Tenable Vulnerability Management Report

Tenable Vulnerability Management

Wed, 18 Feb 2026 00:05:58 UTC

Table Of Contents

Vulnerabilities By Host

vm-win11-stig-s

Scan Information

Start time:	2026/02/17 23:03
End time:	2026/02/18 00:05

Host Information

DNS Name:	vm-win11-stig-s
Netbios Name:	vm-win11-stig-s
OS:	Microsoft Windows 11 Pro Build 26200

Results Summary

Critical	High	Medium	Low	Info	Total
0	3	2	2	124	131

Results Details

/

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.
Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2021/02/10

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The following 2 NetBIOS names have been gathered :

 vm-win11-stig-s  = Computer name
 vm-win11-stig-s  = Workgroup / Domain name
```

11777 - Microsoft Windows SMB Share Hosting Possibly Copyrighted Material

Synopsis

The remote host may contain material (movies/audio) infringing copyright.

Description

This plugin displays a list of media files (such as .mp3, .ogg, .mpg, .avi) which have been found on the remote SMB shares.
Some of these files may contain copyrighted materials, such as commercial movies or music files, that are being shared without the owner's permission.
If any of these files actually contain copyrighted material, and if they are freely swapped around, your organization might be held liable for copyright infringement by associations such as the RIAA or the MPAA.

Solution

Delete the files infringing copyright.

Risk Factor

None

Plugin Information:

Publication date: 2003/06/26, Modification date: 2012/11/29

Ports
vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Here is a list of files which have been found on the remote SMB shares.
Some of these files may contain copyrighted materials, such as commercial
movies or music files.

 + C$ :

C:\Program Files\WindowsApps\Microsoft.GamingApp_2512.1001.36.0_x64__8wekyb3d8bbwe
\AchievementsPublicAssets\Notifications\AchievementUnlocked.mp3
C:\Program Files\WindowsApps\Microsoft.GamingApp_2512.1001.36.0_x64__8wekyb3d8bbwe
\MessagingPublicAssets\Notifications\Message_Notification_SetA_v14_v2.mp3
C:\Program Files\WindowsApps\Microsoft.GamingApp_2512.1001.36.0_x64__8wekyb3d8bbwe
\PartyPublicAssets\Notifications\Group_Voice_Entry_Others_SetA_v1.mp3
C:\Program Files\WindowsApps\Microsoft.GamingApp_2512.1001.36.0_x64__8wekyb3d8bbwe
\PartyPublicAssets\Notifications\Group_Voice_Exit_Others_SetA_v1.mp3
C:\Program Files\WindowsApps\Microsoft.GamingApp_2512.1001.36.0_x64__8wekyb3d8bbwe
\PartyPublicAssets\Notifications\Message_Notification_SetA_v14_v2.mp3
C:\Program Files\WindowsApps\Microsoft.GamingApp_2512.1001.36.0_x64__8wekyb3d8bbwe
\SocialPublicAssets\Notifications\Message_Notification_SetA_v14_v2.mp3
C:\Windows\ImmersiveControlPanel\SystemSettings\Assets\Aria.mp3
C:\Windows\WinSxS\amd64_microsoft-windows-
i..ntrolpanel.appxmain_31bf3856ad364e35_10.0.26100.7824_none_b6565ad1472d77fb\Jenny.mp3
C:\Windows\WinSxS\amd64_microsoft-windows-
i..ntrolpanel.appxmain_31bf3856ad364e35_10.0.26100.7824_none_b6565ad1472d77fb\Guy.mp3
C:\Windows\WinSxS\amd64_microsoft-windows-
i..ntrolpanel.appxmain_31bf3856ad364e35_10.0.26100.7824_none_b6565ad1472d77fb\Aria.mp3
C:\Windows\ImmersiveControlPanel\SystemSettings\Assets\Jenny.mp3
C:\Windows\ImmersiveControlPanel\SystemSettings\Assets\Guy.mp3
C:\Program Files\WindowsApps\Microsoft.GamingApp_2512.1001.36.0_x64__8wekyb3d8bbwe\Assets\Sounds
\Message.mp3
C:\Program Files\WindowsApps\Microsoft.GamingApp_2512.1001.36.0_x64__8wekyb3d8bbwe\Assets\Sounds
\Group_Voice_Exit_Others_SetA_v1.mp3
C:\Program Files\WindowsApps\Microsoft.GamingApp_2512.1001.36.0_x64__8wekyb3d8bbwe\Assets\Sounds
\Group_Voice_Exit_Me_SetA_v1.mp3
C:\Program [...]
```

16193 - Antivirus Software Check

Synopsis

An antivirus application is installed on the remote host.

Description

An antivirus application is installed on the remote host, and its engine and virus definitions are up to date.

See Also

http://www.nessus.org/u?3ed73b52

https://www.tenable.com/blog/auditing-anti-virus-products-with-nessus

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2005/01/18, Modification date: 2025/05/27

Ports
vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Forefront_Endpoint_Protection :

A Microsoft anti-malware product is installed on the remote host :

  Product name                 : Windows Defender
```

```
  Path                           : C:\ProgramData\Microsoft\Windows Defender\Platform
\4.18.26010.5-0\
  Version                        : 4.18.26010.5
  Engine version                 : 1.1.26010.1
  Antivirus signature version    : 1.445.111.0
  Antispyware signature version : 1.445.111.0
```

34097 - BIOS Info (SMB)

Synopsis

BIOS info could be read.

Description

It is possible to get information about the BIOS via the host's SMB interface.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2008/09/08, Modification date: 2024/06/11

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
  Version      : Hyper-V UEFI Release v4.1
  Release date : 20250610000000.000000+000
  Secure boot  : disabled
```

42898 - SMB Registry : Stop the Registry Service after the scan (WMI)

Synopsis

The registry service was stopped after the scan.

Description

To perform a full credentialed scan, Nessus needs the ability to connect to the remote registry service (RemoteRegistry). If the service is down and if Nessus automatically enabled the registry for the duration of the scan, this plugins will stop it afterwards.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2009/11/25, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
The registry service was successfully stopped after the scan.
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.
Note that this plugin is a remote check and does not work on agents.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2017/06/19, Modification date: 2019/11/22

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The remote host supports the following versions of SMB :
  SMBv2
```

155963 - Windows Printer Driver Enumeration

Synopsis

Nessus was able to enumerate one or more of the printer drivers on the remote host.

Description

Nessus was able to enumerate one or more of the printer drivers on the remote host via WMI.

See Also

http://www.nessus.org/u?fab99415

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2021/12/09, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
--- Universal Print Class Driver ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_53c7641b66238d0c\Amd64\mxdwdrv.dll
  Version            : 10.0.26100.7824
  Supported Platform : Windows x64

--- Microsoft Virtual Print Class Driver ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint4.inf_amd64_67837820f65a44e9\Amd64\msdwdrv.dll
  Version            : 10.0.26100.7824
  Supported Platform : Windows x64

--- Microsoft enhanced Point and Print compatibility driver ---

Nessus detected 2 installs of Microsoft enhanced Point and Print compatibility driver:

  Path               : C:\Windows\system32\spool\DRIVERS\x64\3\mxdwdrv.dll
  Version            : 10.0.26100.7824
  Supported Platform : Windows x64

  Path               : C:\Windows\system32\spool\DRIVERS\W32X86\3\mxdwdrv.dll
  Version            : 10.0.26100.7824
  Supported Platform : Windows NT x86

--- Microsoft Print To PDF ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_53c7641b66238d0c\Amd64\mxdwdrv.dll
  Version            : 10.0.26100.4484
  Supported Platform : Windows x64

--- Microsoft IPP Class Driver ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_53c7641b66238d0c\Amd64\mxdwdrv.dll
  Version            : 10.0.26100.7824
  Supported Platform : Windows x64
```

```
--- Remote Desktop Easy Print ---

  Path               : C:\Windows\system32\spool\DRIVERS\x64\3\mxdwdrv.dll
  Version            : 10.0.26100.1882
  Supported Platform : Windows x64
```

160576 - Windows Services Registry ACL

Synopsis

Checks Windows Registry for Service ACLs

Description

Checks Windows Registry for Service ACLs.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2022/05/05, Modification date: 2024/01/15

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Verbosity must be set to 'Report as much information as possible' for this plugin to produce
 output.
```

162174 - Windows Always Installed Elevated Status

Synopsis

Windows AlwaysInstallElevated policy status was found on the remote Windows host

Description

Windows AlwaysInstallElevated policy status was found on the remote Windows host.
You can use the AlwaysInstallElevated policy to install a Windows Installer package with elevated (system) privileges
This option is equivalent to granting full administrative rights, which can pose a massive security risk. Microsoft
strongly discourages the use of this setting.

Solution

If enabled, disable AlwaysInstallElevated policy per your corporate security guidelines.

Risk Factor

None

Plugin Information:

Publication date: 2022/06/14, Modification date: 2022/06/14

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
AlwaysInstallElevated policy is not enabled under HKEY_LOCAL_MACHINE.
AlwaysInstallElevated policy is not enabled under HKEY_USERS
 user:S-1-5-21-2746855186-1286860024-2359785572-500
```

171410 - IP Assignment Method Detection

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2023/02/14, Modification date: 2026/02/03

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
+ Loopback Pseudo-Interface 1
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ Ethernet
  + IPv4
    - Address       : 10.1.0.115
      Assign Method : dynamic
  + IPv6
    - Address       : fe80::b068:ac12:cc65:b51b%4
      Assign Method : dynamic
```

250276 - Microsoft Teams for Desktop < 25122.1415.3698.6812 Remote Code Execution (August 2025)

Synopsis

Microsoft Teams for Desktop is affected by a remote code execution vulnerability.

Description

The version of Microsoft Teams for Desktop on the remote Windows host is prior to 25122.1415.3698.6812 It is, therefore, affected by a remote code execution vulnerability:
- Heap-based buffer overflow in Microsoft Teams allows an unauthorized attacker to execute code over a network. (CVE-2025-53783)
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?8c9e5451

Solution

Upgrade to Microsoft Teams for Desktop version 25122.1415.3698.6812 or later via the Microsoft Store.

Risk Factor

High

Vulnerability Priority Rating (VPR)

6.7

CVSS v3.0 Base Score

7.5 (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS Base Score

7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

STIG Severity

I

References

CVE	CVE-2025-53783
XREF	IAVA-2025-A-0600

Plugin Information:

Publication date: 2025/08/15, Modification date: 2025/08/15

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Path              : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe
Installed version : 1.0.0.0
Fixed version     : 25122.1415.3698.6812
```

298387 - Shor's Harvest Now Decrypt Later

Synopsis

Reports remote services potentially vulnerable to Shor's Algorithm.

Description

This plugin reports network services that may be vulnerable now to a future attack by adversaries using a cryptographically relevant quantum computer (CRQC). Shor's is a theoretical algorithm that leverages the unique ability of quantum computation to do massively parallel calculations developed by Peter Shor in 1994.
This algorithm easily computes two classically difficult mathematical problems used in modern cryptography; discrete logarithms, and factoring numbers formed by multiplying large primes. Shor's reduces both of these problems from taking exponential time in chosen cases to being solvable in polynomial time.
Asymmetric encryption algorithms such as RSA, Diffie-Hellman and Elliptic Curve Diffie-Hellman are impacted by Shor's Algorithm. The most common uses of these algorithms are in symmetric key establishment and authentication. These uses render Shor's Algorithm particularly dangerous because it may give an adversary the ability to harvest network communications now, and in the future, when a CRQC becomes available, extract the symmetric key and decrypt the communication.

See Also

http://www.nessus.org/u?54fba2c1

Solution

Replace affected ciphers with algorithms chosen to resist CRQC attack.

Risk Factor

None

Plugin Information:

Publication date: 2026/02/09, Modification date: 2026/02/09

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
The TLS service on port 3389 offers these ciphers vulnerable to Shor's:
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 with curves:
  secp384r1, secp256r1 or x25519
 TLS_CK_RSA_WITH_AES_256_CBC_SHA
 TLS_AES_256_GCM_SHA384 with curves:
  secp256r1, secp384r1 or x25519
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 with curves:
  secp384r1, secp256r1 or x25519
 TLS_CK_RSA_WITH_AES_128_CBC_SHA
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 with curves:
  secp256r1, x25519 or secp384r1
 TLS_RSA_WITH_AES_128_CBC_SHA256
 TLS_RSA_WITH_AES_256_CBC_SHA256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 with curves:
  secp256r1, x25519 or secp384r1
 TLS_CK_ECDHE_RSA_WITH_AES_256_CBC_SHA with curves:
  secp256r1, x25519 or secp384r1
 TLS_RSA_WITH_AES_256_GCM_SHA384
 TLS_CK_ECDHE_RSA_WITH_AES_128_CBC_SHA with curves:
  secp384r1, secp256r1 or x25519
 TLS_RSA_WITH_AES_128_GCM_SHA256
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :
- Guest account
- Supplied credentials

See Also

http://www.nessus.org/u?5c2589f6

https://support.microsoft.com/en-us/help/246261

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2025/07/21

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
- The SMB tests will be done as tazdevil4/******
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).
The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.
Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information:

Publication date: 2002/02/13, Modification date: 2024/01/31

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The remote host SID value is : S-1-5-21-2746855186-1286860024-2359785572

The value of 'RestrictAnonymous' setting is : 0
```

70331 - Microsoft Windows Process Module Information

Synopsis

Use WMI to obtain running process module information.

Description

Report details on the running processes modules on the machine.
This plugin is informative only and could be used for forensic investigation, malware detection, and to that confirm your system processes conform to your system policies.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2013/10/08, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Process_Modules_10.1.0.115.csv : lists the loaded modules for each process.
```

72367 - Microsoft Internet Explorer Version Detection

Synopsis

Internet Explorer is installed on the remote host.

Description

The remote Windows host contains Internet Explorer, a web browser created by Microsoft.

See Also

https://support.microsoft.com/en-us/help/17621/internet-explorer-downloads

Solution

N/A

Risk Factor

None

References

XREF	IAVT-0001-T-0509

Plugin Information:

Publication date: 2014/02/06, Modification date: 2022/02/01

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Version  : 11.1882.26100.0
```

72684 - Enumerate Users via WMI

Synopsis

Nessus was able to connect to a host via SMB to retrieve a list of users using WMI.

Description

Nessus was able to connect to a host via SMB to retrieve a list of users using WMI. Only identities that the authenticated SMB user has permissions to view will be retrieved by this plugin.
Note: Unable to query local Domain Controllers during Agent scans.
Rendering User data obtained by plugin 171956.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2014/02/25, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Name            : Administrator
SID             : S-1-5-21-2746855186-1286860024-2359785572-1000
Disabled        : False
Lockout         : False
Change password : True
Source          : Local

Name            : DefaultAccount
SID             : S-1-5-21-2746855186-1286860024-2359785572-503
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

Name            : Guest
SID             : S-1-5-21-2746855186-1286860024-2359785572-501
Disabled        : False
Lockout         : False
Change password : True
Source          : Local
```

```
Name            : tazdevil4
SID             : S-1-5-21-2746855186-1286860024-2359785572-500
Disabled        : False
Lockout         : False
Change password : True
Source          : Local

Name            : WDAGUtilityAccount
SID             : S-1-5-21-2746855186-1286860024-2359785572-504
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

No. Of Users : 5
```

92371 - Microsoft Windows DNS Cache

Synopsis

Nessus was able to collect and report DNS cache information from the remote host.

