

# Endida Internal Pen Test Service



## Internal Penetration Test Fix-Actions Report

Prepared for Endida Ltd

Thursday, 21 March 2024



# Weaknesses

---

● Windows SMB Remote Code Execution Vulnerability	6
<b>CRITICAL 10</b>	
<hr/>	
● Weak or Default Credentials - Cracked Credentials	11
<b>CRITICAL 10</b>	
<hr/>	
● SMB Signing Not Required	12
<b>CRITICAL 10</b>	
<hr/>	
● NBT-NS Poisoning Possible	13
<b>CRITICAL 10</b>	
<hr/>	
● Netlogon Elevation of Privilege Vulnerability	18
<b>CRITICAL 10</b>	
<hr/>	
● Unauthenticated Access to the Jenkins Script Console	19
<b>CRITICAL 10</b>	
<hr/>	
● Server Service Vulnerability	20
<b>CRITICAL 9.8</b>	
<hr/>	
● Apache ActiveMQ Remote Code Execution Vulnerability	21
<b>CRITICAL 9.8</b>	
<hr/>	
● Vulnerable Cisco Smart Install	22
<b>CRITICAL 9.8</b>	
<hr/>	
● VMware vCenter Server Access Control Vulnerability	23
<b>CRITICAL 9.8</b>	
<hr/>	
● VMware vCenter vROPS Plugin Remote Code Execution Vulnerability	24
<b>CRITICAL 9.8</b>	
<hr/>	
● VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability	28

**CRITICAL 9.8**

- Weak or Default Credentials - Web Applications 33

**CRITICAL 9.8**

- Weak or Default Credentials - Microsoft SQL Server 34

**CRITICAL 9.4**

- Apache HTTP Server Path Traversal and Remote Code Execution Vulnerability 35

**CRITICAL 9.2**

- Insecure IPMI Implementation 36

**CRITICAL 9.2**

- IPMI Cipher Zero Vulnerability 39

**CRITICAL 9.2**

- Weak or Default Credentials - SSH 40

**CRITICAL 9.2**

- LLMNR Poisoning Possible 41

**CRITICAL 9.2**

- Insecure Java JMX Configuration 44

**CRITICAL 9.1**

- Kerberos Pre-Authentication Disabled 46

**CRITICAL 9**

- Group Policy Preferences Password Elevation of Privilege Vulnerability 47

**HIGH 8.8**

- Weak or Default Credentials - MySQL 49

**HIGH 8.6**

- Weak or Default Credentials - Postgres 50

**HIGH 8.6**

- Remote Desktop Services Remote Code Execution Vulnerability 51

**HIGH 7.8**

- Anonymous FTP Enabled 52

**HIGH 7.8**

- Weak NFS Export Permissions 53

**HIGH 7.8**

- OpenSSL Heartbleed Vulnerability 55

**HIGH 7.5**

- Apache JServ Protocol (AJP) Vulnerability 56

**HIGH 7.5**

- Subdomain Takeover 57

**HIGH 7.5**

- Public Access to Git Repository 58

**HIGH 7.5**

- Credential Reuse 59

**HIGH 7.5**

- Kerberoasting 60

**HIGH 7.5**

- Weak or Default Credentials - Telnet 61

**HIGH 7**

- Unauthenticated Access to Elasticsearch 62

**MEDIUM 6**

- Unauthenticated Docker Registry API Access 63

**MEDIUM 5.5**

- Anonymous Access to ZooKeeper API 64

**MEDIUM 5**

- Anonymous Access to Printer using PjL or PS 65

MEDIUM 5

- 
- Zone Transfer Allowed to Any Server 66

MEDIUM 4.8

- 
- Public Access to Amazon S3 Bucket 67

LOW 3.9

- 
- Guest Account Enabled 68

LOW 3

- 
- Weak or Default Credentials - SNMP 70

LOW 3

- 
- Weak Password Strength Requirements 71

LOW 1

- 
- SMB Null Session Allowed 72

LOW 0.1

- 
- Dangling DNS Record 73

LOW 0.1

- 
- Expired SSL/TLS Certificate 74

LOW 0.1

# Windows SMB Remote Code Execution Vulnerability CVE-2017-0144

## CRITICAL 10

### 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:

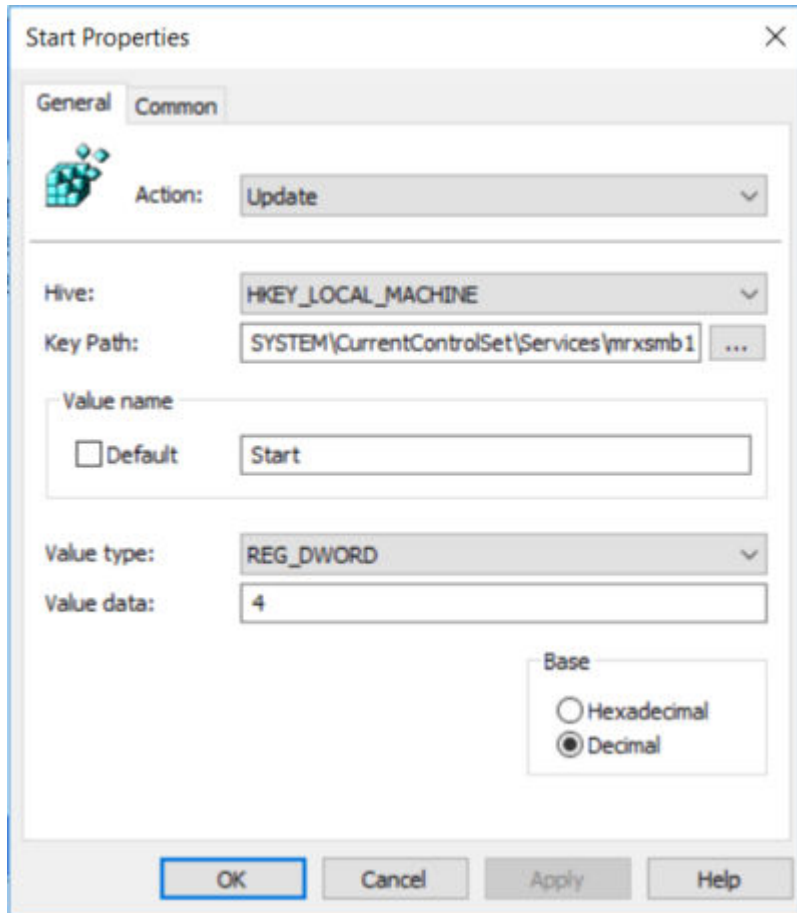
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mrxsm10`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation`

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\mrxsm10
  - **Value name:** Start
  - **Value type:** REG\_DWORD
  - **Value data:** 4

