19b9d04f902946

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**

Public Access to Amazon RDS Snapshot

MEDIUM 4.5

H3-2022-0090

Affected Asset

- AWS RDS Resource arn:aws:rds:us-east-1:209109850873:snapshot:database-take-1-final-snapshot

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**

Active Directory - User Password Not Required

MEDIUM 4.3

H3-2023-0030

Affected Assets

- Cleartext Password for Guest
- Cleartext Password for SM_c48084e09f664184a
- Cleartext Password for Guest
- Cleartext Password for SM_25f4676d3dfa47c59
- Cleartext Password for SM_7c7c4a569dfc46f88

Mitigations

- Remove the PASSWD_NOTREQD from the affected User object's userAccountControl attribute. If a Domain Administrator is not able to remove the flag, it is because the account is enabled and does not have a password specified. You should first specify a password for the user before attempting to remove the flag again.

References

- **Microsoft - Understanding and Remediating "PASSWD_NOTREQD"**
- **Microsoft - Querying UserAccountControl Configurations**
- **Bloodhound - ReadTheDocs - User Node, Extra Properties**

Public Access to Amazon S3 Bucket

LOW 3.9

H3-2021-0001

Affected Assets

- S3 Bucket backpedal-unpack-bling
- S3 Bucket level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
- S3 Bucket twitch-rasping-theme
- S3 Bucket flaws.cloud
- S3 Bucket level3-9afd3927f195e10225021a578e6f78df.flaws.cloud

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**
- **How can I secure the files in my Amazon S3 bucket?**

Guest Account Enabled

LOW 3

H3-2020-0008

Affected Hosts

- 10.0.4.24 (irc.testirc.net)
- 10.0.4.31 (openmediavault.pod04.example.internal)
- 10.0.4.23 (obwa.pod04.example.internal)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- 10.0.4.130 (win10.pod04.example.internal)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- 10.0.220.52 (win7.smoke.net)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.229.1 (dc.smoke.net)

Table of Contents

- **Option 1: Disable the Guest Account**
- **Option 2: Restrict the Guest Account Access**

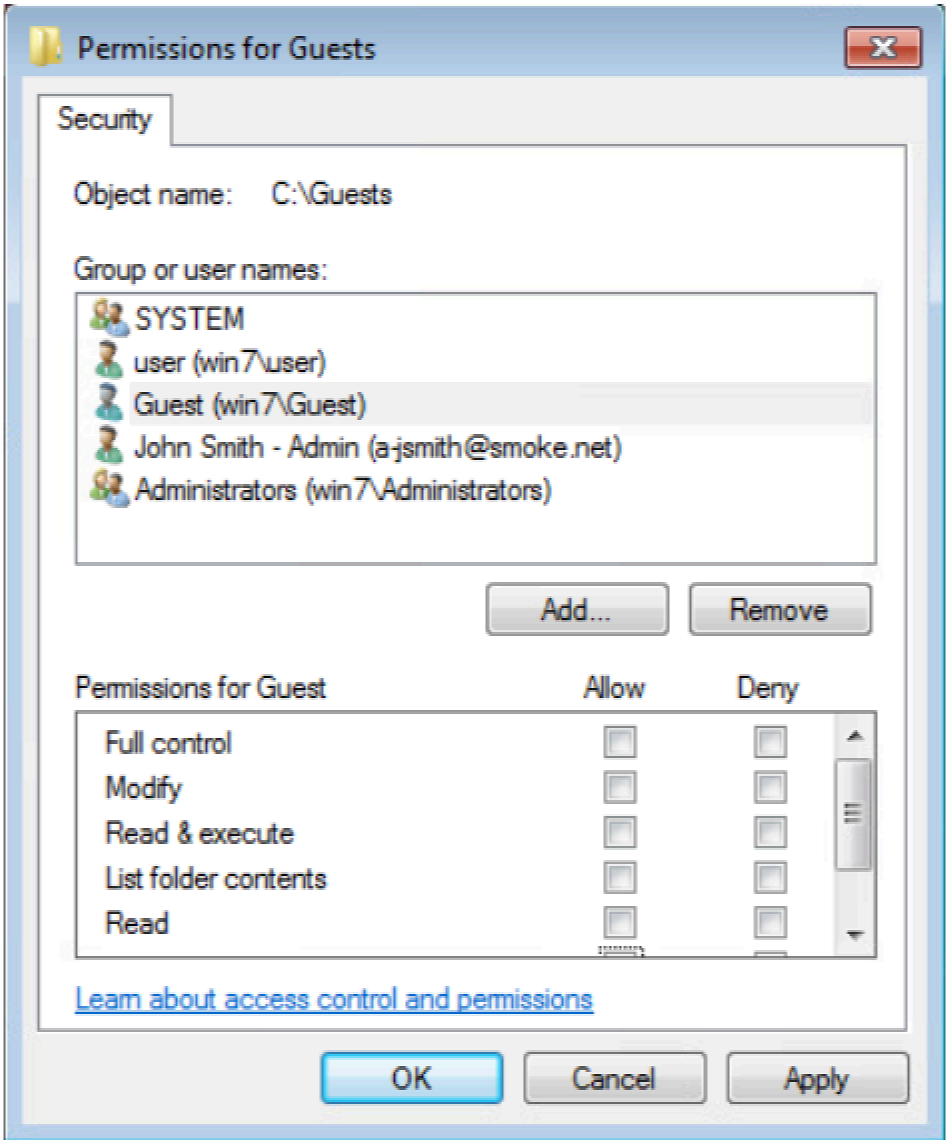
Option 1: Disable the Guest Account

If the Guest account is not in use, completely disable it by opening a Administrative command prompt on the host and issuing the following command:

```
net user guest /active:no
```

Option 2: Restrict the Guest Account Access

If the Guest account is in use, restrict access to available shares by right clicking the share folder on the host, selecting the “Security” tab, selecting the “Guest” user, and removing any privileges.