Description

Nessus was able to collect details of the DNS cache from the remote Windows host and generate a report as a CSV attachment.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2026/02/09

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
_ldap._tcp.dc._msdcs.vm-win11-stig-s
_ldap._tcp.dc._msdcs.zi5bvzlx0idetcyt0okhu05hda.cx.internal.cloudapp.net.
agentserviceapi.guestconfiguration.azure.com
appdata
appdata
au.download.windowsupdate.com
chrome
chrome
client.wns.windows.com
config.edge.skype.com
cp801.prod.do.dsp.mp.microsoft.com
ctldl.windowsupdate.com
dc.services.visualstudio.com
devserver_metadataupload_war
devserver_metadataupload_war
dns.msftncsi.com
download.windowsupdate.com
eastus2-gas.guestconfiguration.azure.com
eastus2-gas.guestconfiguration.azure.com
ecs.office.com
erl
erl
fd.api.iris.microsoft.com
fe2cr.update.microsoft.com
fe3cr.delivery.mp.microsoft.com
g.live.com
geo.prod.do.dsp.mp.microsoft.com
ipv6.msftconnecttest.com
ipv6.msftconnecttest.com
ipv6.msftconnecttest.com
ipv6.msftncsi.com
ipv6.msftncsi.com
kv801.prod.do.dsp.mp.microsoft.com
login.live.com
mobile.events.data.microsoft.com
mqiptservice
mqiptservice
```

```
    msedge.api.cdp.microsoft.com
    msedge.b.tlu.dl.delivery.mp.microsoft.com
    node
    node
    ocsp.digicert.com
    odc.officeapps.live.com
    officeclient.microsoft.com
    oneclient.sfx.ms
    oneocsp.microsoft.com
    outputmessenger
    outputmessenger
    pti.store.microsoft.com
    qcdrpcuotwarpt
    runmqtmc
    runmqtmc
    self.events.data.microsoft.com
    settings-win.data.microsoft.com
    setuprst
    setuprst
    storeedge.microsoft.com
    storeedgefd.dsx.mp.microsoft.com
    tas02.sls.update.microsoft.com
    telerik
    telerik
    time.windows.com
    tsfe.trafficshaping.dsp.mp.microsoft.com
    users
    users
    v10.events.data.microsoft.com
    v20.events.data.microsoft.com
    wdcp.microsoft.com
    windows
    windows
    windows.msn.com
    wpad
    www.msftconnecttest.com
    www.msn.com

DNS cache information attached.
```

92431 - User Shell Folders Settings

Synopsis

Nessus was able to find the folder paths for user folders on the remote host.

Description

Nessus was able to gather a list of settings from the target system that store common user folder locations. A few of the more common locations are listed below :

- Administrative Tools
- AppData
- Cache
- CD Burning
- Cookies
- Desktop
- Favorites
- Fonts
- History
- Local AppData
- My Music
- My Pictures
- My Video
- NetHood
- Personal
- PrintHood
- Programs
- Recent
- SendTo
- Start Menu
- Startup
- Templates

See Also

https://technet.microsoft.com/en-us/library/cc962613.aspx

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
 tazdevil4
  - {7d1d3a04-debb-4115-95cf-2f29da2920da} : C:\Users\tazdevil4\Searches
  - {1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} : C:\Users\tazdevil4\AppData\Roaming\Microsoft\Windows
\Libraries
  - {374de290-123f-4565-9164-39c4925e467b} : C:\Users\tazdevil4\Downloads
  - recent : C:\Users\tazdevil4\AppData\Roaming\Microsoft\Windows\Recent
  - my video : C:\Users\tazdevil4\Videos
  - my music : C:\Users\tazdevil4\Music
  - {56784854-c6cb-462b-8169-88e350acb882} : C:\Users\tazdevil4\Contacts
  - {bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968} : C:\Users\tazdevil4\Links
  - {a520a1a4-1780-4ff6-bd18-167343c5af16} : C:\Users\tazdevil4\AppData\LocalLow
  - sendto : C:\Users\tazdevil4\AppData\Roaming\Microsoft\Windows\SendTo
  - start menu : C:\Users\tazdevil4\AppData\Roaming\Microsoft\Windows\Start Menu
  - cookies : C:\Users\tazdevil4\AppData\Local\Microsoft\Windows\INetCookies
  - personal : C:\Users\tazdevil4\Documents
  - administrative tools : C:\Users\tazdevil4\AppData\Roaming\Microsoft\Windows\Start Menu
\Programs\Administrative Tools
  - startup : C:\Users\tazdevil4\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
  - nethood : C:\Users\tazdevil4\AppData\Roaming\Microsoft\Windows\Network Shortcuts
  - history : C:\Users\tazdevil4\AppData\Local\Microsoft\Windows\History
  - {4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4} : C:\Users\tazdevil4\Saved Games
  - {00bcfc5a-ed94-4e48-96a1-3f6217f21990} : C:\Users\tazdevil4\AppData\Local\Microsoft\Windows
\RoamingTiles
  - !do not use this registry key : Use the SHGetFolderPath or SHGetKnownFolderPath function
 instead
  - local appdata : C:\Users\tazdevil4\AppData\Local
  - my pictures : C:\Users\tazdevil4\Pictures
  - templates : C:\Users\tazdevil4\AppData\Roaming\Microsoft\Windows\Templates
  - printhood : C:\Users\tazdevil4\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
  - cache : C:\Users\tazdevil4\AppData\Local\Microsoft\Windows\INetCache
  - desktop : C:\Users\tazdevil4\Desktop
  - programs : C:\Users\tazdevil4\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
  - [...]
```

93962 - Microsoft Security Rollup Enumeration

Synopsis

This plugin enumerates installed Microsoft security rollups.

Description

Nessus was able to enumerate the Microsoft security rollups installed on the remote Windows host.

See Also

http://www.nessus.org/u?b23205aa

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/10/11, Modification date: 2026/02/10

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Cumulative Rollup : 01_2026_2
Cumulative Rollup : 12_2025
Cumulative Rollup : 11_2025
Cumulative Rollup : 10_2025

Latest effective update level : 01_2026_2
File checked                  : C:\Windows\system32\bcrypt.dll
File version                  : 10.0.26100.7623
Associated KB                 : 5074109
```

136969 - Microsoft Edge Chromium Installed

Synopsis

Microsoft Edge (Chromium-based) is installed on the remote host.

Description

Microsoft Edge (Chromium-based), a Chromium-based web browser, is installed on the remote host.

See Also

https://www.microsoft.com/en-us/edge

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2020/05/29, Modification date: 2026/01/07

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Path    : C:\Program Files (x86)\Microsoft\Edge\Application
Version : 145.0.3800.58
Channel : stable
```

168980 - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information:

Publication date: 2022/12/21, Modification date: 2026/02/03

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Nessus has enumerated the path of the current scan user :

C:\Windows\system32
C:\Windows
C:\Windows\System32\Wbem
C:\Windows\System32\WindowsPowerShell\v1.0\
C:\Windows\System32\OpenSSH\
C:\Users\tazdevil4\AppData\Local\Microsoft\WindowsApps
```

11457 - Microsoft Windows SMB Registry : Winlogon Cached Password Weakness

Synopsis

User credentials are stored in memory.

Description

The registry key 'HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon\CachedLogonsCount' is not 0.
Using a value greater than 0 for the CachedLogonsCount key indicates that the remote Windows host locally caches the passwords of the users when they login, in order to continue to allow the users to login in the case of the failure of the primary domain controller (PDC).
Cached logon credentials could be accessed by an attacker and subjected to brute force attacks.

See Also

http://www.nessus.org/u?184d3eab

http://www.nessus.org/u?fe16cea8

https://technet.microsoft.com/en-us/library/cc957390.aspx

Solution

Consult Microsoft documentation and best practices.

Risk Factor

None

Plugin Information:

Publication date: 2003/03/24, Modification date: 2018/06/05

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Max cached logons : 10
```

48337 - Windows ComputerSystemProduct Enumeration (WMI)

Synopsis

It is possible to obtain product information from the remote host using WMI.

Description

By querying the WMI class 'Win32_ComputerSystemProduct', it is possible to extract product information about the computer system such as UUID, IdentifyingNumber, vendor, etc.

See Also

http://www.nessus.org/u?a21ce849

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2010/08/16, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
+ Computer System Product
  - IdentifyingNumber : 0000-0017-7145-1197-3571-3831-57
  - Description       : Computer System Product
  - Vendor            : Microsoft Corporation
  - Name              : Virtual Machine
  - UUID              : F5D696C8-D220-4F75-B947-BD9723F57732
  - Version           : Hyper-V UEFI Release v4.1
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2022/06/14

Ports

vm-win11-stig-s (TCP/3389) Vulnerability State: Active

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=vm-win11-stig-s
```

58181 - Windows DNS Server Enumeration

Synopsis

Nessus enumerated the DNS servers being used by the remote Windows host.

Description

Nessus was able to enumerate the DNS servers configured on the remote Windows host by looking in the registry.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2012/03/01, Modification date: 2022/02/01

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Nessus enumerated DNS servers for the following interfaces :

Interface: {372f9cab-10df-49f3-8fbb-28e94a5c7cf6}
Network Connection : Ethernet
DhcpNameServer: 168.63.129.16

Interface: Default
DhcpNameServer: 168.63.129.16
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.
Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2013/02/13, Modification date: 2023/05/23

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.
Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information:

Publication date: 2013/07/08, Modification date: 2026/02/10

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
. You need to take the following action :

[ Microsoft Teams for Desktop < 25122.1415.3698.6812 Remote Code Execution (August 2025)
 (250276) ]

+ Action to take : Upgrade to Microsoft Teams for Desktop version 25122.1415.3698.6812 or later
 via the Microsoft Store.
```

71246 - Enumerate Local Group Memberships

Synopsis

Nessus was able to connect to a host via SMB to retrieve a list of local Groups and their Members.

Description

Nessus was able to connect to a host via SMB to retrieve a list of local Groups and their Members.
Note: Unable to query local Domain Controllers during Agent scans.
Rendering Group data obtained by plugin 171956.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2013/12/06, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
 Group Name : Access Control Assistance Operators
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-579
```

```
Members    :

Group Name : Administrators
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-544
Members    :
  Name : tazdevil4
    Domain : vm-win11-stig-s
    Class  : Win32_UserAccount
    SID    : S-1-5-21-2746855186-1286860024-2359785572-500
  Name : Administrator
    Domain : vm-win11-stig-s
    Class  : Win32_UserAccount
    SID    : S-1-5-21-2746855186-1286860024-2359785572-1000
  Name : Guest
    Domain : vm-win11-stig-s
    Class  : Win32_UserAccount
    SID    : S-1-5-21-2746855186-1286860024-2359785572-501

Group Name : Backup Operators
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-551
Members    :

Group Name : Cryptographic Operators
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-569
Members    :

Group Name : Device Owners
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-583
Members    :

Group Name : Distributed COM Users
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-562
Members    :

Group Name : Event Log Readers
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-573
Members    :

Group Name : Guests
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-546
Members    :
  Name : Guest
    Domain : vm-win11-stig-s
    Class  : Win32_UserAccount
    SID    : S-1-5-21-2746855186-1286860024-2359785572-501

Group Name : Hyper-V Administrators
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-578
Members    :

Group Name : IIS_IUSRS
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-568
Members    :
  Name : IUSR
    Domain : vm-win11-stig-s
    Class  : Win32_SystemAccount
    SID    : S-1-5-17

Group Name : Network Configuration Operators
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-556
Members    :

Group Name : OpenSSH Users
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-585
```

```
Members    :

Group Name : Performance Log Users
Host Name  : vm-win11-stig-s
Group SID  : S-1-5-32-559
Members    :

Group Name : Performance Monitor Users
Host Name  : vm-win11-stig-s
Group [...]
```

92365 - Microsoft Windows Hosts File

Synopsis

Nessus was able to collect the hosts file from the remote host.

Description

Nessus was able to collect the hosts file from the remote Windows host and report it as attachment.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2020/01/27

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Windows hosts file attached.

MD5: 3688374325b992def12793500307566d
SHA-1: 4bed0823746a2a8577ab08ac8711b79770e48274
SHA-256: 2d6bdfb341be3a6234b24742377f93aa7c7cfb0d9fd64efa9282c87852e57085
```

92368 - Microsoft Windows Scripting Host Settings

Synopsis

Nessus was able to collect and report the Windows scripting host settings from the remote host.

Description

Nessus was able to collect system and user level Windows scripting host settings from the remote Windows host and generate a report as a CSV attachment.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\displaylogo : 1
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\usewinsafer : 1
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\silentterminate : 0
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\activedebugging : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\displaylogo : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\usewinsafer : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\silentterminate : 0
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\activedebugging : 1

Windows scripting host configuration attached.
```

92434 - User Download Folder Files

Synopsis

Nessus was able to enumerate downloaded files on the remote host.

Description

Nessus was able to generate a report of all files listed in the default user download folder.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
C:\\Users\Public\Downloads\desktop.ini
C:\\Users\tazdevil4\Downloads\desktop.ini

Download folder content report attached.
```

171956 - Windows Enumerate Accounts

Synopsis

Enumerate Windows accounts.

Description

Enumerate Windows accounts.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2023/02/28, Modification date: 2026/01/26

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Windows accounts enumerated. Results output to DB.
User data gathered in scan starting at : 2026/2/17 23:04 UTC
```

187318 - Microsoft Windows Installed

Synopsis

The remote host is running Microsoft Windows.

Description

The remote host is running Microsoft Windows.

See Also

https://www.microsoft.com/en-us/windows

https://www.microsoft.com/en-us/windows-server

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2023/12/27, Modification date: 2026/01/05

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
OS Name      : Microsoft Windows 11 25H2
Vendor       : Microsoft
```

```
Product      : Windows
Release      : 11 25H2
Edition      : Pro
Version      : 10.0.26200.7840
Role         : client
Kernel       : Windows NT 10.0
Architecture : x64
CPE v2.2     : cpe:/o:microsoft:windows_11_25h2:10.0.26200.7840:-:~~pro~~x64~
CPE v2.3     : cpe:2.3:o:microsoft:windows_11_25h2:10.0.26200.7840:-:*:*:pro:*:x64:*
Type         : local
Method       : SMB
Confidence   : 100
```

277650 - Remote Services Not Using Post-Quantum Ciphers

Synopsis

Reports remote services that do not offer post-quantum ciphers.

Description

This plugin reports network services that do not offer post-quantum ciphers. Tenable makes no attempt to determine whether the remote service would be vulnerable to a post-quantum attack.
However, cryptography that depends on the classic difficulty of solving the discrete logarithm problem or on the classic difficulty of large prime factorization is broken by Shor's algorithm. Examples of this are RSA asymmetric encryption and Diffie-Hellman key exchange.