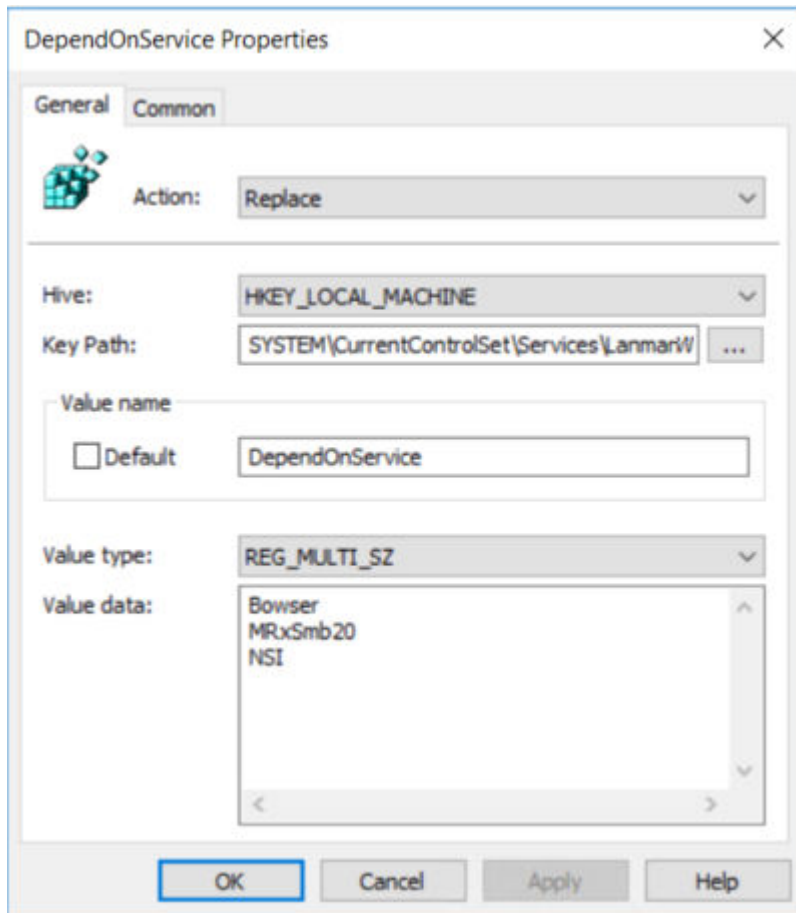
*NOTE:* The default value includes **MRxSMB10** in many versions of Windows, so by replacing them with this multi-value string, it is in effect removing **MRxSMB10** as a dependency for **LanmanServer** and going from four default values down to just these three values

above.



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).