Object name: C:\Guests

Group or user names:

- SYSTEM
- user (win7\user)
- Guest (win7\Guest)
- John Smith - Admin (a-jsmith@smoke.net)
- Administrators (win7\Administrators)

Permissions for Guest	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□

Mitigations

- Disable the Guest account if not needed.
- If needed, ensure Guest account does not have access to sensitive information.

References

- **Accounts: Guest account status - security policy setting**

Weak or Default Credentials - SNMP

LOW 3

H3-2021-0015

Affected Hosts

- 10.2.51.107
- 10.2.51.107
- 10.0.229.4 (ex2.smoke.net)
- 10.0.229.4 (ex2.smoke.net)

Table of Contents

- **Option 1: Disable the SNMP Service**
- **Option 2: Update the Community String to a Strong Password**

Option 1: Disable the SNMP Service

If the service is not in use, the best mitigation is to disable it. With a wide variety of devices possible running the SNMP service, instructions for updating SNMP settings is not a one-size fits all solution. Typically instructions can be found on the vendor website. If none are available, SNMP settings can often be configured in the webpage of that device in the network settings.

Option 2: Update the Community String to a Strong Password

With a wide variety of devices possible running the SNMP service, updating the SNMP community string is not a one-size fits all solution. Typically instructions for updating the SNMP community string can be found on the vendor website. If none are available, SNMP community string settings can often be configured in the webpage of that device in the network settings.

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**
- **T1110: Brute Force**

Web Directory Listing

LOW 3

H3-2022-0069

Affected Hosts

- 10.2.51.102
- 10.0.4.23 (obwa.pod04.example.internal)
- 10.2.51.103
- 10.0.40.63
- 10.0.40.71
- 10.2.51.102
- 10.0.4.24 (irc.testirc.net)

Mitigations

- Disable directory listing on the web server.

References

- **CWE-552**
- **Disable directory listing in Apache**
- **Disable directory listing in nginx**
- **Disable directory listing in IIS**

Exposed Kubernetes Version

LOW 2

H3-2022-0082

Affected Hosts

- 10.2.13.29
- 10.2.4.12
- 10.2.4.10
- 10.2.13.31

Mitigations

- Modify the KubeletConfiguration file by setting the enableDebuggingHandlers bool to false.

References

- **Kubelet Configuration**

Weak Password Strength Requirements

LOW 1

H3-2021-0028

Affected Hosts

- 10.2.4.5 (horizon.pod04.example.internal)
- 10.0.220.53 (win10.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.2.4.5 (horizon.pod04.example.internal)
- 10.2.4.5 (horizon.pod04.example.internal)
- 10.0.220.53 (win10.smoke.net)
- 10.0.220.53 (win10.smoke.net)
- 10.2.4.5 (horizon.pod04.example.internal)
- 10.0.220.53 (win10.smoke.net)
- 10.2.4.5 (horizon.pod04.example.internal)
- 10.2.4.5 (horizon.pod04.example.internal)

Mitigations

- Configure your password policy to set a high minimum password length of 12 characters or more.

References

- **NIST Special Publication 800-63B: Digital Identity Guidelines**
- **Microsoft - Password Policy Recommendations**

SMB Null Session Allowed

LOW 0.1

H3-2020-0007

Affected Hosts

- 10.0.4.136 (win7-32)
- 10.0.4.129 (win7.pod04.example.internal)
- 10.0.4.14 (win2008)
- Domain Controller 10.0.4.2 (dc02.pod04.example.internal)
- 10.0.40.70
- 10.0.40.53 (sambacry)
- 10.0.4.24 (irc.testirc.net)
- 10.0.220.52 (win7.smoke.net)
- 10.0.4.31 (openmediavault.pod04.example.internal)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- 10.0.220.54 (winxp.smoke.net)
- Domain Controller 10.0.229.2 (dc2.smoke.net)
- Domain Controller 10.0.4.1 (dc01.pod04.example.internal)
- 10.0.4.23 (obwa.pod04.example.internal)

Mitigations

- Disable SMB Null Sessions if not needed using Group Policy or other enterprise configuration management solution.
- If SMB Null Sessions are required, implement strong NTFS permissions for more granular access control to authorized resources.

References

- **CWE-284: Improper Access Control**
- **Network security: Allow LocalSystem NULL session fallback**
- **How to disable SMB/NETBIOS NULL Session on domain controllers**
- **Network access: Restrict anonymous access to Named Pipes and Shares**
- **SMB and Null Sessions: Why Your Pen Test is Probably Wrong**
- **Share Permissions**

Expired SSL/TLS Certificate

LOW 0.1

H3-2021-0025

Affected Hosts

- 10.2.51.101
- 10.0.4.26
- 10.2.13.31
- 10.2.13.31
- 10.2.13.32
- 10.0.220.200 (coldfusion18.smoke.net)
- 10.0.220.50
- 10.2.13.88
- 10.0.229.4 (ex2.smoke.net)
- 10.0.40.79
- 10.2.13.29
- 10.2.13.29
- 10.2.13.30
- 10.0.220.200 (coldfusion18.smoke.net)
- 10.2.13.30
- 10.2.13.30
- 10.0.229.4 (ex2.smoke.net)
- 10.0.220.50
- 10.0.40.1 (pfsense.smoke.net)
- 10.0.40.82

Mitigations

- Renew the certificate.
- If not in use, shut down the web site with the expired certificate.

References

- **Let's Encrypt**
- **Public Key Certificate**
- **HTTP Strict Transport Security**