See Also

http://www.nessus.org/u?7a390f87

http://www.nessus.org/u?ad7d6b3b

http://www.nessus.org/u?1c0c61e0

http://www.nessus.org/u?5eec4b28

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2025/12/08, Modification date: 2025/12/08

Ports

vm-win11-stig-s (TCP/3389) Vulnerability State: Active

```
The target TLS server offers no post-quantum ciphers.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2023/12/04

Ports

vm-win11-stig-s (UDP/0) Vulnerability State: Active

```
For your information, here is the traceroute from 10.0.0.8 to 10.1.0.115 :
10.0.0.8
10.1.0.115
```

```
Hop Count: 1
```

10400 - Microsoft Windows SMB Registry Remotely Accessible

Synopsis

Access the remote Windows Registry.

Description

It was possible to access the remote Windows Registry using the login / password combination used for the Windows local checks (SMB tests).

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2025/12/16

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

20811 - Microsoft Windows Installed Software Enumeration (credentialed check)

Synopsis

It is possible to enumerate installed software.

Description

This plugin lists software potentially installed on the remote host by crawling the registry entries in : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall HKLM\SOFTWARE\Microsoft\Updates
Note that these entries do not necessarily mean the applications are actually installed on the remote host - they may have been left behind by uninstallers, or the associated files may have been manually removed.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF	IAVT-0001-T-0501

Plugin Information:

Publication date: 2006/01/26, Modification date: 2022/02/01

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The following software are installed on the remote host :

Microsoft Edge  [version 145.0.3800.58]  [installed on 2026/02/17]
Microsoft Edge Update  [version 1.3.221.3]
Microsoft Edge WebView2 Runtime  [version 145.0.3800.58]  [installed on 2026/02/17]
```

24270 - Computer Manufacturer Information (WMI)

Synopsis

It is possible to obtain the name of the remote computer manufacturer.

Description

By making certain WMI queries, it is possible to obtain the model of the remote computer as well as the name of its manufacturer and its serial number.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2007/02/02, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Computer Manufacturer : Microsoft Corporation
Computer Model : Virtual Machine
Computer SerialNumber : 0000-0017-7145-1197-3571-3831-57
Computer Type : Desktop

Computer Physical CPU's : 1
Computer Logical CPU's  : 1
  CPU0
    Architecture  : x64
    Physical Cores: 1
    Logical Cores : 1

Computer Memory : 3578 MB
  None
    Form Factor: Unknown
    Type       : Unknown
    Capacity   : 1024 MB
  None
    Form Factor: Unknown
    Type       : Unknown
    Capacity   : 2560 MB
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2008/09/23, Modification date: 2026/02/09

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active


```
 {"listening":
[{"port":445,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"cifs","plugin_output":"
 Win32 process 'System' is listening on this port (pid 4)."},
{"port":139,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"smb","plugin_output":"\n
 Win32 process 'System' is listening on this port (pid 4)."},
{"port":135,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"epmap","plugin_output":"
 Win32 process 'svchost.exe' is listening on this port (pid 1012).\n\nThis process
 'svchost.exe' (pid 1012) is hosting the following Windows services :\nRpcEptMapper
 (@%windir%\\system32\\RpcEpMap.dll,-1001)\nRpcSs (@combase.dll,-5010)\n\n"},
{"port":49664,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"dce-
rpc","plugin_output":"\nThe Win32 process 'lsass.exe' is listening on this
 port (pid 800).\n\nThis process 'lsass.exe' (pid 800) is hosting the following
 Windows services :\nKeyIso (@keyiso.dll,-100)\nSamSs (@%SystemRoot%\\system32\
\samsrv.dll,-1)\nVaultSvc (@%SystemRoot%\\system32\\vaultsvc.dll,-1003)\n\n"},
{"port":49665,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"dce-
rpc","plugin_output":"\nThe Win32 process 'wininit.exe' is listening on this port (pid 672)."},
{"port":49666,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"dce-
rpc","plugin_output":"\nThe Win32 process 'svchost.exe' is listening on this port (pid
 1192).\n\nThis process 'svchost.exe' (pid 1192) is hosting the following Windows services :
\nAppinfo (@%systemroot%\\system32\\appinfo.dll,-100)\nIKEEXT (@%SystemRoot%\\system32\
\ikeext.dll,-501)\niphlpsvc (@%SystemRoot%\\system32\\iphlpsvc.dll,-500)\nLanmanServer
 (@%systemroot%\\system32\\srvsvc.dll,-100)\nsacsvr (@%systemroot%\\system32\
\sacsvr.dll,-500)\nSchedule (@%SystemRoot%\\system32\\schedsvc.dll,-100)\nseclogon
 (@%SystemRoot%\\system32\\seclogon.dll,-7001)\nSessionEnv (@%SystemRoot%\\System32\
\SessEnv.dll,-1026)\nShellHWDetection (@%SystemRoot%\\System32\\shsvcs.dll,-12288)\nThemes [...]
```

38689 - Microsoft Windows SMB Last Logged On User Disclosure

Synopsis

Nessus was able to identify the last logged on user on the remote host.

Description

By connecting to the remote host with the supplied credentials, Nessus was able to identify the username associated with the last successful logon.
Microsoft documentation notes that interactive console logons change the DefaultUserName registry entry to be the last logged-on user.

See Also

http://www.nessus.org/u?a29751b5

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2009/05/05, Modification date: 2019/09/02

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Last Successful logon : .\Administrator
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/06/30, Modification date: 2026/02/03

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Hostname : vm-win11-stig-s
  vm-win11-stig-s (WMI)
```

62042 - SMB QuickFixEngineering (QFE) Enumeration

Synopsis

The remote host has quick-fix engineering updates installed.

Description

By connecting to the host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via the registry.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2012/09/11, Modification date: 2022/02/01

Ports
vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Here is a list of quick-fix engineering updates installed on the
remote system :

KB5054156, Installed on: 2026/02/06
KB5066128
```

63080 - Microsoft Windows Mounted Devices

Synopsis

It is possible to get a list of mounted devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates mounted devices that have been connected to the remote host in the past.

See Also

http://www.nessus.org/u?99fcc329

Solution

Make sure that the mounted drives agree with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2012/11/28, Modification date: 2022/02/01

Ports
vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
  Name     : \dosdevices\e:
  Data     : \??\SCSI#CdRom&Ven_Msft&Prod_Virtual_DVD-ROM#5&394b69d0&0&000002#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f004d0073006600740026005000720 06f006

  Name     : \dosdevices\d:
  Data     :
  Raw data : c896d6f50000100000000000

  Name     : \dosdevices\c:
  Data     : DMIO:ID:m#A>*7=
  Raw data : 444d494f3a49443aa7f39a6d96a42341941b3e2a99d6373d

  Name     : \??\volume{f34be2f5-0b97-11f1-be9e-806e6f6e6963}
  Data     : \??\SCSI#CdRom&Ven_Msft&Prod_Virtual_DVD-ROM#5&394b69d0&0&000002#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f004d0073006600740026005000720 06f006
```

70329 - Microsoft Windows Process Information

Synopsis

Use WMI to obtain running process information.

Description

Report details on the running processes on the machine.
This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2013/10/08, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
 Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- Memory Compression (2036)
 0 :    |- smss.exe (452)
 2 : csrss.exe (2020)
 2 : winlogon.exe (504)
 2 : |- dwm.exe (4652)
 2 : |- fontdrvhost.exe (4724)
 2 : explorer.exe (5512)
 2 : |- SecurityHealthSystray.exe (468)
 2 : |- OneDrive.exe (5976)
 2 : |- mmc.exe (7500)
 0 : csrss.exe (608)
 0 : wininit.exe (672)
 0 : |- services.exe (764)
 0 :    |- svchost.exe (1012)
 0 :    |- svchost.exe (1068)
 0 :    |- svchost.exe (1084)
 0 :    |- svchost.exe (1092)
 0 :    |- svchost.exe (1104)
 2 :       |- rdpclip.exe (2968)
 0 :    |- svchost.exe (1192)
 0 :       |- taskhostw.exe (1316)
 2 :       |- taskhostw.exe (2140)
 2 :       |- sihost.exe (4060)
 2 :          |- ShellHost.exe (5528)
 2 :          |- CrossDeviceResume.exe (5820)
 0 :       |- MoUsoCoreWorker.exe (4124)
 0 :       |- MicrosoftEdgeUpdate.exe (5132)
 0 :    |- svchost.exe (1204)
 0 :    |- svchost.exe (1300)
 2 :       |- ctfmon.exe (7296)
 0 :    |- svchost.exe (1308)
 0 :    |- svchost.exe (1368)
 0 :    |- svchost.exe (1656)
 0 :    |- svchost.exe (1680)
 0 :    |- svchost.exe (1728)
 0 :    |- svchost.exe (1784)
 0 :    |- svchost.exe (1852)
 0 :    |- svchost.exe (1996)
 0 :    |- svchost.exe (2056)
 0 :    |- svchost.exe (2124)
 0 :    |- svchost.exe (2232)
 0 :    |- svchost.exe (2256)
 0 :    |- svchost.exe (2360)
 0 :    |- svchost.exe (2416)
 0 :    |- spoolsv.exe (2504)
 0 :    |- svchost.exe (2580)
 0 :    |- svchost.exe (2688)
 0 :    |- svchost.exe (2708)
 0 :       |- AggregatorHost.exe (3676)
 0 :    |- svchost.exe (2764)
 0 :    |- WaAppAgent.exe (2812)
 0 :       |- WaSecAgentProv.exe (3772)
 0 :          |- conhost.exe (796)
 0 :    |- svchost.exe (2824)
 0 :    |- WindowsAzureGuestAgent.exe (2832)
 2 :    |- svchost.exe (2888)
 0 :    |- svchost.exe (3364)
 0 :    |- svchost.exe (3536)
 0 :    |- svchost.exe (3604)
 0 :    |- svchost.exe (3796)
 0 :    |- NisSrv.exe (4000) [...]
```

92364 - Microsoft Windows Environment Variables

Synopsis

Nessus was able to collect and report environment variables from the remote host.

Description

Nessus was able to collect system and active account environment variables on the remote Windows host and generate a report as a CSV attachment.

Solution

N/A

Risk Factor

None

References

XREF	IAVT-0001-T-0757

Plugin Information:

Publication date: 2016/07/19, Modification date: 2026/01/29

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Global Environment Variables :
  processor_level : 6
  comspec : %SystemRoot%\system32\cmd.exe
  number_of_processors : 1
  username : SYSTEM
  os : Windows_NT
  temp : %SystemRoot%\TEMP
  processor_revision : 6a06
  path : %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%
\System32\WindowsPowerShell\v1.0\;%SYSTEMROOT%\System32\OpenSSH\
  tmp : %SystemRoot%\TEMP
  processor_identifier : Intel64 Family 6 Model 106 Stepping 6, GenuineIntel
  driverdata : C:\Windows\System32\Drivers\DriverData
  pathext : .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
  processor_architecture : AMD64
  psmodulepath : %ProgramFiles%\WindowsPowerShell\Modules;%SystemRoot%\system32\WindowsPowerShell
\v1.0\Modules
  windir : %SystemRoot%

Active User Environment Variables
  - S-1-5-21-2746855186-1286860024-2359785572-500
    userdomain : vm-win11-stig-s
    username : tazdevil4
    temp : %USERPROFILE%\AppData\Local\Temp
    path : %USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
    logonserver : \\vm-win11-stig-s
    localappdata : C:\Users\tazdevil4\AppData\Local
    tmp : %USERPROFILE%\AppData\Local\Temp
    homedrive : C:
    homepath : \Users\tazdevil4
    userdomain_roamingprofile : vm-win11-stig-s
    userprofile : C:\Users\tazdevil4
    onedrive : C:\Users\tazdevil4\OneDrive
    appdata : C:\Users\tazdevil4\AppData\Roaming
```

92366 - Microsoft Windows Last Boot Time

Synopsis

Nessus was able to collect the remote host's last boot time in a human readable format.

Description

Nessus was able to collect and report the remote host's last boot time as an ISO 8601 timestamp.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/07/09

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Last reboot : 2026-02-17T22:38:22+00:00 (20260217223822.791629+000)
```

92421 - Internet Explorer Typed URLs

Synopsis

Nessus was able to enumerate URLs that were manually typed into the Internet Explorer address bar.

Description

Nessus was able to generate a list URLs that were manually typed into the Internet Explorer address bar.

See Also

https://forensafe.com/blogs/typedurls.html

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2024/05/08

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
http://go.microsoft.com/fwlink/p/?LinkId=255141

Internet Explorer typed URL report attached.
```

92435 - UserAssist Execution History

Synopsis

Nessus was able to enumerate program execution history on the remote host.

Description

Nessus was able to gather evidence from the UserAssist registry key that has a list of programs that have been executed.

See Also

https://www.nirsoft.net/utils/userassist_view.html

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2019/11/12

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
microsoft.screensketch_8wekyb3d8bbwe!app
{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\windows powershell\windows powershell.lnk
microsoft.windowsterminal_8wekyb3d8bbwe!app
microsoft.windowscalculator_8wekyb3d8bbwe!app
microsoft.windowsfeedbackhub_8wekyb3d8bbwe!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\compmgmt.msc
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\windowspowershell\v1.0\powershell.exe
microsoft.paint_8wekyb3d8bbwe!app
microsoft.windows.shell.rundialog
microsoft.windowsnotepad_8wekyb3d8bbwe!app
microsoft.windows.startmenuexperiencehost_cw5n1h2txyewy!fulltrustapp
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\wf.msc
microsoft.microsoftstickynotes_8wekyb3d8bbwe!app
ueme_ctlcuacount:ctor
microsoft.windows.cloudexperiencehost_cw5n1h2txyewy!app
microsoft.windows.explorer
ueme_ctlsession
microsoft.windows.shellexperiencehost_cw5n1h2txyewy!app
```

```
microsoftwindows.client.cbs_cw5n1h2txyewy!cortanaui

Extended userassist report attached.
```

131023 - Windows Defender Installed

Synopsis

Windows Defender is installed on the remote Windows host.

Description

Windows Defender, an antivirus component of Microsoft Windows is installed on the remote Windows host.