*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
```

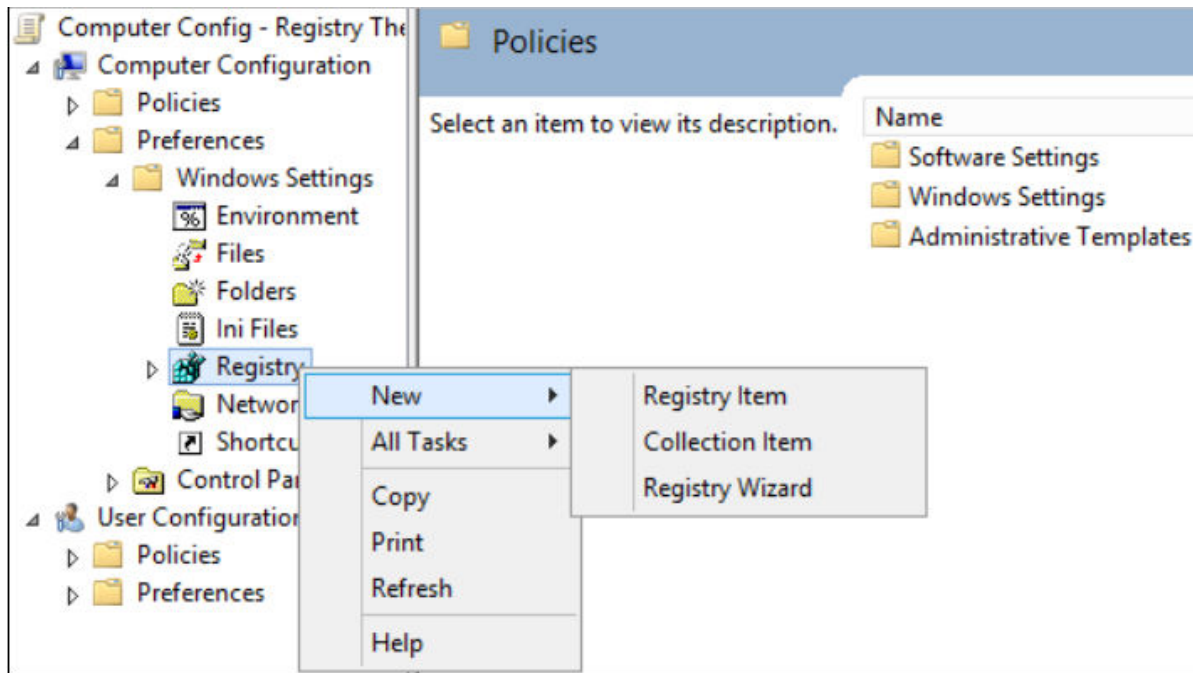
Configured with:

- Registry entry: **SMB1**
- REG\_DWORD: **0** = Disabled

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

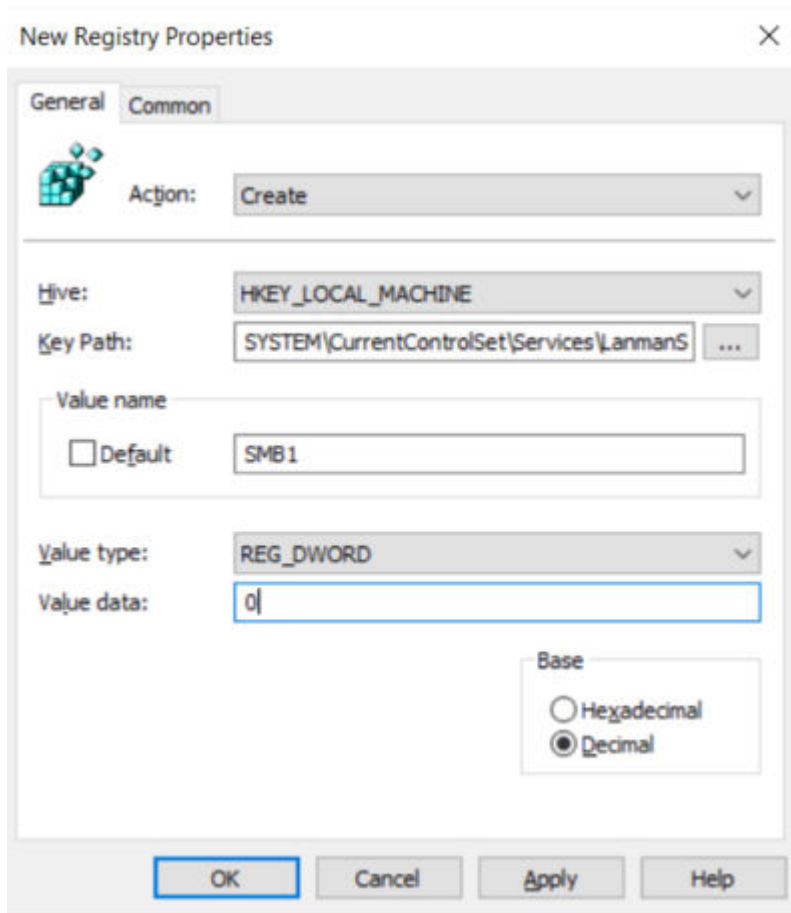
1. Open the **Group Policy Management Console**. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click **Edit**.
2. In the console tree under **Computer Configuration**, expand the **Preferences** folder, and then expand the **Windows Settings** folder.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



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](#)

# Weak or Default Credentials - Cracked Credentials H3-2021-0020

## CRITICAL 10

### 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 H3-2021-0030

## CRITICAL 10

### 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 \(Covering Both SMB1 and SMB2\)](#)

# NBT-NS Poisoning Possible H3-2021-0035

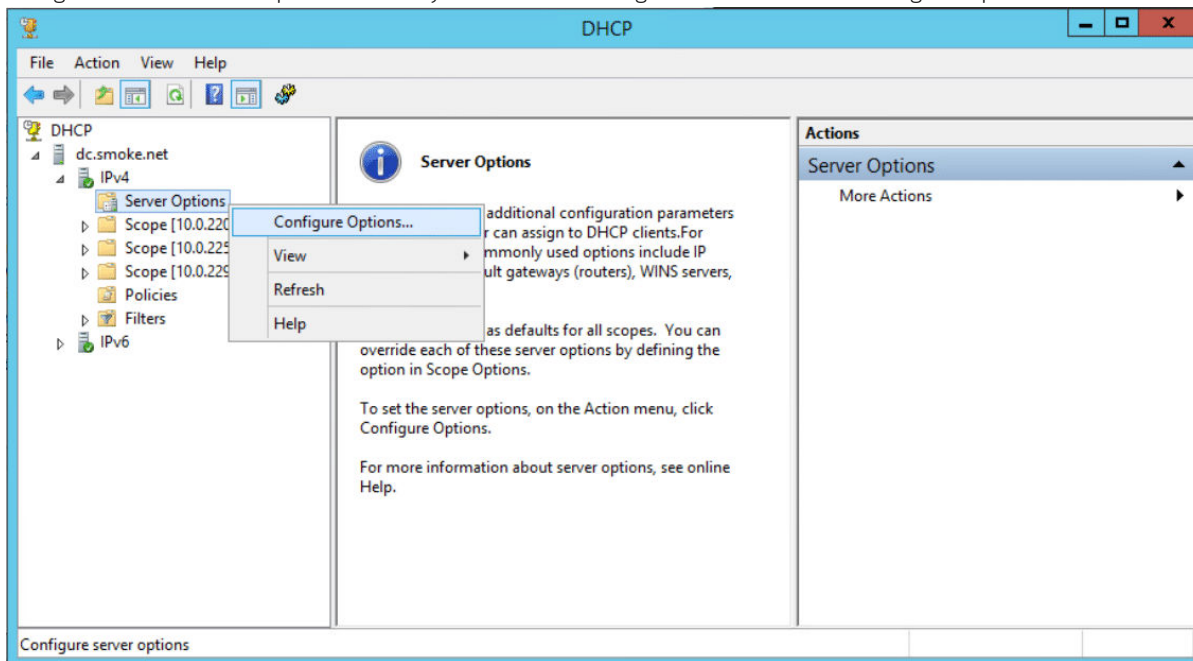
## CRITICAL 10

### Table of Contents

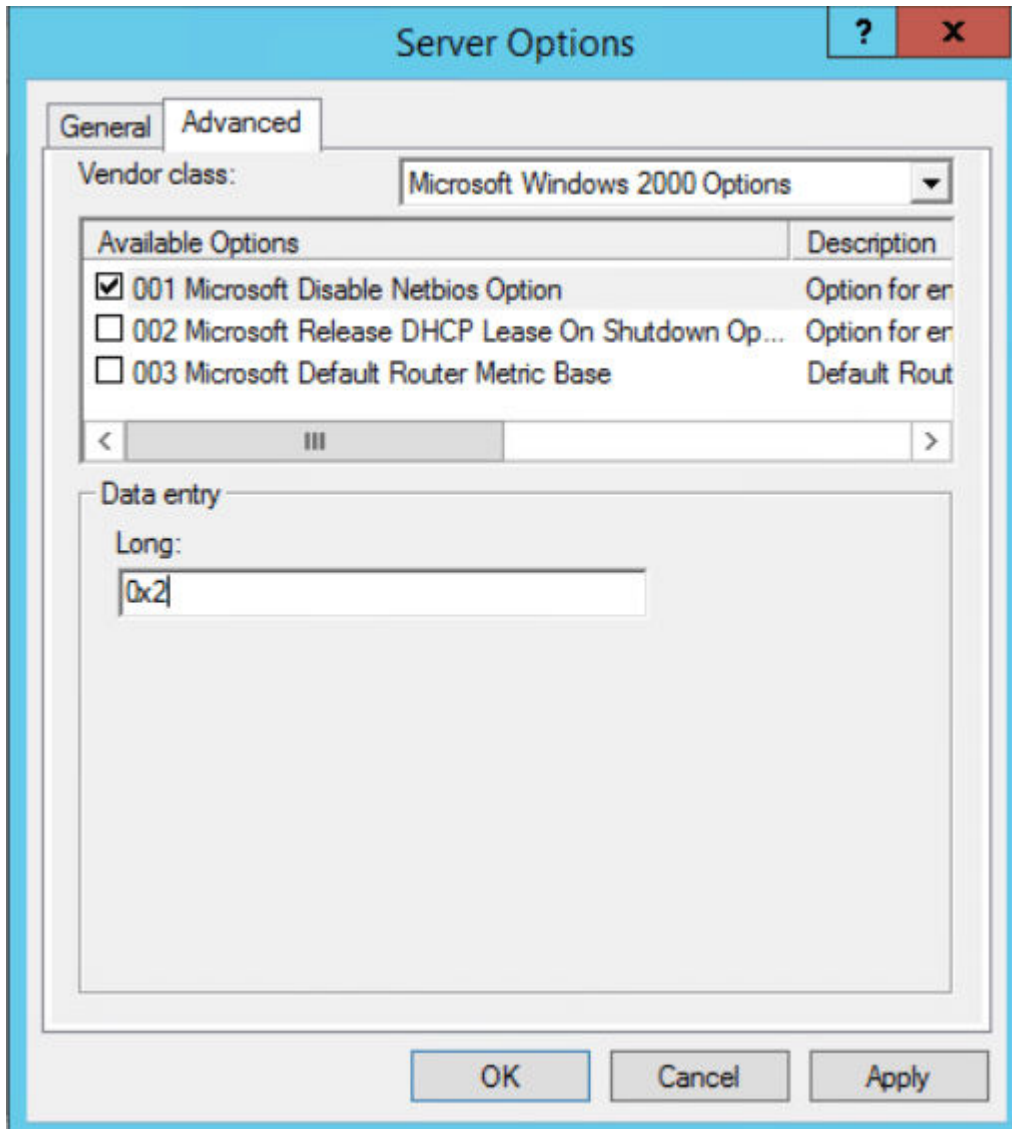
- [Option 1: Disable via DHCP](#)
- [Option 2: Disable via Specific Host](#)

### 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...”

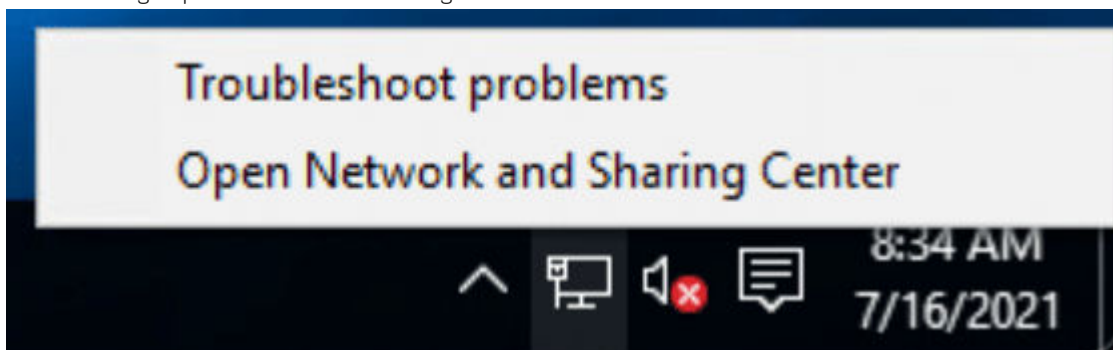


3. Select the “Advanced” tab, select the “Microsoft Windows 2000 Options”, select “001 Microsoft Disable Netbios Option”, change the value to “0x2”, and select “Ok”.

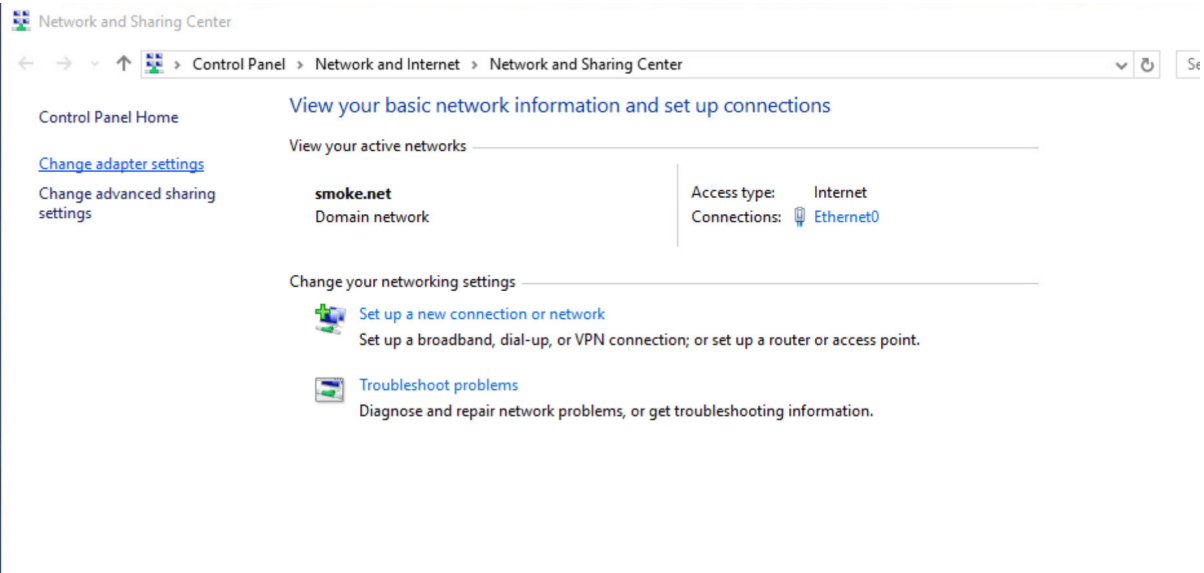


## Option 2: Disable on Specific Host

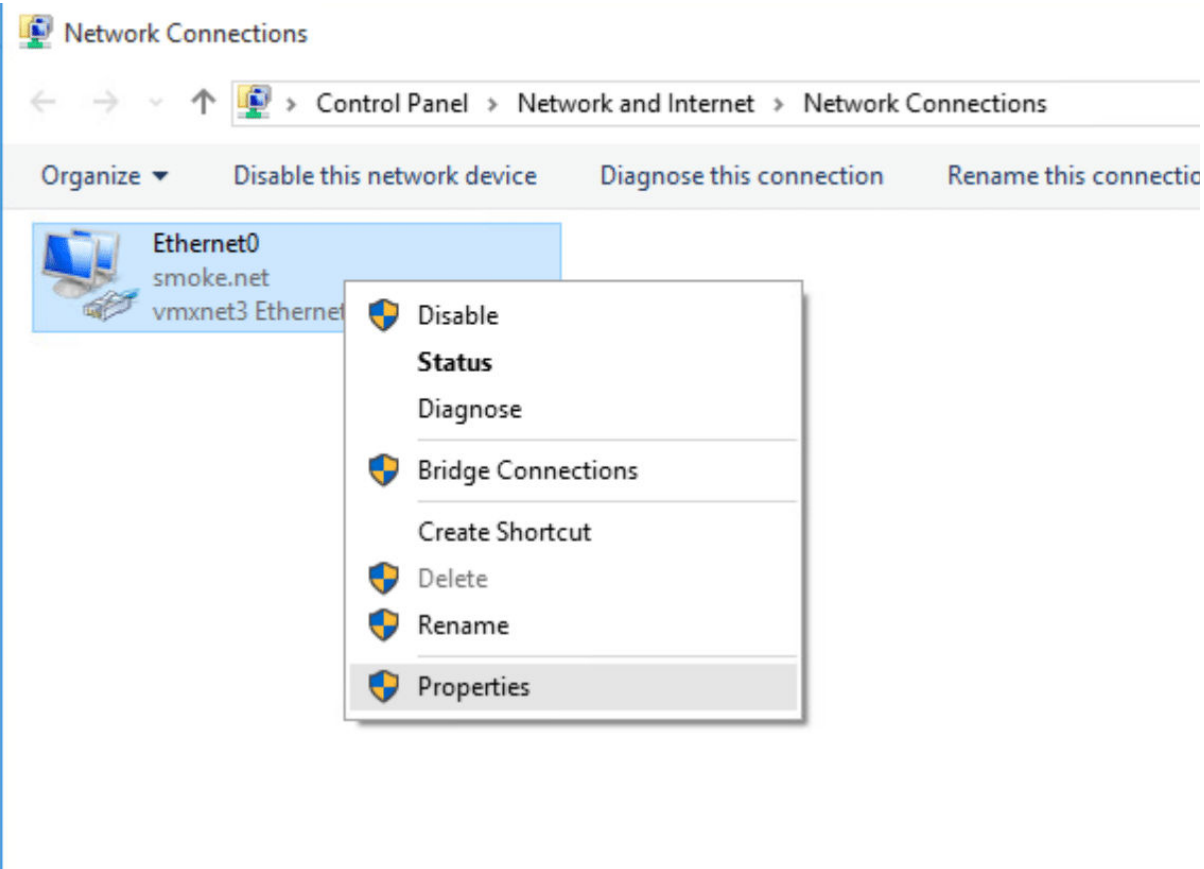
1. Log on to the host and open the “Network and Sharing Center” by searching or right clicking the Network icon in the bottom right and selecting “Open Network and Sharing Center”.



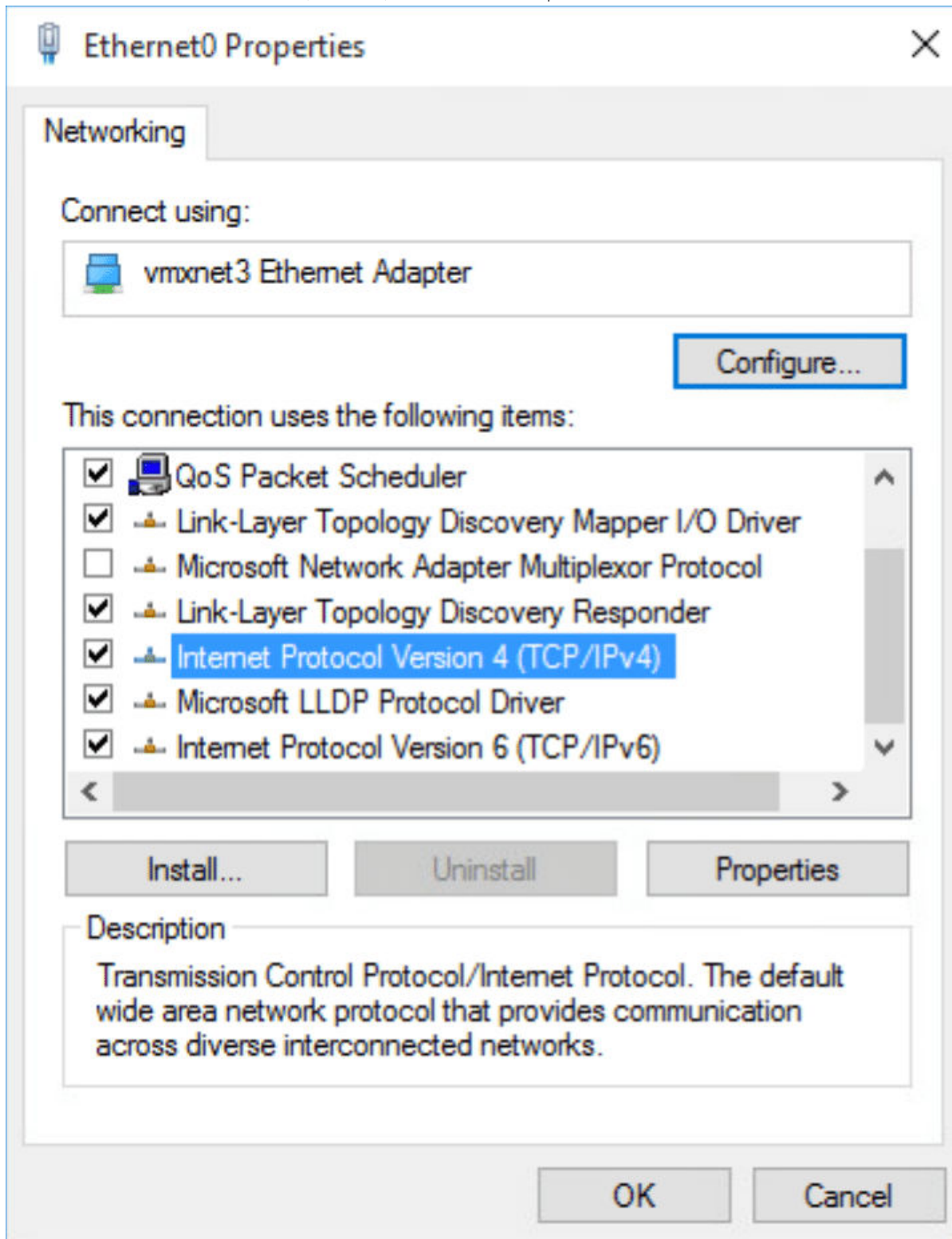
2. Click “Change adapter settings”.



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

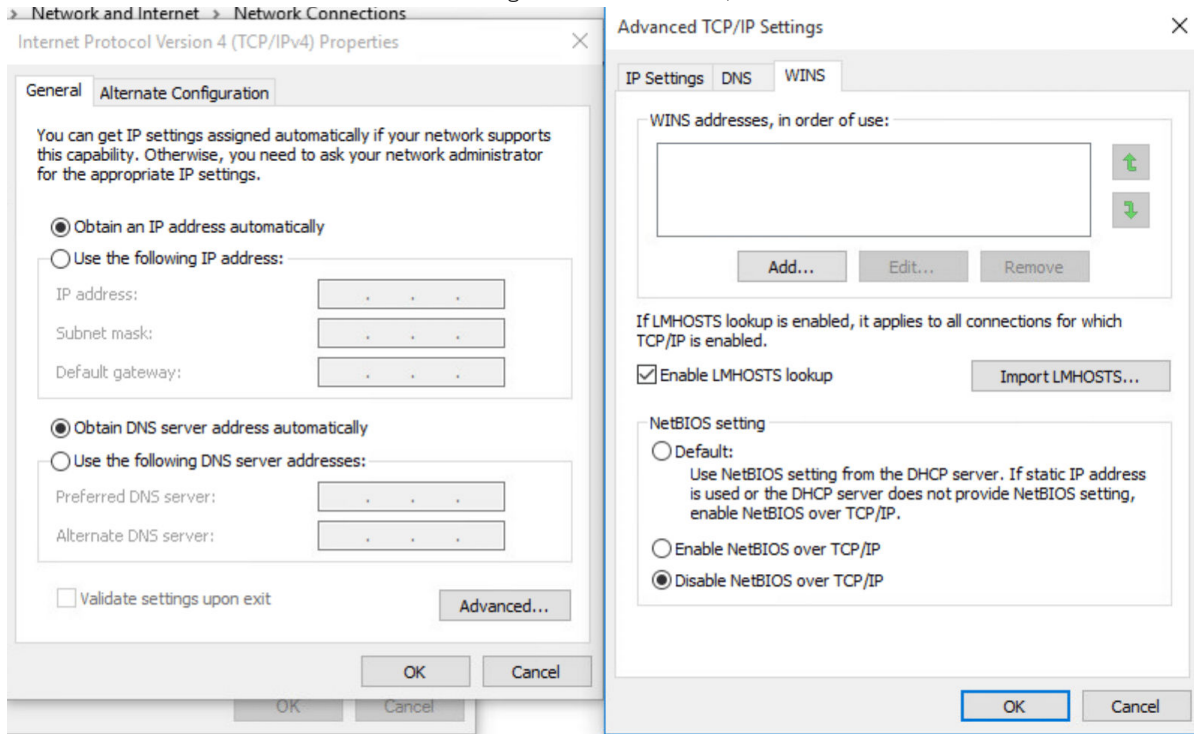


4. Select "Internet Protocol Version 4 (TCP/IPv4)" and click on "Properties".





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



## 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 NBT-NS Poisoning](#)
- [How to Disable LLMNR and Why You Want To](#)

# Netlogon Elevation of Privilege Vulnerability CVE-2020-1472

## CRITICAL 10

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](#)

# Unauthenticated Access to the Jenkins Script Console H3-2020-0021

**CRITICAL 10**

## 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 \(Metasploit\)](#)

# Server Service Vulnerability CVE-2008-4250

**CRITICAL 9.8**

## Mitigations

- Apply the updates referenced in Microsoft Security Bulletin MS08-067.
- Block access to SMB services (139/tcp, 445/tcp) from untrusted networks such as the Internet.

## References

- [CVE-2008-4250](#)