See Also

https://www.microsoft.com/en-us/windows/comprehensive-security

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2019/11/15, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Path                      : C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.26010.5-0\
Version                   : 4.18.26010.5
Engine Version            : 1.1.26010.1
Malware Signature Timestamp : Feb. 17, 2026 at 16:40:16 GMT
Malware Signature Version   : 1.445.111.0
Signatures Last Updated     : Feb. 17, 2026 at 22:57:00 GMT
```

280146 - Microsoft Azure Guest Agent Installed (Windows)

Synopsis

Microsoft Azure Guest Agent is installed on the remote Windows host.

Description

Microsoft Azure Guest Agent is installed on the remote Windows host.

See Also

http://www.nessus.org/u?4da9ec88

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2025/12/30, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Path    : C:\WindowsAzure\GuestAgent_2.7.41491.1183_2026-02-17_003539\CollectVMHealth.exe
Version : 2.7.41491.1183
```

10396 - Microsoft Windows SMB Shares Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials. Depending on the share rights, it may allow an attacker to read / write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2021/10/04

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The following shares can be accessed as tazdevil4 :

- ADMIN$  - (readable,writable)
  + Content of this share :
..
appcompat
apppatch
AppReadiness
assembly
bcastdvr
bfsvc.exe
Boot
bootstat.dat
Branding
BrowserCore
CbsTemp
command_results.log
Containers
CSC
Cursors
debug
diagnostics
DiagTrack
DigitalLocker
Downloaded Program Files
DtcInstall.log
ELAMBKUP
en-US
explorer.exe
Fonts
GameBarPresenceWriter
Globalization
Help
HelpPane.exe
hh.exe
IdentityCRL
IME
ImmersiveControlPanel
InboxApps
INF
InputMethod
Installer
L2Schemas
LanguageOverlayCache
LiveKernelReports
Logs
lsasetup.log
Media
mib.bin
Microsoft
Microsoft.NET
Migration
ModemLogs
notepad.exe
OCR
OEM
Offline Web Pages
Panther
Performance
PFRO.log
PLA
```

```
PolicyDefinitions
Prefetch
Professional.xml
Provisioning
regedit.exe
Registration
RemotePackages
rescache
Resources
SchCache
schemas
security
ServiceProfiles
ServiceState
servicing
Setup
setupact.log
setuperr.log
ShellComponents
ShellExperiences
SKB
SoftwareDistribution
Speech
Speech_OneCore
splwow64.exe
System
system.ini
System32
SystemApps
SystemResources
SystemTemp
SysWOW64
TAPI
Tasks
Temp
tracing

- C$  - (readable,writable)
  + Content of this share :
Documents and Settings
inetpub
Packages
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
swapfile.sys
System Volume Information
Users
Windows
WindowsAzure

- D$  - (readable,writable)
  + Content of this share :
CollectGuestLogsTemp
DATALOSS_WARNING_README.txt
DumpStack.log.tmp
pagefile.sys
System Volume Information
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2021/09/20

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Nessus was able to obtain the following information about the host, by
parsing the SMB2 Protocol's NTLM SSP message:

 Target Name: vm-win11-stig-s
 NetBIOS Domain Name: vm-win11-stig-s
 NetBIOS Computer Name: vm-win11-stig-s
 DNS Domain Name: vm-win11-stig-s
 DNS Computer Name: vm-win11-stig-s
 DNS Tree Name: unknown
 Product Version: 10.0.26100
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2024/09/11

Ports

vm-win11-stig-s (TCP/3389) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
    TLS_AES_256_GCM_SHA384        0x13, 0x02       -             -        AES-GCM(256)
 SHA384


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDHE         RSA      AES-GCM(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
```

```
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDHE         RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE         RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
SHA256
   RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
SHA256


SSL Version : TLSv11
  High Strength Ciphers (>= 112-bit key)

 [...]
```

24272 - Network Interfaces Enumeration (WMI)

Synopsis

Nessus was able to obtain the list of network interfaces on the remote host.

Description

Nessus was able, via WMI queries, to extract a list of network interfaces on the remote host and the IP addresses attached to them.
Note that this plugin only enumerates IPv6 addresses for systems running Windows Vista or later.

See Also

http://www.nessus.org/u?b362cab2

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2007/02/03, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
+ Network Interface Information :

 - Network Interface = [00000000] Microsoft Hyper-V Network Adapter
 - MAC Address = 7C:1E:52:B3:C4:B3
 - IPAddress/IPSubnet = 10.1.0.115/255.255.248.0
 - IPAddress/IPSubnet = fe80::b068:ac12:cc65:b51b/64

+ Network Interface Information :

 - Network Interface = [00000003] Mellanox ConnectX-5 Virtual Adapter
 - MAC Address = 7C:1E:52:B3:C4:B3


+ Routing Information :

    Destination     Netmask         Gateway
    -----------     -------         -------
    0.0.0.0         0.0.0.0         10.1.0.1
    10.1.0.0        255.255.248.0   0.0.0.0
    10.1.0.115      255.255.255.255 0.0.0.0
    10.1.7.255      255.255.255.255 0.0.0.0
    127.0.0.0       255.0.0.0       0.0.0.0
    127.0.0.1       255.255.255.255 0.0.0.0
    127.255.255.255 255.255.255.255 0.0.0.0
```

```
168.63.129.16   255.255.255.255 10.1.0.1
169.254.169.254 255.255.255.255 10.1.0.1
224.0.0.0       240.0.0.0       0.0.0.0
224.0.0.0       240.0.0.0       0.0.0.0
255.255.255.255 255.255.255.255 0.0.0.0
255.255.255.255 255.255.255.255 0.0.0.0
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2008/09/16, Modification date: 2026/02/09

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active


```
 {"listening":
[{"port":445,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"cifs","plugin_output":n
{"port":139,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"smb","plugin_output":nul
{"port":135,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"epmap","plugin_output":n
{"port":49664,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"dce-
rpc","plugin_output":null},
{"port":49665,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"dce-
rpc","plugin_output":null},
{"port":49666,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"dce-
rpc","plugin_output":null},
{"port":49667,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"dce-
rpc","plugin_output":null},
{"port":49668,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"dce-
rpc","plugin_output":null},
{"port":49670,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"dce-
rpc","plugin_output":null},
{"port":0,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":"\nNes
 was able to find 25 open ports.\n"},
{"port":3389,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"msrdp","plugin_output":
{"port":5040,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nul
{"port":123,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":null
{"port":500,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":null
{"port":3389,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nul
{"port":4500,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nul
{"port":5050,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nul
{"port":5353,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nul
{"port":5355,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nul
{"port":49659,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nu
{"port":58391,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nu
{"port":62227,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nu
{"port":137,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":null
{"port":138,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":null
{"port":1900,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nul
{"port":49662,"protocol":"UDP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":nu
{"TCP":{"discrete":[49669],"ranges":[[1,134],[136,138],[140,444],[446,3388],[3390,5039],
[5041,49663],[49671,65535]]},"UDP":{"discrete":[5354],"ranges":[[1,122],[124,136],[139,499],
[501,1899],[1901,3388],[3390,4499],[4 [...]
```


48763 - Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting

Synopsis

CWDIllegalInDllSearch Settings: Improper settings could allow code execution attacks.

Description

Windows Hosts can be hardened against DLL hijacking attacks by setting the The 'CWDIllegalInDllSearch' registry entry in to one of the following settings:
- 0xFFFFFFFF (Removes the current working directory from the default DLL search order)
- 1 (Blocks a DLL Load from the current working directory if the current working directory is set to a WebDAV folder)
- 2 (Blocks a DLL Load from the current working directory if the current working directory is set to a remote folder)

See Also

http://www.nessus.org/u?0c574c56

http://www.nessus.org/u?5234ef0c

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2010/08/26, Modification date: 2019/12/20

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Name  : SYSTEM\CurrentControlSet\Control\Session Manager\CWDIllegalInDllSearch
Value : Registry Key Empty or Missing
```

48942 - Microsoft Windows SMB Registry : OS Version and Processor Architecture

Synopsis

It was possible to determine the processor architecture, build lab strings, and Windows OS version installed on the remote system.

Description

Nessus was able to determine the processor architecture, build lab strings, and the Windows OS version installed on the remote system by connecting to the remote registry with the supplied credentials.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2010/08/31, Modification date: 2022/02/01

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Operating system version = 10.26200
Architecture = x64
Build lab extended = 26100.1.amd64fre.ge_release.240331-1435
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2025/06/16

Ports
vm-win11-stig-s (TCP/3389) Vulnerability State: Active

```
This port supports TLSv1.3/TLSv1.0/TLSv1.1/TLSv1.2.
```

85736 - Windows Store Application Enumeration

Synopsis

It is possible to obtain the list of applications installed from the Windows Store.

Description

This plugin connects to the remote Windows host with the supplied credentials and uses WMI and Powershell to enumerate applications installed on the host from the Windows Store.

See Also

https://www.microsoft.com/en-us/store/apps

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2015/09/02, Modification date: 2026/02/09

Ports
vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
  -1527c705-839a-4832-9118-54d4Bd6a0c89
      Version : 10.0.19640.1000
      InstallLocation : C:\Windows\SystemApps\Microsoft.Windows.FilePicker_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -c5e2524a-ea46-4f67-841f-6a9465d9d515
      Version : 10.0.26100.1
      InstallLocation : C:\Windows\SystemApps\Microsoft.Windows.FileExplorer_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -E2A4F912-2574-4A75-9BB0-0D023378592B
      Version : 10.0.19640.1000
      InstallLocation : C:\Windows\SystemApps\Microsoft.Windows.AppResolverUX_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE
      Version : 10.0.26100.1
      InstallLocation : C:\Windows\SystemApps
\Microsoft.Windows.AddSuggestedFoldersToLibraryDialog_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -Microsoft.AAD.BrokerPlugin
      Version : 1000.19580.1000.2
      InstallLocation : C:\Windows\SystemApps\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -Microsoft.AccountsControl
      Version : 10.0.26100.1
      InstallLocation : C:\Windows\SystemApps\Microsoft.AccountsControl_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -Microsoft.AsyncTextService
      Version : 10.0.26100.1
      InstallLocation : C:\Windows\SystemApps\Microsoft.AsyncTextService_8wekyb3d8bbwe
      Architecture : Neutral
      Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
```

```
  -Microsoft.BioEnrollment
      Version : 10.0.19587.1000
 [...]
```

148541 - Windows Language Settings Detection

Synopsis

This plugin enumerates language files on a windows host.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates language IDs listed on the host.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2021/04/14, Modification date: 2022/02/01

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Default Install Language Code: 1033

Default Active Language Code: 1033

Other common microsoft Language packs may be scanned as well.
```

164690 - Windows Disabled Command Prompt Enumeration

Synopsis

This plugin determines if the DisableCMD policy is enabled or disabled on the remote host for each local user.

Description

The remote host may employ the DisableCMD policy on a per user basis. Enumerated local users may have the following registry key:
'HKLM\Software\Policies\Microsoft\Windows\System\DisableCMD'
- Unset or 0: The command prompt is enabled normally.
- 1: The command promt is disabled.
- 2: The command prompt is disabled however windows batch processing is allowed.

See Also

http://www.nessus.org/u?b40698bc

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2022/09/06, Modification date: 2026/01/26

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Username: DefaultAccount
  SID: S-1-5-21-2746855186-1286860024-2359785572-503
  DisableCMD: Unset

Username: Administrator
  SID: S-1-5-21-2746855186-1286860024-2359785572-1000
  DisableCMD: Unset

Username: WDAGUtilityAccount
  SID: S-1-5-21-2746855186-1286860024-2359785572-504
  DisableCMD: Unset
```

```
Username: tazdevil4
  SID: S-1-5-21-2746855186-1286860024-2359785572-500
  DisableCMD: Unset

Username: Guest
  SID: S-1-5-21-2746855186-1286860024-2359785572-501
  DisableCMD: Unset
```

193266 - Security Updates Outlook for Windows (April 2024)

Synopsis

The Microsoft Outlook application installed on the remote host is missing a security update.

Description

The Microsoft Outlook application installed on the remote host is missing a security update. It is, therefore, affected by a spoofing vulnerability. External attackers could send specially crafted emails that will cause a connection from the victim to an untrusted location of attackers' control. This will leak the Net-NTLMv2 hash of the victim to the untrusted network which an attacker can then relay to another service and authenticate as the victim.
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?02d9198f

Solution

Microsoft has released KB5002574 to address this issue.

Risk Factor

High

Vulnerability Priority Rating (VPR)

5.2

CVSS v3.0 Base Score

8.1 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

7.1 (E:U/RL:O/RC:C)

CVSS Base Score

9.4 (AV:N/AC:L/Au:N/C:C/I:C/A:N)

CVSS Temporal Score

7.0 (E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-20670
XREF	IAVA-2024-A-0225-S
XREF	MSFT-MS24-5002574
XREF	MSKB-5002574

Plugin Information:

Publication date: 2024/04/12, Modification date: 2024/07/30

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.OutlookForWindows_1.0.0.0_neutral__8wekyb3d8bbwe
  Installed version : 1.0.0.0
  Fixed version     : 1.2023.0322.0100
```

277654 - TLS Supported Groups

Synopsis

The remote service negotiates TLS supported curve groups.

Description

This plugin detects which TLS supported groups entries are supported by the remote service.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2025/12/08, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/3389) Vulnerability State: Active

```
These are the TLS supported groups offered by the remote server :


TLS supported groups :

Name                Code
--------------------------
secp256r1           0x0017
secp384r1           0x0018
x25519              0x001d
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

Vulnerability Priority Rating (VPR)

2.2

CVSS Base Score

2.1 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE-200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2024/10/07

Ports

vm-win11-stig-s (ICMP/0) Vulnerability State: Active

```
The ICMP timestamps seem to be in little endian format (not in network format)
The remote clock is synchronized with the local clock.
```

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2022/02/01

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Here are the SMB shares available on the remote host when logged in as tazdevil4:

  - ADMIN$
  - C$
  - D$
  - IPC$
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2025/06/16

Ports

vm-win11-stig-s (TCP/3389) Vulnerability State: Active

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=vm-win11-stig-s
|-Issuer  : CN=vm-win11-stig-s
```

63620 - Windows Product Key Retrieval

Synopsis

This plugin retrieves the Windows Product key of the remote Windows host.

Description

Using the supplied credentials, Nessus was able to obtain the retrieve the Windows host's partial product key'.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2013/01/18, Modification date: 2013/01/18

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
  Product key : XXXXX-XXXXX-XXXXX-XXXXX-T83GX

Note that all but the final portion of the key has been obfuscated.
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2021/02/03

Ports

vm-win11-stig-s (TCP/3389) Vulnerability State: Active

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                        Code            KEX           Auth     Encryption
MAC
```

```
   ----------------------        ----------       ---          ----     --------------------
---
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDHE        RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE        RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA          RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA          RSA      AES-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE        RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE        RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x3C       RSA          RSA      AES-CBC(128)
SHA256
   RSA-AES256-SHA256             0x00, 0x3D       RSA          RSA      AES-CBC(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

72482 - Windows Display Driver Enumeration

Synopsis

Nessus was able to enumerate one or more of the display drivers on the remote host.

Description

Nessus was able to enumerate one or more of the display drivers on the remote host via WMI.

See Also

http://www.nessus.org/u?b6e87533

Solution

N/A

Risk Factor

None

References

XREF	IAVT-0001-T-0756

Plugin Information:

Publication date: 2014/02/06, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
  Device Name         : Microsoft Hyper-V Video
  Driver File Version : 10.0.26100.1150
  Driver Date         : 06/21/2006

  Device Name         : Microsoft Remote Display Adapter
  Driver File Version : 10.0.26100.7705
  Driver Date         : 06/21/2006
```

92424 - MUICache Program Execution History

Synopsis

Nessus was able to enumerate recently executed programs on the remote host.

Description

Nessus was able to query the MUIcache registry key to find evidence of program execution.

See Also

https://forensicartifacts.com/2010/08/registry-muicache/

http://windowsir.blogspot.com/2005/12/mystery-of-muicachesolved.html

http://www.nirsoft.net/utils/muicache_view.html

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
 @%systemroot%\system32\drivers\wpdupfltr.sys,-100 : WPD Upper Class Filter Driver
@%systemroot%\system32\srvsvc.dll,-100 : Server
@tzres.dll,-352 : FLE Standard Time
@combase.dll,-5013 : The DCOMLAUNCH service launches COM and DCOM servers in response to object
 activation requests. If this service is stopped or disabled, programs using COM or DCOM will not
 function properly. It is strongly recommended that you have the DCOMLAUNCH service running.
@tzres.dll,-671 : AUS Eastern Daylight Time
@tzres.dll,-2980 : (UTC+03:00) Moscow, St. Petersburg
@%systemroot%\system32\axinstsv.dll,-103 : ActiveX Installer (AxInstSV)
@%systemroot%\system32\smphost.dll,-101 : Host service for the Microsoft Storage Spaces management
 provider. If this service is stopped or disabled, Storage Spaces cannot be managed.
@%systemroot%\system32\appxdeploymentserver.dll,-1 : AppX Deployment Service (AppXSVC)
@tzres.dll,-630 : (UTC+09:00) Osaka, Sapporo, Tokyo
@%systemroot%\system32\wlidsvc.dll,-100 : Microsoft Account Sign-in Assistant
@%systemroot%\system32\wcncsvc.dll,-3 : Windows Connect Now - Config Registrar
@%windir%\system32\drivers\pacer.sys,-101 : QoS Packet Scheduler
@%systemroot%\system32\refsdedupsvc.exe,-101 : ReFS data deduplication and compression service to
 track file changes and run scheduled optimization jobs.
@%systemroot%\system32\efssvc.dll,-100 : Encrypting File System (EFS)
@%systemroot%\system32\lltdres.dll,-6 : Link-Layer Topology Discovery Mapper I/O Driver
@tzres.dll,-252 : Dateline Standard Time
@tzres.dll,-401 : Arabic Daylight Time
@tzres.dll,-2890 : (UTC+02:00) Khartoum
@%systemroot%\system32\drivers\rdpdr.sys,-100 : Remote Desktop Device Redirector Driver
@tzres.dll,-82 : Atlantic Standard Time
@%systemroot%\system32\aphostres.dll,-10002 : Sync Host
@c:\windows\system32\rdpendp.dll,-1001 : Remote Audio
@tzres.dll,-620 : (UTC+09:00) Seoul
@%systemroot%\system32\devicesetupmanager.dll,-1000 : Device Setup Manager
@tzres.dll,-372 : Jerusalem Standard Time
@%systemroot%\system32\workfolderssvc.dll,-101 : This service [...]
```

117885 - Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but there were intermittent authentication failures.