# Apache ActiveMQ Remote Code Execution Vulnerability CVE-2016-3088

**CRITICAL 9.8**

## 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](#)

# Vulnerable Cisco Smart Install CVE-2018-0171

**CRITICAL 9.8**

## 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 4876 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](#)

# VMware vCenter Server Access Control Vulnerability CVE-2020-3952

**CRITICAL 9.8**

## 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

CVE-2021-21972

**CRITICAL 9.8**

## 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:



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:

	Name	Version	Status	VMware Certified	Vendor	Description
<input type="radio"/>	VMware Cloud Director Availability	0.4.0.0	Deployed / Enabled	No	VMware	VMware Cloud Director Availability
<input type="radio"/>	vCenter Server Life-cycle Manager	1.0.0.0	Deployed / Enabled	No	VMware, Inc.	Life-cycle Management for vCenter Server
<input type="radio"/>	VMware vSAN H5 Client Plugin	7.0.1.0	Deployed / Enabled	No	VMware, Inc.	VMware vSAN H5 Client Plugin
<input type="radio"/>	VMware vSphere Lifecycle Manager	7.0.1.16858590	Deployed / Enabled	Yes	VMware	VMware vSphere Lifecycle Manager
<input type="radio"/>	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 vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability CVE-2021-21985

**CRITICAL 9.8**

## 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:

```
3!--
  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](#)



# Weak or Default Credentials - Web Applications H3-2021-0021

## CRITICAL 9.8

### 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 - Microsoft SQL Server H3-2021-0016

## CRITICAL 9.4

### 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 HTTP Server Path Traversal and Remote Code Execution Vulnerability CVE-2021-42013

**CRITICAL 9.2**

## Mitigations

- This vulnerability affects Apache HTTP Server 2.4.49 and 2.4.50. Upgrade to version 2.4.51.

## References


- [Apache 2.4 Vulnerabilities](#)
- [CVE-2021-42013](#)

# Insecure IPMI Implementation H3-2020-0016

## CRITICAL 9.2

### 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  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".

The screenshot shows the HP iLO 4 Administration web interface for a ProLiant BL460c Gen9. The page is titled 'Access Settings' and is divided into two tabs: 'Access Settings' and 'Language'. The left sidebar contains a navigation menu with categories like Information, iLO Federation, Remote Console, Virtual Media, Power Management, Network, Remote Support, Administration, and Access Settings. The 'Access Settings' tab is active, showing a 'Notes' section with two bullet points and a table of service settings. The 'IPMI/DCMI over LAN Access' setting is highlighted with a red box, and its dropdown menu is open, showing 'Enabled', 'Enabled', and 'Disabled' options. A red arrow points to the 'Access Settings' menu item in the sidebar. An 'Apply' button is located at the bottom of the settings table.

Service	Access Op
Secure Shell (SSH) Access	Idle Connection
Secure Shell (SSH) Port	iLO Functionalit
Remote Console Port	iLO ROM-Base
Web Server Non-SSL Port	Require Login f
Web Server SSL Port	Show iLO IP du
Virtual Media Port	Serial Comman
SNMP Access	Serial Comman
SNMP Port	Virtual Serial Pc
SNMP Trap Port	Minimum Passw
IPMI/DCMI over LAN Access	Server Name
IPMI/DCMI over LAN Port	Server FQDN /
	Authentication I
	Authentication I
	Authentication I

## 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 additional 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](#)

# IPMI Cipher Zero Vulnerability H3-2020-0017

**CRITICAL 9.2**

## 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](#)

# Weak or Default Credentials - SSH H3-2021-0014

## CRITICAL 9.2

### 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](#)



# LLMNR Poisoning Possible H3-2021-0034

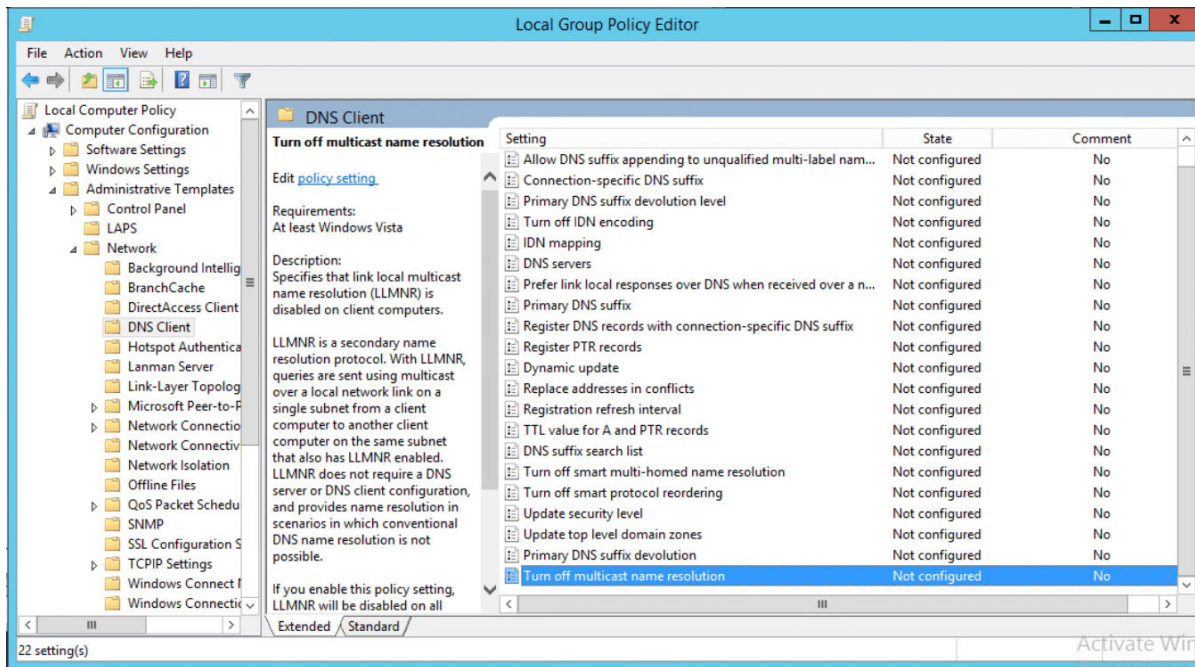
## CRITICAL 9.2

### Table of Contents

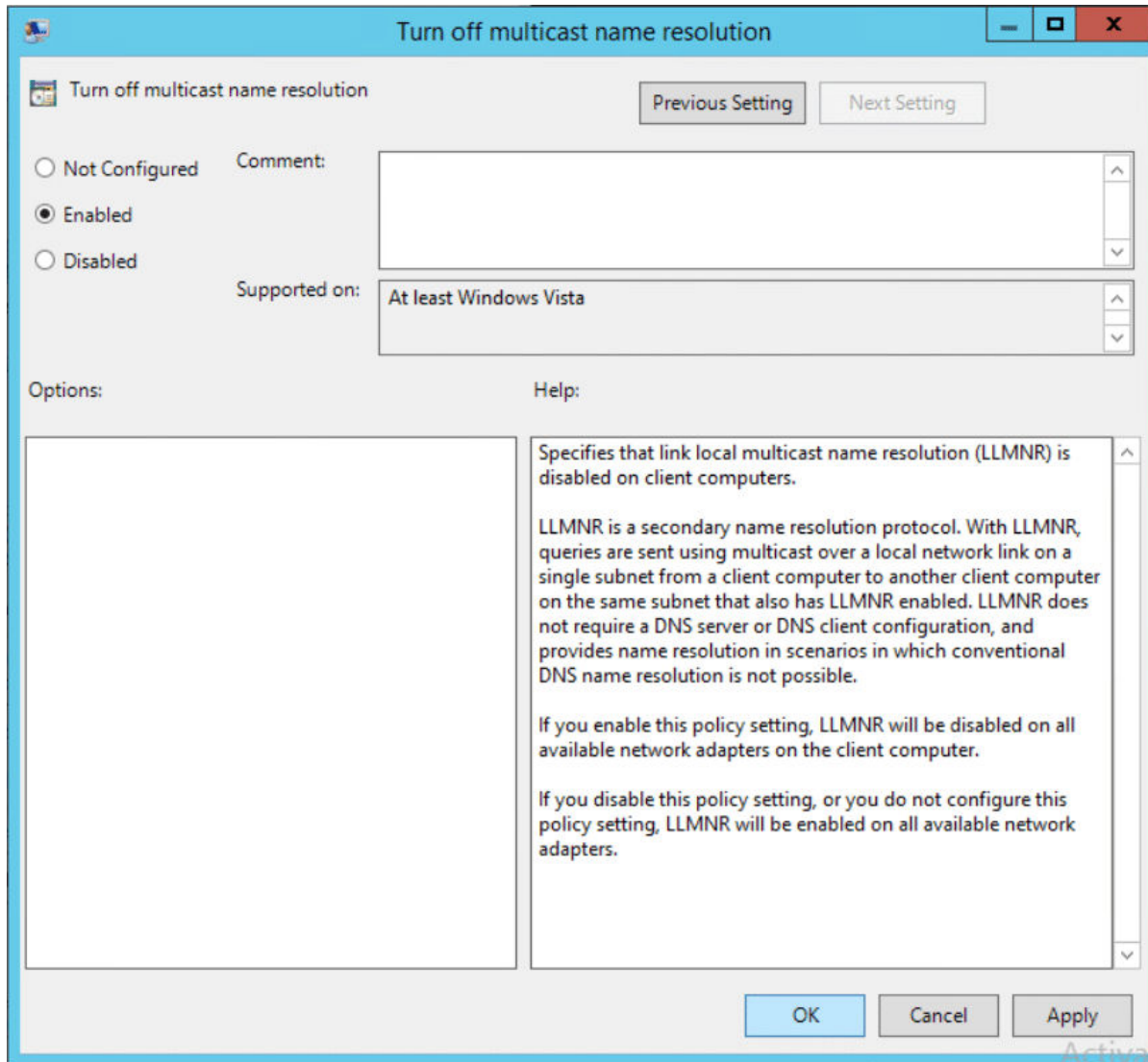
- [Option 1: Disable via Group Policy](#)
- [Option 2: Disable on Selected Hosts](#)