Description

Nessus was able to successfully authenticate to the remote host on an authentication protocol at least once using credentials provided in the scan policy.
However, one or more plugins failed to authenticate to the remote host on the same port and protocol using the same credential set that was previously successful. This may indicate an intermittent authentication problem with the remote host, which could be caused by session rate limits, session concurrency limits, or other issues preventing consistent authentication success.
These intermittent authentication failures may have affected the results of some plugins. See plugin output for failure details.

Solution

N/A

Risk Factor

None

References

XREF	IAVB-0001-B-0509

Plugin Information:

Publication date: 2018/10/02, Modification date: 2024/03/25

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Nessus was able to successfully log into the remote host as :

User:       '10.1.0.115\tazdevil4'
Port:       445
Proto:      SMB
Method:     password


Successful authentication was reported by the following plugin :

  Plugin      : smb_login.nasl
  Plugin ID   : 10394
  Plugin Name : Microsoft Windows SMB Log In Possible

However, one or more subsequent plugins failed to authenticate to the
remote host on the same port and protocol using the same credential
set that previously succeeded. This may indicate an intermittent
authentication problem with the remote host which may have affected
the results of the following plugins.

Error message statistics :

  12 Failed to open a socket on port 445. This failure may have prevented
     a login attempt. The failure references the previously successful
     login account for tracking purposes.


Failure Details :

  - Plugin      : wix_win_installed.nbin
    Plugin ID   : 190558
    Plugin Name : Wix Toolset Installed (Windows)
    Message     :
Failed to open a socket on port 445. This failure may have prevented
a login attempt. The failure references the previously successful
login account for tracking purposes.


  - Plugin      : veritas_system_recovery_win_installed.nbin
    Plugin ID   : 198160
    Plugin Name : Veritas System Recovery Installed (Windows)
    Message     :
Failed to open a socket on port 445. This failure may have prevented
a login attempt. The failure references the previously successful
login account for tracking purposes.


  - Plugin      : telerik_ui_for_aspnet_ajax_installed.nbin
    Plugin ID   : 101160
    Plugin Name : Progress Telerik UI for ASP.NET AJAX Installed (Windows)
    Message     :
Failed to open a socket on port 445. This failure may have prevented
a login attempt. The failure references the previously successful
login account for tracking purposes.


  - Plugin      : srimax_output_messenger_win_installed.nbin
    Plugin ID   : 237652
    Plugin Name : Srimax Output Messenger Installed (Windows)
    Message     :
Failed [...]
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.
Please note the following :
- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2020/10/15, Modification date: 2024/03/25

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Nessus was able to log in to the remote host via the following :

User:       '10.1.0.115\tazdevil4'
Port:       445
Proto:      SMB
Method:     password
```

162560 - Microsoft Internet Explorer Installed

Synopsis

A web browser is installed on the remote Windows host.

Description

Microsoft Internet Explorer, a web browser bundled with Microsoft Windows, is installed on the remote Windows host.

See Also

https://support.microsoft.com/products/internet-explorer

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2022/06/28, Modification date: 2026/01/07

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Path    : C:\Windows\system32\mshtml.dll
Version : 11.0.26100.7705
```

171077 - SQLite Detection (Windows)

Synopsis

SQLite is installed on the remote Windows host.

Description

One or more instances of SQLite, a SQL database engine, is installed on the remote Windows host.
Note: Thorough tests is required for this plugin to run.

See Also

https://www.sqlite.org/

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2023/02/07, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Nessus detected 11 installs of SQLite:

  Path    : C:\Program Files\WindowsApps\Microsoft.WindowsStore_22512.1401.6.0_x64__8wekyb3d8bbwe
\e_sqlite3.dll
  Version : unknown

  Path    : C:\Windows\SystemApps\Shared
\e_sqlite3\39923CFDAD272169C217406A60214FFE9BD6C1B3BD396A3EFF94B781BD8D3376\e_sqlite3.dll
  Version : unknown

  Path    : C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\PersonaCardManager
\e_sqlite3.dll
  Version : unknown

  Path    : C:\Users\tazdevil4\AppData\Local\Microsoft\OneDrive
\26.012.0119.0002\FileSyncSqlite3.dll
  Version : 26.12.119.2

  Path    : C:\Program Files\WindowsApps\Microsoft.BingWeather_4.54.63029.0_x64__8wekyb3d8bbwe
\sqlite3.dll
  Version : 3.50.4.0

  Path    : C:\Program Files\WindowsApps\Microsoft.ZuneMusic_11.2512.10.0_x64__8wekyb3d8bbwe
\e_sqlite3.dll
  Version : unknown

  Path    : C:\Windows\SysWOW64\winsqlite3.dll
  Version : 3.51.1.0

  Path    : C:\Windows\SystemApps\Shared
\e_sqlite3\DCCBABB2BC7E7D4302C44D9CE41B70721A7D0914FA4D289E2F340D39766AD102\e_sqlite3.dll
  Version : unknown

  Path    : C:\Windows\System32\winsqlite3.dll
  Version : 3.51.1.0

  Path    : C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\ActionFXRuntime
\e_sqlite3.dll
  Version : unknown

  Path    : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe\sqlite3.dll
  Version : 3.46.1.0
```

178102 - Microsoft Windows Installed Software Version Enumeration

Synopsis

Enumerates installed software versions.

Description

This plugin enumerates the installed software version by interrogating information obtained from various registry entries and files on disk. This plugin provides a best guess at the software version and a confidence level for that version.

Note that the versions detected here do not necessarily indicate the actual installed version nor do they necessarily mean that the application is actually installed on the remote host. In some cases there may be artifacts left behind by uninstallers on the system.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2023/07/10, Modification date: 2024/07/15

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The following software information is available on the remote host :

 - Microsoft Edge WebView2 Runtime
     Best Confidence Version  : 145.0.3800.58
     Version Confidence Level : 3
     All Possible Versions    :  145.0.3800.58
     Other Version Data
       [InstallDate] :
           Raw Value           : 2026/02/17
       [DisplayIcon] :
           Raw Value           : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\145.0.3800.58\msedgewebview2.exe,0
           Parsed File Path    : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\145.0.3800.58\msedgewebview2.exe
           Parsed File Version : 145.0.3800.58
       [InstallLocation] :
           Raw Value           : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
       [UninstallString] :
           Raw Value           : "C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\145.0.3800.58\Installer\setup.exe" --uninstall --msedgewebview --system-level --verbose-logging
           Parsed File Path    : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\145.0.3800.58\Installer\setup.exe
           Parsed File Version : 145.0.3800.58
       [VersionMinor] :
           Raw Value           : 58
       [Version] :
           Raw Value           : 145.0.3800.58
       [VersionMajor] :
           Raw Value           : 3800
       [DisplayVersion] :
           Raw Value           : 145.0.3800.58
       [DisplayName] :
           Raw Value           : Microsoft Edge WebView2 Runtime

 - Microsoft Edge
     Best Confidence Version  : 145.0.3800.58
     Version Confidence Level : 3
     All Possible Versions    :  145.0.3800.58
     Other Version Data
       [InstallDate] :
           Raw Value           : 2026/02/17
       [DisplayIcon] :
           Raw Value           : C:\Program Files (x86)\Microsoft\Edge\Application
\145.0.3800.58\msedge.exe,0
           Parsed File Path    : C:\Program Files (x86)\Microsoft\Edge\Application
\145.0.3800.58\msedge.exe
           Parsed File Version : 145.0.3800.58
       [InstallLocation] [...]
```

200493 - Microsoft Windows Start Menu Software Version Enumeration

Synopsis

Enumerates Start Menu software versions.

Description

This plugin enumerates the installed software version by interrogating information obtained from various registry entries and files on disk. This plugin provides a best guess at the software version and a confidence level for that version.
Note that the versions detected here do not necessarily indicate the actual installed version nor do they necessarily mean that the application is actually installed on the remote host. In some cases there may be artifacts left behind by uninstallers on the system.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2024/06/13, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The following software information is available on the remote host :

- Microsoft Edge.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Microsoft Edge.lnk
    Target       : C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
    Version      : 145.0.3800.58

- Remote Desktop Connection.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\Remote
Desktop Connection.lnk
    Target       : C:\Windows\system32\mstsc.exe
    Version      : 10.0.26100.7705

- Steps Recorder.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\Steps
Recorder.lnk
    Target       : C:\Windows\system32\psr.exe
    Version      : 10.0.26100.7705

- Windows Media Player Legacy.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\Windows
Media Player Legacy.lnk
    Target       : C:\Program Files (x86)\Windows Media Player\wmplayer.exe
    Version      : 12.0.26100.1882

- Character Map.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\System Tools
\Character Map.lnk
    Target       : C:\Windows\system32\charmap.exe
    Version      : 5.2.3668.0

- Component Services.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Administrative Tools
\Component Services.lnk
    Target       : C:\Windows\system32\comexp.msc
    Version      : unknown

- Computer Management.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Administrative Tools
\Computer Management.lnk
    Target       : C:\Windows\system32\compmgmt.msc
    Version      : unknown

- dfrgui.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Administrative Tools
\dfrgui.lnk
    Target       : C:\Windows\system32\dfrgui.exe
    Version      : 10.0.26100.7019

- Disk Cleanup.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Administrative Tools
\Disk Cleanup.lnk
    Target       [...]
```

204960 - Windows System Driver Enumeration (Windows)

Synopsis

One or more kernel or file system drivers were enumerated on the remote Windows host.

Description

One or more kernel or file system drivers were enumerated on the remote Windows host.

See Also

http://www.nessus.org/u?43f8ab81

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2024/08/01, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Total : 397

  Name         : 1394ohci
  Path         : C:\Windows\system32\drivers\1394ohci.sys
  Service Type : Kernel Driver
  Description  : 1394 OHCI Compliant Host Controller
  State        : Stopped

  Name         : 3ware
  Path         : C:\Windows\system32\drivers\3ware.sys
  Service Type : Kernel Driver
  Description  : 3ware
  State        : Stopped

  Name         : ACPI
  Path         : C:\Windows\system32\drivers\ACPI.sys
  Service Type : Kernel Driver
  Description  : Microsoft ACPI Driver
  State        : Running

  Name         : AcpiAudioCompositorInbox
  Path         : C:\Windows\system32\DriverStore\FileRepository
\acpiaudiocompositor.inf_amd64_047f553a6f70b169\AcpiAudioCompositor.sys
  Service Type : Kernel Driver
  Description  : ACPI Audio Compositor Driver
  State        : Stopped

  Name         : AcpiDev
  Path         : C:\Windows\system32\drivers\AcpiDev.sys
  Service Type : Kernel Driver
  Description  : ACPI Devices driver
  State        : Stopped

  Name         : acpiex
  Path         : C:\Windows\system32\Drivers\acpiex.sys
  Service Type : Kernel Driver
  Description  : Microsoft ACPIEx Driver
  State        : Running

  Name         : acpipagr
  Path         : C:\Windows\system32\DriverStore\FileRepository
\acpipagr.inf_amd64_d1093347a27ff89c\acpipagr.sys
  Service Type : Kernel Driver
  Description  : ACPI Processor Aggregator Driver
  State        : Stopped

  Name         : AcpiPmi
  Path         : C:\Windows\system32\DriverStore\FileRepository
\acpipmi.inf_amd64_3ced06eb61dcc792\acpipmi.sys
  Service Type : Kernel Driver
  Description  : ACPI Power Meter Driver
```

```
  State        : Stopped

  Name         : acpitime
  Path         : C:\Windows\system32\drivers\acpitime.sys
  Service Type : Kernel Driver
  Description  : ACPI Wake Alarm Driver
  State        : Stopped

  Name         : Acx01000
  Path         : C:\Windows\system32\drivers\Acx01000.sys
  Service Type : Kernel Driver
  Description  : Acx01000
  State        : Stopped

  Name         : ADP80XX
  Path         : C:\Windows\system32\drivers\ADP80XX.SYS
[...]
```

264898 - Microsoft Teams for Desktop < 25163.3611.3774.6315 Elevation of Privilege (July 2025)

Synopsis

Microsoft Teams for Desktop is affected by an elevation of privilege vulnerability.

Description

The version of Microsoft Teams for Desktop on the remote Windows host is prior to 25163.3611.3774.6315 It is, therefore, affected by an elevation of privilege vulnerability:
- Improper handling of insufficient permissions or privileges in Microsoft Teams allows an authorized attacker to elevate privileges over a network. (CVE-2025-49731)
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?705592ec

Solution

Upgrade to Microsoft Teams for Desktop version 25163.3611.3774.6315 or later via the Microsoft Store.

Risk Factor

Low

Vulnerability Priority Rating (VPR)

2.2

CVSS v3.0 Base Score

3.1 (AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N)

STIG Severity

I

References

CVE	CVE-2025-49731
XREF	IAVA-2025-A-0493-S

Plugin Information:

Publication date: 2025/09/16, Modification date: 2025/10/29

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
  Path              : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.0.0
  Fixed version     : 25163.3611.3774.6315
```

10456 - Microsoft Windows SMB Service Enumeration

Synopsis

It is possible to enumerate remote services.

Description

This plugin implements the SvcOpenSCManager() and SvcEnumServices() calls to obtain, using the SMB protocol, the list of active and inactive services of the remote host.
An attacker may use this feature to gain better knowledge of the remote host.

Solution

To prevent the listing of the services from being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.

Risk Factor

None

References

XREF IAVT-0001-T-0751

Plugin Information:

Publication date: 2000/07/03, Modification date: 2022/02/01

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Active Services :

Application Identity [ AppIDSvc ]
Application Information [ Appinfo ]
AppX Deployment Service (AppXSVC) [ AppXSvc ]
Windows Audio Endpoint Builder [ AudioEndpointBuilder ]
Windows Audio [ Audiosrv ]
Base Filtering Engine [ BFE ]
Background Tasks Infrastructure Service [ BrokerInfrastructure ]
Capability Access Manager Service [ camsvc ]
Connected Devices Platform Service [ CDPSvc ]
Certificate Propagation [ CertPropSvc ]
CoreMessaging [ CoreMessagingRegistrar ]
Cryptographic Services [ CryptSvc ]
DCOM Server Process Launcher [ DcomLaunch ]
DHCP Client [ Dhcp ]
Connected User Experiences and Telemetry [ DiagTrack ]
Display Policy Service [ DispBrokerDesktopSvc ]
DNS Client [ Dnscache ]
Diagnostic Policy Service [ DPS ]
Data Usage [ DusmSvc ]
Windows Event Log [ EventLog ]
COM+ Event System [ EventSystem ]
Windows Font Cache Service [ FontCache ]
Guest Configuration Service [ GCService ]
IKE and AuthIP IPsec Keying Modules [ IKEEXT ]
Microsoft Store Install Service [ InstallService ]
Inventory and Compatibility Appraisal service [ InventorySvc ]
IP Helper [ iphlpsvc ]
CNG Key Isolation [ KeyIso ]
Server [ LanmanServer ]
Workstation [ LanmanWorkstation ]
Geolocation Service [ lfsvc ]
TCP/IP NetBIOS Helper [ lmhosts ]
Local Session Manager [ LSM ]
Windows Defender Firewall [ mpssvc ]
Network Connection Broker [ NcbService ]
Network List Service [ netprofm ]
Network Store Interface Service [ nsi ]
Program Compatibility Assistant Service [ PcaSvc ]
Performance Logs & Alerts [ pla ]
Plug and Play [ PlugPlay ]
IPsec Policy Agent [ PolicyAgent ]
Power [ Power ]
User Profile Service [ ProfSvc ]
RdAgent [ RdAgent ]
Remote Registry [ RemoteRegistry ]
Radio Management Service [ RmSvc ]
RPC Endpoint Mapper [ RpcEptMapper ]
Remote Procedure Call (RPC) [ RpcSs ]
Special Administration Console Helper [ sacsvr ]
Security Accounts Manager [ SamSs ]
```

```
Smart Card Device Enumeration Service [ ScDeviceEnum ]
Task Scheduler [ Schedule ]
Secondary Logon [ seclogon ]
Windows [...]
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2021/02/11

Ports

vm-win11-stig-s (TCP/139) Vulnerability State: Active

```
An SMB server is running on this port.
```

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
A CIFS server is running on this port.
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2025/06/03

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Remote operating system : Microsoft Windows 11 Pro Build 26200
Confidence level : 101
Method : Misc

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

ICMP:!::0:1:0:128:1:128:1:0:::0::1:X:X:X:X:X:X:X:X:X:1:1:128:65535:MNWST:8:1:1
SinFP:!:
   P1:B11113:F0x12:W65535:O0204ffff:M1410:
   P2:B11113:F0x12:W65535:O0204ffff010303080402080affffffff44454144:M1410:
   P3:B11121:F0x04:W0:O0:M0
   P4:191602_7_p=49666R
SSLcert:!:i/CN:vm-win11-stig-ss/CN:vm-win11-stig-s
c7b31d9144adf4092c80c08ac87de5566b68d3cf
```

```
The remote host is running Microsoft Windows 11 Pro Build 26200
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2005/03/30, Modification date: 2015/01/12

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The following password policy is defined on the remote host:

Minimum password len: 0
Password history len: 0
Maximum password age (d): 42
Password must meet complexity requirements: Enabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 600
Time between failed logon (s): 600
Number of invalid logon before locked out (s): 10
```

42897 - SMB Registry : Start the Registry Service during the scan (WMI)

Synopsis

The registry service was enabled for the duration of the scan.

Description

To perform a full credentialed scan, Nessus needs the ability to connect to the remote registry service (RemoteRegistry). If the service is down, this plugin will attempt to start for the duration of the scan.
For this plugin to work, you need to select the option 'Start the Remote Registry service during the scan' on the credentials page when you add your Windows credentials.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2009/11/25, Modification date: 2026/02/17

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
The registry service was successfully started for the duration of the scan.
```

44871 - WMI Windows Feature Enumeration

Synopsis

It is possible to enumerate Windows features using WMI.

Description

Nessus was able to enumerate the server features of the remote host by querying the 'Win32_ServerFeature' class of the '\Root\cimv2' WMI namespace for Windows Server versions or the 'Win32_OptionalFeature' class of the '\Root\cimv2' WMI namespace for Windows Desktop versions.
Note that Features can only be enumerated for Windows 7 and later for desktop versions.

See Also

https://msdn.microsoft.com/en-us/library/cc280268

https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/querying-the-status-of-optional-features

Solution

N/A

Risk Factor

None

References

XREF	IAVT-0001-T-0754

Plugin Information:

Publication date: 2010/02/24, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Nessus enumerated the following Windows features :

  - MSRDC-Infrastructure
  - MediaPlayback
  - NetFx4-AdvSrvs
  - Printing-Foundation-Features
  - Printing-Foundation-InternetPrinting-Client
  - Printing-PrintToPDFServices-Features
  - SearchEngine-Client-Package
  - SmbDirect
  - WCF-Services45
  - WCF-TCP-PortSharing45
  - Windows-Defender-Default-Definitions
  - WindowsMediaPlayer
  - WorkFolders-Client
```

51187 - WMI Encryptable Volume Enumeration

Synopsis

The remote Windows host has encryptable volumes available.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates encryptable volume information available on the remote host via WMI.

See Also

http://www.nessus.org/u?8aa7973e

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2010/12/15, Modification date: 2026/02/09

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Here is a list of encryptable volumes available on the remote system :

+ DriveLetter D:

  - Automatic Unlock : Disabled
  - BitLocker Version : None
  - Conversion Status : Fully Decrypted
  - DeviceID : \\?\Volume{f5d696c8-0000-0000-0000-100000000000}\
  - Encryption Method : None
```

```
  - Identification Field : None
  - Key Protectors : None Found
  - Lock Status : Unlocked
  - Percentage Encrypted : 0.0%
  - Protection Status : Protection Off
  - Size : 7.00 GB

+ DriveLetter C:

  - BitLocker Version : None
  - Conversion Status : Fully Decrypted
  - DeviceID : \\?\Volume{6d9af3a7-a496-4123-941b-3e2a99d6373d}\
  - Encryption Method : None
  - Identification Field : None
  - Key Protectors : None Found
  - Lock Status : Unlocked
  - Percentage Encrypted : 0.0%
  - Protection Status : Protection Off
  - Size : 126.45 GB
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2021/03/09

Ports

vm-win11-stig-s (TCP/3389) Vulnerability State: Active

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDHE         RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDHE         RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE         RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         RSA      AES-CBC(256)
 SHA384

The fields above are :
```

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

77668 - Windows Prefetch Folder

Synopsis

Nessus was able to retrieve the Windows prefetch folder file list.

Description

Nessus was able to retrieve and display the contents of the Windows prefetch folder (%systemroot%\prefetch*). This information shows programs that have run with the prefetch and superfetch mechanisms enabled.

See Also

http://www.nessus.org/u?8242d04f

http://www.nessus.org/u?d6b15983

http://www.forensicswiki.org/wiki/Prefetch

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2014/09/12, Modification date: 2018/11/15

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
 + HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
rootdirpath :
enableprefetcher : 3

+ Prefetch file list :
  - \Windows\prefetch\APPACTIONS.EXE-FDAFF098.pf
  - \Windows\prefetch\ATBROKER.EXE-8B8F7F7C.pf
  - \Windows\prefetch\AUDIODG.EXE-9848A323.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-0E2A6669.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-128FCAF6.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-1DF5D951.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-27DD6AFB.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-6C0BB8DC.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-D0E06976.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-2046E6BC.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-80328473.pf
  - \Windows\prefetch\BFETOOLWIN8.EXE-2486FDD5.pf
  - \Windows\prefetch\CMD.EXE-CD245F9E.pf
  - \Windows\prefetch\COLLECTGUESTLOGS.EXE-0E413307.pf
  - \Windows\prefetch\COMPATTELRUNNER.EXE-93B5AB09.pf
  - \Windows\prefetch\CONHOST.EXE-F98A1078.pf
  - \Windows\prefetch\CROSSDEVICERESUME.EXE-84F8AEDF.pf
  - \Windows\prefetch\CSRSS.EXE-A7A2B218.pf
  - \Windows\prefetch\CTFMON.EXE-5E6E7DF5.pf
  - \Windows\prefetch\DEFRAG.EXE-22AD8A37.pf
  - \Windows\prefetch\DIRECTXDATABASEUPDATER.EXE-B419FBAB.pf
  - \Windows\prefetch\DISMHOST.EXE-71696596.pf
  - \Windows\prefetch\DLLHOST.EXE-02F39419.pf
  - \Windows\prefetch\DLLHOST.EXE-2A97EA94.pf
  - \Windows\prefetch\DLLHOST.EXE-2F638E4F.pf
  - \Windows\prefetch\DLLHOST.EXE-38926D07.pf
  - \Windows\prefetch\DLLHOST.EXE-3C40F7FB.pf
  - \Windows\prefetch\DLLHOST.EXE-620FA5BD.pf
  - \Windows\prefetch\DLLHOST.EXE-6BABA3E7.pf
  - \Windows\prefetch\DLLHOST.EXE-9A24B39E.pf
  - \Windows\prefetch\DLLHOST.EXE-A8127979.pf
  - \Windows\prefetch\DLLHOST.EXE-B331F1D0.pf
```

```
  - \Windows\prefetch\DLLHOST.EXE-D6E392F8.pf
  - \Windows\prefetch\DLLHOST.EXE-F9D69405.pf
  - \Windows\prefetch\DWM.EXE-F29FE9E2.pf
  - \Windows\prefetch\EXPLORER.EXE-03C49D11.pf
  - \Windows\prefetch\FILECOAUTH.EXE-4AD02380.pf
  - \Windows\prefetch\FILECOAUTH.EXE-65C7FF02.pf
  - \Windows\prefetch\FILESYNCCONFIG.EXE-8257F9C3.pf
[...]
```

92370 - Microsoft Windows ARP Table

Synopsis

Nessus was able to collect and report ARP table information from the remote host.

Description

Nessus was able to collect ARP table information from the remote Windows host and generate a report as a CSV attachment.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2026/02/09

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
10.1.0.1 : 12-34-56-78-9a-bc
10.1.7.255 : ff-ff-ff-ff-ff-ff
224.0.0.22 : 01-00-5e-00-00-16
224.0.0.251 : 01-00-5e-00-00-fb
224.0.0.252 : 01-00-5e-00-00-fc
239.255.255.250 : 01-00-5e-7f-ff-fa
255.255.255.255 : ff-ff-ff-ff-ff-ff

Extended ARP table information attached.
```

92373 - Microsoft Windows SMB Sessions

Synopsis

Nessus was able to collect and report SMB session information from the remote host.

Description

Nessus was able to collect details of SMB sessions from the remote Windows host and generate a report as a CSV attachment.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2026/02/09

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
tazdevil4

Extended SMB session information attached.
```

92423 - Windows Explorer Recently Executed Programs

Synopsis

Nessus was able to enumerate recently executed programs on the remote host.

Description

Nessus was able to find evidence of program execution using Windows Explorer registry logs and settings.

See Also

http://www.forensicswiki.org/wiki/LastVisitedMRU

http://www.nessus.org/u?7e00b191

http://www.nessus.org/u?ac4dd3fb

http://www.nessus.org/u?c409cb41

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2019/08/15

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
a
wf.msc\1

 MRU programs details in attached report.
```

117887 - OS Security Patch Assessment Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

N/A

Risk Factor

None

References

XREF	IAVB-0001-B-0516

Plugin Information:

Publication date: 2018/10/02, Modification date: 2021/07/12

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
OS Security Patch Assessment is available.

Account  : 10.1.0.115\tazdevil4
Protocol : SMB
```

126527 - Microsoft Windows SAM user enumeration

Synopsis

Nessus was able to enumerate domain users from the local SAM.

Description

Using the domain security identifier (SID), Nessus was able to enumerate the domain users on the remote Windows system using the Security Accounts Manager.
Note: Unable to obtain SMB SAMR user data during Agent scans.
Rendering User data obtained by plugin 171956

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2019/07/08, Modification date: 2025/06/04

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
 - Administrator (id S-1-5-21-2746855186-1286860024-1000, Administrator)
 - DefaultAccount (id S-1-5-21-2746855186-1286860024-503, A user account managed by the system.)
 - Guest (id S-1-5-21-2746855186-1286860024-501, Built-in account for guest access to the
computer/domain, Guest account)
 - tazdevil4 (id S-1-5-21-2746855186-1286860024-500, Built-in account for administering the
computer/domain, Administrator account)
 - WDAGUtilityAccount (id S-1-5-21-2746855186-1286860024-504, A user account managed and used by
the system for Windows Defender Application Guard scenarios.)
```

151440 - Microsoft Windows Print Spooler Service Enabled

Synopsis

The Microsoft Windows Print Spooler service on the remote host is enabled.

Description

The Microsoft Windows Print Spooler service (spoolsv.exe) on the remote host is enabled.

See Also

http://www.nessus.org/u?8fc5df24

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2021/07/07, Modification date: 2021/07/07

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The Microsoft Windows Print Spooler service on the remote host is enabled.
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:
TLSv1.3:
- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256
TLSv1.2:
- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information:

Publication date: 2022/01/20, Modification date: 2024/02/12

Ports

vm-win11-stig-s (TCP/3389) Vulnerability State: Active

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    RSA-AES128-SHA256             0x00, 0x9C        RSA           RSA       AES-GCM(128)
SHA256
    RSA-AES256-SHA384             0x00, 0x9D        RSA           RSA       AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDHE         RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDHE         RSA       AES-CBC(256)
SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA       AES-CBC(128)
SHA1
    AES256-SHA                    0x00, 0x35        RSA           RSA       AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDHE         RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDHE         RSA       AES-CBC(256)
SHA384
    RSA-AES128-SHA256             0x00, 0x3C        RSA           RSA       AES-CBC(128)
SHA256
    RSA-AES256-SHA256             0x00, 0x3D        RSA           RSA       AES-CBC(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

161691 - The Microsoft Windows Support Diagnostic Tool (MSDT) RCE Workaround Detection (CVE-2022-30190)

Synopsis

Checks for the HKEY_CLASSES_ROOT\ms-msdt registry key.

Description

The remote host has the HKEY_CLASSES_ROOT\ms-msdt registry key. This is a known exposure for CVE-2022-30190.
Note that Nessus has not tested for CVE-2022-30190. It is only checking if the registry key exists. The recommendation is to apply the latest patch.

See Also

http://www.nessus.org/u?440e4ba1

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

http://www.nessus.org/u?b9345997

Solution

Apply the latest Cumulative Update.

Risk Factor

None

Plugin Information:

Publication date: 2022/05/31, Modification date: 2022/07/28

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The HKEY_CLASSES_ROOT\ms-msdt registry key exists on the target. This may indicate that the target
 is vulnerable to CVE-2022-30190, if the vendor patch is not applied.
```

166555 - WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

Synopsis

The remote Windows host is potentially missing a mitigation for a remote code execution vulnerability.