### 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”



3. Click "Enabled" and select "OK"



## 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](#)

# Insecure Java JMX Configuration H3-2020-0022

## CRITICAL 9.1

### 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 \(Metasploit\)](#)

# Kerberos Pre-Authentication Disabled H3-2021-0011

CRITICAL 9

## 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](#)

# Group Policy Preferences Password Elevation of Privilege Vulnerability CVE-2014-1812

HIGH 8.8

## Table of Contents:

- [Option 1: Patch the Host](#)
- [Option 2: Remove Old or Unused Policies](#)

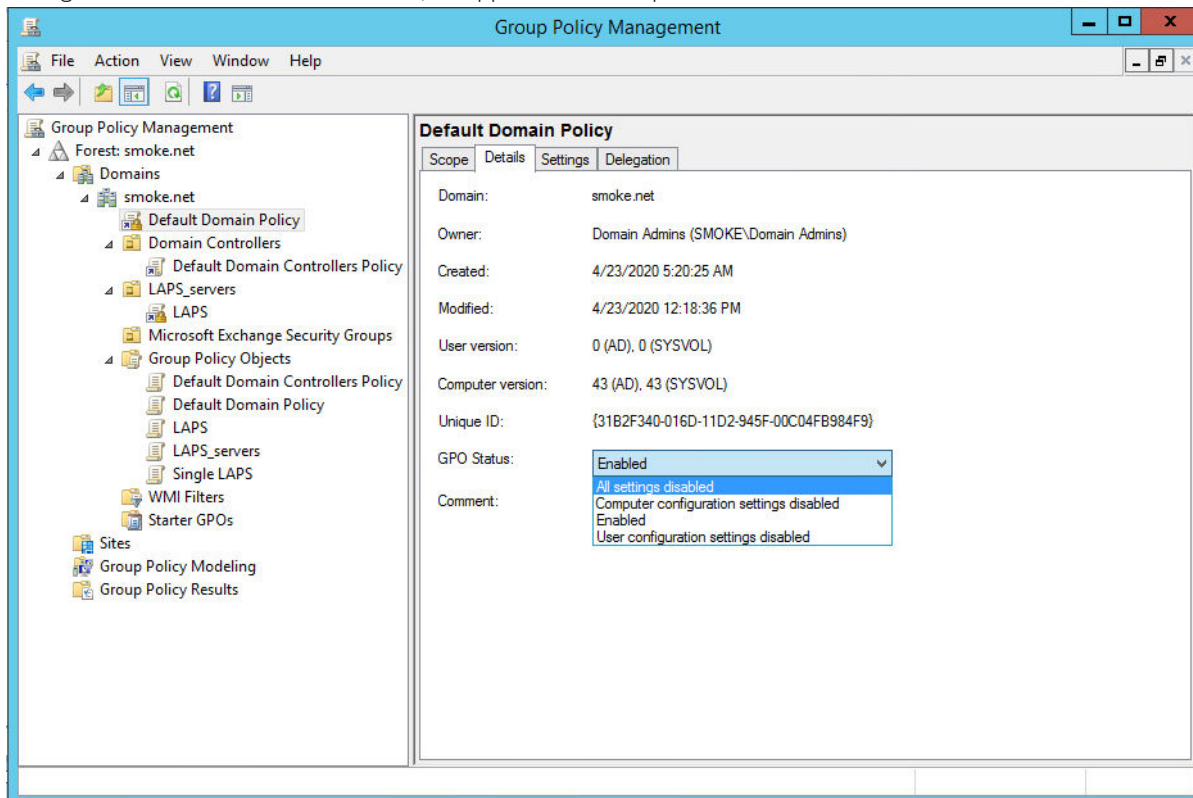
## Option 1: Patch the Host

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.

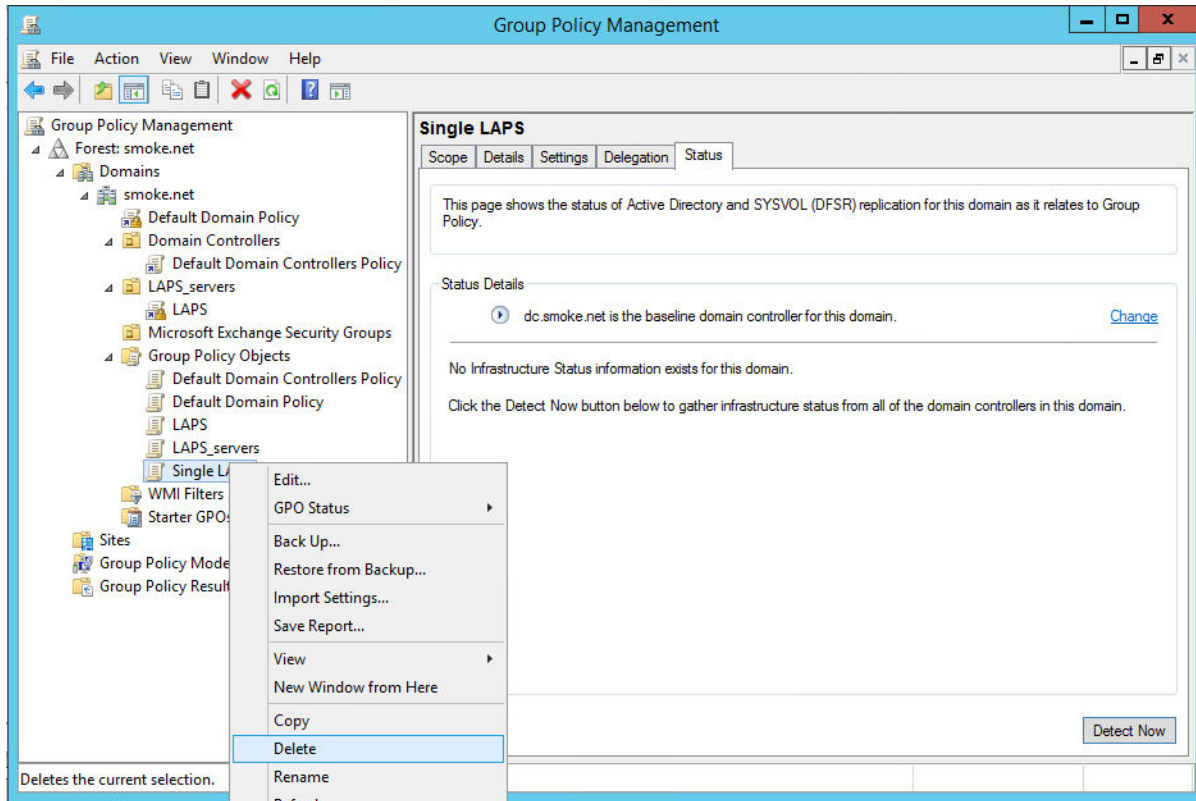
## Option 2: Remove Old or Unused Policies

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.