Description

The remote system may be in a vulnerable state to CVE-2013-3900 due to a missing or misconfigured registry keys:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config
\EnableCertPaddingCheck An unauthenticated, remote attacker could exploit this, by sending specially crafted requests, to execute arbitrary code on an affected host.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

http://www.nessus.org/u?9780b9d2

Solution

Add and enable registry value EnableCertPaddingCheck:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
Additionally, on 64 Bit OS systems, Add and enable registry value EnableCertPaddingCheck:
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config
\EnableCertPaddingCheck

Risk Factor

High

Vulnerability Priority Rating (VPR)

9.0

CVSS v3.0 Base Score

8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.4 (E:H/RL:O/RC:C)

CVSS Base Score

7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.6 (E:H/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2013-3900
XREF	CISA-KNOWN-EXPLOITED-2022/07/10
XREF	IAVA-2013-A-0227

Plugin Information:

Publication date: 2022/10/26, Modification date: 2025/12/17

Ports
vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Nessus detected the following potentially insecure registry key configuration:
   - Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the
registry.
   - Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not
present in the registry.
```

176212 - Microsoft Edge Add-on Enumeration (Windows)

Synopsis

One or more Microsoft Edge browser extensions are installed on the remote host.

Description

Nessus was able to enumerate Microsoft Edge browser extensions installed on the remote host.

See Also

https://microsoftedge.microsoft.com/addons

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2023/05/22, Modification date: 2026/02/03

Ports
vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
User : tazdevil4
|- Browser : Edge
  |- Add-on information :

    Name        : Google Docs Offline
    Description : Edit, create, and view your documents, spreadsheets, and presentations — all
 without internet access.
    Version     : 1.100.1
    Path        : C:\Users\tazdevil4\AppData\Local\Microsoft\Edge\User Data\Default\Extensions
\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.100.1_0

    Name        : Edge relevant text changes
    Description : Edge relevant text changes on select websites to improve user experience and
 precisely surfaces the action they want to take.
    Version     : 1.2.1
    Update Date : Feb. 17, 2026 at 01:52:53 GMT
    Path        : C:\Users\tazdevil4\AppData\Local\Microsoft\Edge\User Data\Default\Extensions
\jmjflgjpcpepeafmmgdpfkogkghcpiha\1.2.1_0
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2021/10/04

Ports

vm-win11-stig-s (TCP/49665) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49665 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49665
IP : 10.1.0.115
```

vm-win11-stig-s (TCP/49667) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49667 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
TCP Port : 49667
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49667
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49667
IP : 10.1.0.115
```

vm-win11-stig-s (TCP/49670) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49670 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49670
IP : 10.1.0.115
```

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\vm-win11-stig-s

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 01ceb31c-6da7-44f8-b93b-a390db4f0d97, version 1.0
```

```
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\vm-win11-stig-s

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\vm-win11-stig-s

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\vm-win11-stig-s

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\vm-win11-stig-s

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\vm-win11-stig-s

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\vm-win11-stig-s

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named [...]
```

vm-win11-stig-s (TCP/49666) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49666 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.115

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
```

```
TCP Port : 49666
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 29770a8f-829b-4158-90a2-78cd488501f7, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server [...]
```

vm-win11-stig-s (TCP/49668) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49668 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49668
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
```

```
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 10.1.0.115
```

vm-win11-stig-s (TCP/135) Vulnerability State: Active

```
The following DCERPC services are available locally :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : Vault

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : SidKey Local End Point

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsasspirpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsapolicylookup

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
```

```
Description : Unknown RPC service
Annotation : Ngc [...]
```

vm-win11-stig-s (TCP/49664) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49664 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49664
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49664
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 49664
IP : 10.1.0.115

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49664
IP : 10.1.0.115
```

10902 - Microsoft Windows 'Administrators' Group User List

Synopsis

There is at least one user in the 'Administrators' group.

Description

Using the supplied credentials, it is possible to extract the member list of the 'Administrators' group. Members of this group have complete access to the remote system.

Solution

Verify that each member of the group should have this type of access.

Risk Factor

None

Plugin Information:

Publication date: 2002/03/15, Modification date: 2018/05/16

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The following users are members of the 'Administrators' group :

  - vm-win11-stig-s\tazdevil4 (User)
  - vm-win11-stig-s\Administrator (User)
  - vm-win11-stig-s\Guest (User)
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2025/10/29

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Information about this scan :

Nessus version : 10.11.2
Nessus build : 20042
Plugin feed version : 202602170907
Scanner edition used : Nessus
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Disa-Scan-Win-11-Fred
Scan policy used : Fred-Win-11-Stig-Scan-Template
Scanner IP : 10.0.0.8
Port scanner(s) : wmi_netstat
Port range : default
Ping RTT : 15.628 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as '10.1.0.115\tazdevil4' via SMB
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2026/2/17 23:04 UTC
Scan duration : 3672 sec
Scan for malware : no
```

23974 - Microsoft Windows SMB Share Hosting Office Files

Synopsis

The remote share contains Office-related files.

Description

This plugin connects to the remotely accessible SMB shares and attempts to find office related files (such as .doc, .ppt, .xls, .pdf etc).

Solution

Make sure that the files containing confidential information have proper access controls set on them.

Risk Factor

None

Plugin Information:

Publication date: 2007/01/04, Modification date: 2011/03/21

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Here is a list of office files which have been found on the remote SMB
shares :

  + C$ :

    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.26100.5074_none_b413a7fad9bdd241\MsoIrmProtector.doc
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.26100.1_none_151382ec926a1266\MsoIrmProtector.doc
    - C:\Windows\WinSxS\amd64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.26100.5074_none_a9befda8a55d1046\MsoIrmProtector.doc
    - C:\Windows\SysWOW64\MSDRM\MsoIrmProtector.doc
    - C:\Windows\System32\MSDRM\MsoIrmProtector.doc
    - C:\Windows\System32\en-US\Licenses\_Default\IoTEnterpriseK\license.rtf
    - C:\Windows\System32\en-US\Licenses\_Default\Professional\license.rtf
    - C:\Windows\System32\en-US\lpeula.rtf
    - C:\Windows\System32\Licenses\neutral\_Default\IoTEnterpriseK\license.rtf
    - C:\Windows\System32\Licenses\neutral\_Default\Professional\de-license.rtf
    - C:\Windows\System32\Licenses\neutral\_Default\Professional\license.rtf
    - C:\Windows\System32\Licenses\neutral\OEM\IoTEnterprise\license.rtf
    - C:\Windows\System32\oobe\en-US\OOBE_HELP_Opt_in_Details.rtf
    - C:\Windows\System32\oobe\en-US\privacy.rtf
    - C:\Windows\System32\oobe\en-US\vofflps.rtf
    - C:\Windows\SysWOW64\en-US\Licenses\_Default\IoTEnterpriseK\license.rtf
    - C:\Windows\SysWOW64\en-US\Licenses\_Default\Professional\license.rtf
    - C:\Windows\SysWOW64\en-US\lpeula.rtf
    - C:\Windows\SysWOW64\Licenses\neutral\_Default\IoTEnterpriseK\license.rtf
    - C:\Windows\SysWOW64\Licenses\neutral\_Default\Professional\de-license.rtf
    - C:\Windows\SysWOW64\Licenses\neutral\_Default\Professional\license.rtf
    - C:\Windows\SysWOW64\Licenses\neutral\OEM\IoTEnterprise\license.rtf
    - C:\Windows\WinSxS\amd64_microsoft-windows-
h..indetails.resources_31bf3856ad364e35_10.0.26100.1_en-
us_fb9ab23dbd81f789\OOBE_HELP_Opt_in_Details.rtf
    - C:\Windows\WinSxS\amd64_microsoft-windows-
h..learnmore.resources_31bf3856ad364e35_10.0.26100.1_en-
us_c10f0a9707273178\OOBE_HELP_Cortana_Learn_More.rtf
 [...]
```

24269 - WMI Available

Synopsis

WMI queries can be made against the remote host.

Description

The supplied credentials can be used to make WMI (Windows Management Instrumentation) requests against the remote host over DCOM.
These requests can be used to gather information about the remote host, such as its current state, network interface configuration, etc.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2007/02/03, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The remote host returned the following caption from Win32_OperatingSystem:

 Microsoft Windows 11 Pro
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2023/10/17

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Synopsis

It is possible to obtain the network name of the remote host.

Description

The remote host listens on tcp port 445 and replies to SMB requests.
By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2009/11/06, Modification date: 2019/11/22

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The following 2 NetBIOS names have been gathered :

 vm-win11-stig-s  = Computer name
 vm-win11-stig-s  = Workgroup / Domain name
```

44401 - Microsoft Windows SMB Service Config Enumeration

Synopsis

It was possible to enumerate configuration parameters of remote services.

Description

Nessus was able to obtain, via the SMB protocol, the launch parameters of each active service on the remote host (executable path, logon type, etc.).

Solution

Ensure that each service is configured properly.

Risk Factor

None

References

XREF	IAVT-0001-T-0752

Plugin Information:

Publication date: 2010/02/05, Modification date: 2022/05/16

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The following services are set to start automatically :

  AppXSvc startup parameters :
    Display name : AppX Deployment Service (AppXSVC)
    Service name : AppXSvc
    Log on as : LocalSystem
    Executable path : C:\Windows\system32\svchost.exe -k wsappx -p
    Dependencies : rpcss/staterepository/

  AudioEndpointBuilder startup parameters :
    Display name : Windows Audio Endpoint Builder
    Service name : AudioEndpointBuilder
    Log on as : LocalSystem
    Executable path : C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p

  Audiosrv startup parameters :
    Display name : Windows Audio
    Service name : Audiosrv
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
    Dependencies : AudioEndpointBuilder/RpcSs/

  BFE startup parameters :
    Display name : Base Filtering Engine
    Service name : BFE
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
    Dependencies : RpcSs/

  BrokerInfrastructure startup parameters :
    Display name : Background Tasks Infrastructure Service
    Service name : BrokerInfrastructure
    Log on as : LocalSystem
    Executable path : C:\Windows\system32\svchost.exe -k DcomLaunch -p
    Dependencies : RpcEptMapper/DcomLaunch/RpcSs/

  CDPSvc startup parameters :
    Display name : Connected Devices Platform Service
    Service name : CDPSvc
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\system32\svchost.exe -k LocalService -p
    Dependencies : ncbservice/RpcSS/Tcpip/

  CDPUserSvc_c3f54 startup parameters :
    Display name : Connected Devices Platform User Service_c3f54
    Service name : CDPUserSvc_c3f54
    Executable path : C:\Windows\system32\svchost.exe -k UnistackSvcGroup

  CoreMessagingRegistrar startup parameters :
    Display name : CoreMessaging
    Service name : CoreMessagingRegistrar
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\system32\svchost.exe [...]
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2026/01/05

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_11 -> Microsoft Windows 11

Following application CPE's matched on the remote system :

  cpe:/a:haxx:curl:8.16.0.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:8.10.1.0 -> Haxx libcurl
  cpe:/a:microsoft:.net_framework:4.8.1 -> Microsoft .NET Framework
  cpe:/a:microsoft:edge:145.0.3800.58 -> Microsoft Edge
  cpe:/a:microsoft:ie:11.1882.26100.0 -> Microsoft Internet Explorer
  cpe:/a:microsoft:internet_explorer:11.0.26100.7705 -> Microsoft Internet Explorer
  cpe:/a:microsoft:onedrive:26.12.119.2 -> Microsoft OneDrive
  cpe:/a:microsoft:remote_desktop_connection:10.0.26100.7705 -> Microsoft Remote Desktop
 Connection
  cpe:/a:microsoft:system_center_endpoint_protection:4.18.26010.5 -> Microsoft System Center
 Endpoint Protection
  cpe:/a:microsoft:windows_defender:4.18.26010.5 -> Microsoft Windows Defender
  cpe:/a:sqlite:sqlite -> SQLite
  cpe:/a:sqlite:sqlite:26.12.119.2 -> SQLite
  cpe:/a:sqlite:sqlite:3.46.1.0 -> SQLite
  cpe:/a:sqlite:sqlite:3.50.4.0 -> SQLite
  cpe:/a:sqlite:sqlite:3.51.1.0 -> SQLite
  x-cpe:/a:microsoft:azure_guest_agent:2.7.41491.1183
```

52001 - WMI QuickFixEngineering (QFE) Enumeration

Synopsis

The remote Windows host has quick-fix engineering updates installed.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via WMI.

See Also

http://www.nessus.org/u?0c4ec249

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/02/16, Modification date: 2026/01/20

Ports
vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Here is a list of quick-fix engineering updates installed on the
remote system :

+ KB5066128
  - Description : Update
  - InstalledOn : 2/6/2026

+ KB5054156
  - Description : Update
  - InstalledOn : 2/6/2026

+ KB5077181
  - Description : Security Update
  - InstalledOn : 2/6/2026

+ KB5077869
  - Description : Security Update
  - InstalledOn : 2/6/2026

Note that for detailed information on installed QFE's such as InstalledBy, Caption,
and so on, please run the scan with 'Report Verbosity' set to 'verbose'.
```

66424 - Microsoft Malicious Software Removal Tool Installed

Synopsis

An antimalware application is installed on the remote Windows host.

Description

The Microsoft Malicious Software Removal Tool is installed on the remote host. This tool is an application that attempts to detect and remove known malware from Windows systems.

See Also

http://www.nessus.org/u?47a3e94d

https://support.microsoft.com/en-us/help/891716

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2013/05/15, Modification date: 2023/01/10

Ports
vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
  File                : C:\Windows\system32\MRT.exe
  Version             : 5.139.26020.1001
  Release at last run : unknown
  Report infection information to Microsoft : Yes
```

92415 - Application Compatibility Cache

Synopsis

Nessus was able to gather application compatibility settings on the remote host.

Description

Nessus was able to generate a report on the application compatibility cache on the remote Windows host.

See Also

https://dl.mandiant.com/EE/library/Whitepaper_ShimCacheParser.pdf

http://www.nessus.org/u?4a076105

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Application compatibility cache report attached.
```

103871 - Microsoft Windows Network Adapters

Synopsis

Identifies the network adapters installed on the remote host.

Description

Using the supplied credentials, this plugin enumerates and reports the installed network adapters on the remote Windows host.

Solution

Make sure that all of the installed network adapters agrees with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF	IAVT-0001-T-0758

Plugin Information:

Publication date: 2017/10/17, Modification date: 2022/02/01

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Network Adapter Driver Description : Mellanox ConnectX-5 Virtual Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-5 Virtual Adapter
Network Adapter Driver Version     : 23.4.26054.1
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2018/02/09, Modification date: 2020/03/11

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
The remote host supports the following SMB dialects :
 _version_  _introduced in windows version_
 2.0.2      Windows 2008
```

```
 2.1        Windows 7
 3.0        Windows 8
 3.0.2      Windows 8.1
 3.1.1      Windows 10

The remote host does NOT support the following SMB dialects :
 _version_  _introduced in windows version_
 2.2.2      Windows 8 Beta
 2.2.4      Windows 8 Beta
 3.1        Windows 10
```

125835 - Microsoft Remote Desktop Connection Installed

Synopsis

A graphical interface connection utility is installed on the remote Windows host

Description

Microsoft Remote Desktop Connection (also known as Remote Desktop Protocol or Terminal Services Client) is installed on the remote Windows host.

See Also

http://www.nessus.org/u?1c33f0e7

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2019/06/12, Modification date: 2022/10/10

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Path    : C:\Windows\\System32\\mstsc.exe
Version : 10.0.26100.7705
```

138603 - Microsoft OneDrive Installed

Synopsis

A file hosting application is installed on the remote host.

Description

Microsoft OneDrive, a file hosting service, is installed on the remote host.

See Also

http://www.nessus.org/u?23c14184

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2020/07/17, Modification date: 2026/01/07

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Path    : C:\Users\tazdevil4\AppData\Local\Microsoft\OneDrive\
Version : 26.12.119.2
```

139785 - DISM Package List (Windows)

Synopsis

Use DISM to extract package info from the host.