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.



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 H3-2021-0017

HIGH 8.6

## 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 H3-2021-0018

HIGH 8.6

## 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](#)

# Remote Desktop Services Remote Code Execution Vulnerability

CVE-2019-0708

HIGH 7.8

## 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](#)

# Anonymous FTP Enabled H3-2020-0005

HIGH 7.8

## Mitigations

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

## References

- [CWE-284: Improper Access Control](#)

# Weak NFS Export Permissions H3-2020-0009

HIGH 7.8

## 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](#)

# OpenSSL Heartbleed Vulnerability CVE-2014-0160

HIGH 7.5

## 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 CVE-2020-1938

HIGH 7.5

## 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](#)



# Subdomain Takeover H3-2021-0002

HIGH 7.5

## Table of Contents

- [Option 1: Remove Dangling CNAME](#)
- [Option 2: Update CNAME](#)

## Option 1: Remove Dangling CNAME

1. If the subdomain is no longer in use, then from your DNS zone, remove the subdomain's DNS record.
  2. Review application code and configuration for references to subdomains no longer in use and remove those references.
- 

## Option 2: Update the CNAME

1. If the subdomain is still in use, update the subdomain's DNS record so that its CNAME(s) point to valid resources.
- 

## References

- [Subdomain Takeovers: Thoughts on Risk](#)
- [Prevent Dangling DNS Entries and Avoid Subdomain Takeover](#)

## Mitigations

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

## References

- [Subdomain Takeovers: Thoughts on Risk](#)
- [Prevent Dangling DNS Entries and Avoid Subdomain Takeover](#)

# Public Access to Git Repository H3-2021-0031

HIGH 7.5

## 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 H3-2021-0032

HIGH 7.5

## Mitigations

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

## References

- [NIST Password Guidelines](#)

# Kerberoasting H3-2021-0038

HIGH 7.5

## 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](#)

## Weak or Default Credentials - Telnet H3-2021-0013

HIGH 7

### 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](#)

# Unauthenticated Access to Elasticsearch H3-2021-0036

MEDIUM 6

## 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](#)

# Unauthenticated Docker Registry API Access H3-2021-0009

MEDIUM 5.5

## 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](#)

# Anonymous Access to ZooKeeper API H3-2020-0002

MEDIUM 5

## 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 H3-2020-0003

MEDIUM 5

## 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](#)

# Zone Transfer Allowed to Any Server H3-2020-0004

MEDIUM 4.8

## Mitigations

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

## References

- [CAPEC-291: DNS Zone Transfers](#)
- [AXFR Requests May Leak Domain Information](#)

# Public Access to Amazon S3 Bucket H3-2021-0001

LOW 3.9

## 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 H3-2020-0008

LOW 3

## Table of Contents

- [Option 1: Disable the Guest Account](#)
- [Option 2: Restrict the Guest Account Access](#)

## Option 1: Disable the Guest Account

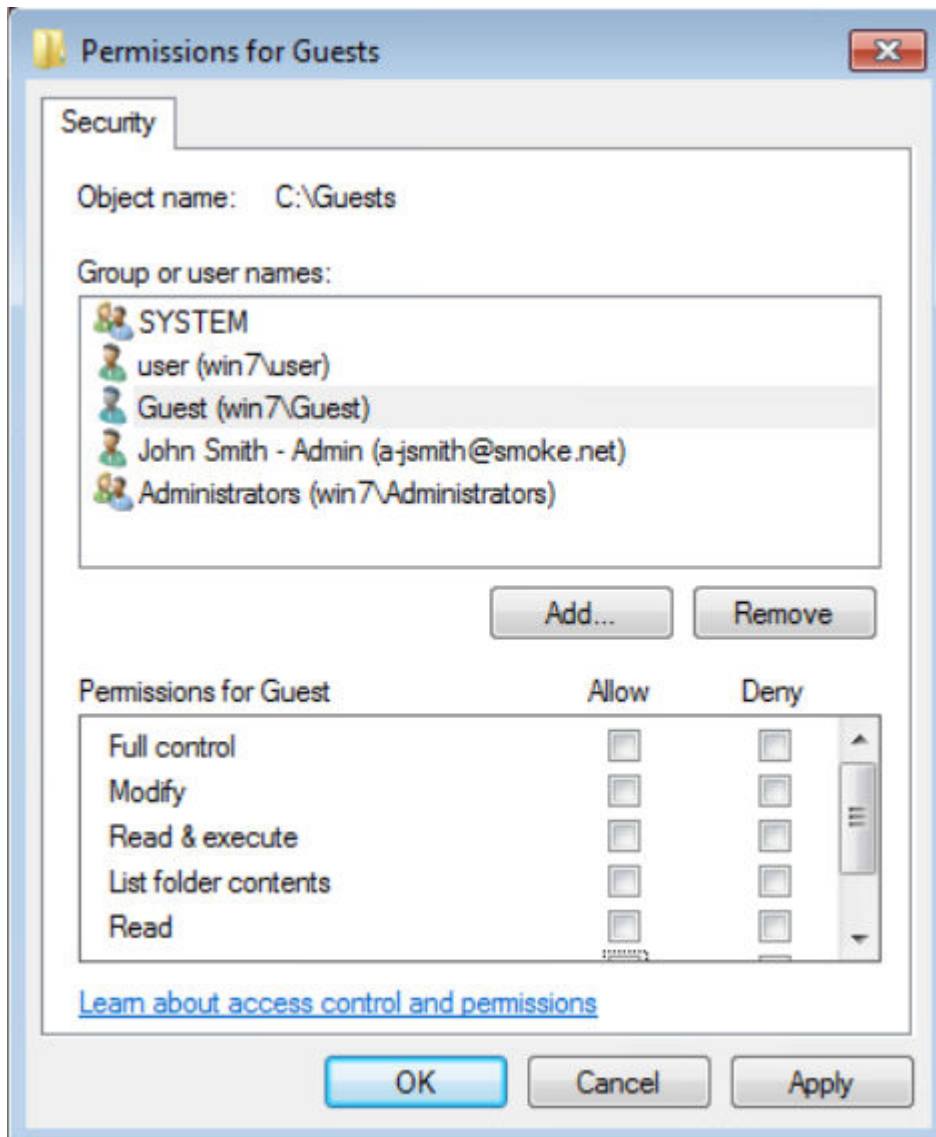
If the Guest account is not in use, completely disable it by opening a Administrative command prompt on the host and issuing the following command:

```
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.



## 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 H3-2021-0015

LOW 3

## 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 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](#)

# Weak Password Strength Requirements H3-2021-0028

LOW 1

## 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 H3-2020-0007

LOW 0.1

## 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](#)



# Dangling DNS Record H3-2021-0024

LOW 0.1

## Mitigations

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

## References

- [Subdomain Takeovers: Thoughts on Risk](#)
- [Prevent Dangling DNS Entries and Avoid Subdomain Takeover](#)

# Expired SSL/TLS Certificate H3-2021-0025

LOW 0.1

## 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](#)