Description

Using the Deployment Image Servicing Management tool, this plugin enumerates installed packages.

See Also

http://www.nessus.org/u?cbb428b2

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2020/08/25, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
 The following packages were enumerated using the Deployment Image Servicing and Management Tool:

Package      : Microsoft-OneCore-ApplicationModel-Sync-Desktop-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State        : Staged
Release Type : OnDemand Pack
Install Time :

Package      : Microsoft-OneCore-ApplicationModel-Sync-Desktop-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.7824
State        : Installed
Release Type : OnDemand Pack
Install Time : 2/6/2026 11:03 PM

Package      : Microsoft-OneCore-DirectX-Database-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State        : Staged
Release Type : OnDemand Pack
Install Time :

Package      : Microsoft-OneCore-DirectX-Database-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.7824
State        : Installed
Release Type : OnDemand Pack
Install Time : 2/6/2026 11:03 PM

Package      : Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~10.0.26100.1742
State        : Staged
Release Type : Language Pack
Install Time :

Package      : Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~10.0.26100.7840
State        : Installed
Release Type : Language Pack
Install Time : 2/6/2026 11:03 PM

Package      : Microsoft-Windows-EMS-SAC-Desktop-Tools-FoD-Package~31bf3856ad364e35~amd64~en-
US~10.0.26100.1742
State        : Staged
Release Type : OnDemand Pack
Install Time :

Package      : Microsoft-Windows-EMS-SAC-Desktop-Tools-FoD-Package~31bf3856ad364e35~amd64~en-
US~10.0.26100.7824
State        : Installed
Release Type : OnDemand Pack
Install Time : 2/7/2026 12:11 AM

Package      : Microsoft-Windows-EMS-SAC-Desktop-Tools-FoD-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State        : Staged
Release Type : OnDemand Pack
Install Time :
```

```
Package      : Microsoft-Windows-EMS-SAC-Desktop-Tools-FoD-
Package~31bf3856ad364e35~amd64~~10.0.26100.7824
State        : Installed
Release Type : OnDemand Pack
Install Time : 2/7/2026 12:11 AM

Package      : Microsoft-Windows-Ethernet-Client-Intel-E1i68x64-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State [...]
```

159817 - Windows Credential Guard Status

Synopsis

Retrieves the status of Windows Credential Guard.

Description

Retrieves the status of Windows Credential Guard.
Credential Guard prevents attacks such as such as Pass-the-Hash or Pass-The-Ticket by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials.

See Also

http://www.nessus.org/u?fb8c8c37

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2022/04/18, Modification date: 2023/08/25

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Windows Credential Guard is not fully enabled.
The following registry keys have not been set :
  - System\CurrentControlSet\Control\DeviceGuard\RequirePlatformSecurityFeatures : Key not found.
  - System\CurrentControlSet\Control\LSA\LsaCfgFlags : Key not found.
  - System\CurrentControlSet\Control\DeviceGuard\EnableVirtualizationBasedSecurity : Key not
 found.
```

171860 - Curl Installed (Windows)

Synopsis

Curl is installed on the remote Windows host.

Description

Curl, a command line tool for transferring data with URLs, was detected on the remote Windows host.
Please note, if the installation is located in either the Windows\System32 or Windows\SysWOW64 directory, it will be considered as managed by the OS. In this case, paranoid scanning is require to trigger downstream vulnerabilty checks. Paranoid scanning has no affect on this plugin itself.

See Also

https://curl.se/

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2023/02/23, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Nessus detected 2 installs of Curl:
```

```
Path          : c:\windows\system32\curl.exe
Version       : 8.16.0.0
Managed by OS : True

Path          : c:\windows\syswow64\curl.exe
Version       : 8.16.0.0
Managed by OS : True
```

182962 - libcurl Installed (Windows)

Synopsis

libcurl is installed on the remote Windows host.

Description

libcurl, a library used for transferring data with URLs, was detected on the remote Windows host.

See Also

https://libcurl.se/

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2023/10/12, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Path    : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe\libcurl.dll
Version : 8.10.1.0
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2025/02/26, Modification date: 2025/03/03

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Following OS Fingerprints were found

Remote operating system : Microsoft Windows Server 2025
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Microsoft Windows 11 Pro Build 26200
Confidence level : 101
Method : Misc
Type : general-purpose
Fingerprint : unknown

Remote operating system : Microsoft Windows 11 Pro Build 26200
```

```
Confidence level : 100
Method : SMB_OS
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
 ICMP:!::0:1:0:128:1:128:1:0:::0::1:X:X:X:X:X:X:X:X:X:1:1:128:65535:MNWST:8:1:1
SinFP:!:
   P1:B11113:F0x12:W65535:O0204ffff:M1410:
   P2:B11113:F0x12:W65535:O0204ffff010303080402080affffffff44454144:M1410:
   P3:B11121:F0x04:W0:O0:M0
   P4:191602_7_p=49666R
SSLcert:!:i/CN:vm-win11-stig-ss/CN:vm-win11-stig-s
c7b31d9144adf4092c80c08ac87de5566b68d3cf
```

57033 - Microsoft Patch Bulletin Feasibility Check

Synopsis

Nessus is able to check for Microsoft patch bulletins.

Description

Using credentials supplied in the scan policy, Nessus is able to collect information about the software and patches installed on the remote Windows host and will use that information to check for missing Microsoft security updates. Note that this plugin is purely informational.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/12/06, Modification date: 2021/07/12

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Nessus is able to test for missing patches using :
  Nessus
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2015/10/16, Modification date: 2025/06/10

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
The following is a consolidated list of detected MAC addresses:
  - 7C:1E:52:B3:C4:B3
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2025/03/12

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Remote device type : general-purpose
Confidence level : 101
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/10/12, Modification date: 2018/06/19

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
20260217223822.791629+000
```

159929 - Windows LSA Protection Status

Synopsis

Windows LSA Protection is disabled on the remote Windows host.

Description

The LSA Protection validates users for local and remote sign-ins and enforces local security policies to prevent reading memory and code injection by non-protected processes. This provides added security for the credentials that the LSA stores and manages. This protects against Pass-the-Hash or Mimikatz-style attacks.

Solution

Enable LSA Protection per your corporate security guidelines.

Risk Factor

None

Plugin Information:

Publication date: 2022/04/20, Modification date: 2025/06/16

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
LSA Protection is enabled (without UEFI).
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2021/02/03

Ports

vm-win11-stig-s (TCP/3389) Vulnerability State: Active

```
 Subject Name:

Common Name: vm-win11-stig-s

Issuer Name:

Common Name: vm-win11-stig-s

Serial Number: 17 84 0C A2 1A 17 00 AF 4B 03 33 4C 9E E0 56 33

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 16 00:32:37 2026 GMT
Not Valid After: Aug 18 00:32:37 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C4 85 65 BF EE 50 89 58 84 13 94 ED B0 54 FF 15 D0 5C 82
            E1 7B DF 08 42 6C F1 08 1A 4E 42 CB 9A 6A 30 EE 14 6F EC AA
            E0 A9 8E B4 89 63 3F 80 B8 82 C6 34 FD 11 A9 5E FA D2 B0 B6
            0D 8F 79 AE F3 74 22 16 F7 77 10 8B C5 B8 86 55 B7 12 DA 97
            E6 42 7C 42 93 A7 A6 AB 97 AB 5F AA 4A 92 CA 46 DC 6A F8 ED
            1D 99 9F 29 32 BB E5 F7 22 D7 8A 96 F0 EF DE 83 1A A4 30 41
            9A 00 F3 DA 98 AB 05 1F B1 12 F7 7F 46 36 50 4A C8 6A 4E A7
            4B 5C 8A 11 40 5A DE B8 5A F4 9A 6F 49 43 37 43 CF 87 F3 66
            18 09 C8 A9 DB 1B 95 80 B9 7E 91 BB 30 F6 5E 84 B7 73 38 9F
            B7 8E 7A 33 6B B4 21 D1 A8 F6 1E D8 2B 46 68 97 38 A3 79 69
            79 6A 01 C8 1D 36 9A 37 61 E8 D8 09 77 1D EF 22 AA 19 1C 86
            13 53 A6 69 F1 E2 E5 A7 DC B6 96 A4 64 07 44 C0 00 AB 54 C9
            92 26 FD A2 03 0F 43 51 DA F0 7E 55 DA 62 E0 FD 95
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 84 0F C0 3A BB C9 B6 99 07 8F FD A7 3B A6 14 0A D5 A8 B3
           DA A5 27 7E 03 F7 DC 87 21 63 1C 7D 37 2C BB 3F 72 46 D6 71
           19 4D F5 A1 52 3E B4 CD 35 E0 BE 1F 06 AC 21 F3 74 DD 8A 23
           44 62 04 66 FE 48 9D 16 E9 52 0D 3A 53 0D F7 91 B2 A8 45 E9
           81 06 BF 9A C4 BB BF CC F8 17 48 CD 43 DB A9 E3 7D 2D CD F7
           38 43 68 CE C0 65 A4 51 12 13 D5 07 FD EE 1D 98 A1 13 91 15
           E9 99 E2 8F 0B 65 AC 74 54 9F 1B 9B FB 81 A3 8C 2B 14 98 F9
           A7 33 69 AB E0 AA A3 D7 50 77 17 EC B0 7D 14 26 BE CB 95 C8
           8D 7C C9 CD BD CF C5 33 E0 08 1E A8 AA D9 25 7B 7A 06 9D 90
           15 81 AA 09 D9 F9 [...]
```

34096 - BIOS Info (WMI)

Synopsis

The BIOS info could be read.

Description

It is possible to get information about the BIOS via the host's WMI interface.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2008/09/05, Modification date: 2026/01/20

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
Vendor       : Microsoft Corporation
Version      : Hyper-V UEFI Release v4.1
Release date : 20250610000000.000000+000
UUID         : F5D696C8-D220-4F75-B947-BD9723F57732
Secure boot  : disabled
```

161502 - Microsoft Windows Logged On Users

Synopsis

Nessus was able to determine the logged on users from the registry

Description

Using the HKU registry, Nessus was able to enumerate the SIDs of logged on users

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2022/05/25, Modification date: 2025/10/01

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Logged on users :
  - S-1-5-21-2746855186-1286860024-2359785572-500
    Domain   : vm-win11-stig-s
    Username : tazdevil4
```

51351 - Microsoft .NET Framework Detection

Synopsis

A software framework is installed on the remote host.

Description

Microsoft .NET Framework, a software framework for Microsoft Windows operating systems, is installed on the remote host.

See Also

https://www.microsoft.com/net

http://www.nessus.org/u?15ae6806

Solution

N/A

Risk Factor

None

References

XREF	IAVT-0001-T-0655

Plugin Information:

Publication date: 2010/12/20, Modification date: 2025/10/15

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
Nessus detected 2 installs of Microsoft .NET Framework:
```

```
Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
Version      : 4.8.1
Full Version : 4.8.09221
Install Type : Full
Release      : 533509

Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
Version      : 4.8.1
Full Version : 4.8.09221
Install Type : Client
Release      : 533509
```

92369 - Microsoft Windows Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Windows host and generate a report as a CSV attachment.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2023/06/06

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\TimeZoneKeyName : UTC
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardName : @tzres.dll,-932
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightName : @tzres.dll,-931
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DynamicDaylightTimeDisabled : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardBias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightBias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\Bias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightStart :
 00000000000000000000000000000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardStart :
 00000000000000000000000000000000
```

92429 - Recycle Bin Files

Synopsis

Nessus was able to enumerate files in the recycle bin on the remote host.

Description

Nessus was able to generate a list of all files found in $Recycle.Bin subdirectories.

See Also

http://www.nessus.org/u?0c1a03df

http://www.nessus.org/u?61293b38

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

vm-win11-stig-s (TCP/0) Vulnerability State: Active

```
C:\\$Recycle.Bin\\.
C:\\$Recycle.Bin\\..
```

```
C:\\$Recycle.Bin\\S-1-5-18
C:\\$Recycle.Bin\\S-1-5-21-2746855186-1286860024-2359785572-500
C:\\$Recycle.Bin\\S-1-5-21-3754889540-2232864964-3060716865-500
C:\\$Recycle.Bin\\S-1-5-18\.
C:\\$Recycle.Bin\\S-1-5-18\..
C:\\$Recycle.Bin\\S-1-5-18\desktop.ini
C:\\$Recycle.Bin\\S-1-5-21-2746855186-1286860024-2359785572-500\.
C:\\$Recycle.Bin\\S-1-5-21-2746855186-1286860024-2359785572-500\..
C:\\$Recycle.Bin\\S-1-5-21-2746855186-1286860024-2359785572-500\desktop.ini
C:\\$Recycle.Bin\\S-1-5-21-3754889540-2232864964-3060716865-500\.
C:\\$Recycle.Bin\\S-1-5-21-3754889540-2232864964-3060716865-500\..
C:\\$Recycle.Bin\\S-1-5-21-3754889540-2232864964-3060716865-500\desktop.ini
```

160486 - Server Message Block (SMB) Protocol Version Detection

Synopsis

Verify the version of SMB on the remote host.

Description

The Server Message Block (SMB) Protocol provides shared access to files and printers across nodes on a network.

See Also

http://www.nessus.org/u?f463096b

http://www.nessus.org/u?1a4b3744

Solution

Disable SMB version 1 and block all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

Risk Factor

None

Plugin Information:

Publication date: 2022/05/04, Modification date: 2022/05/04

Ports

vm-win11-stig-s (TCP/445) Vulnerability State: Active

```
- SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB2 : Key not found.
- SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB3 : Key not found.
- SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB1 : Key not found.
```

Assets Summary (Executive)

vm-win11-stig-s

Summary

Critical	High	Medium	Low	Info	Total
0	3	2	2	124	131

Details

Severity	Plugin Id	Name
High	193266	Security Updates Outlook for Windows (April 2024)
High	250276	Microsoft Teams for Desktop < 25122.1415.3698.6812 Remote Code Execution (August 2025)
High	166555	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)
Medium	57582	SSL Self-Signed Certificate
Medium	51192	SSL Certificate Cannot Be Trusted
Low	10114	ICMP Timestamp Request Remote Date Disclosure
Low	264898	Microsoft Teams for Desktop < 25163.3611.3774.6315 Elevation of Privilege (July 2025)
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	136969	Microsoft Edge Chromium Installed
Info	66334	Patch Report
Info	139785	DISM Package List (Windows)
Info	92365	Microsoft Windows Hosts File
Info	56984	SSL / TLS Versions Supported
Info	92366	Microsoft Windows Last Boot Time
Info	164690	Windows Disabled Command Prompt Enumeration
Info	176212	Microsoft Edge Add-on Enumeration (Windows)
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	72367	Microsoft Internet Explorer Version Detection
Info	25220	TCP/IP Timestamps Supported
Info	19506	Nessus Scan Information
Info	171077	SQLite Detection (Windows)
Info	92434	User Download Folder Files
Info	11457	Microsoft Windows SMB Registry : Winlogon Cached Password Weakness
Info	162174	Windows Always Installed Elevated Status

Info	63620	Windows Product Key Retrieval
Info	44871	WMI Windows Feature Enumeration
Info	155963	Windows Printer Driver Enumeration
Info	57033	Microsoft Patch Bulletin Feasibility Check
Info	85736	Windows Store Application Enumeration
Info	44401	Microsoft Windows SMB Service Config Enumeration
Info	48337	Windows ComputerSystemProduct Enumeration (WMI)
Info	277654	TLS Supported Groups
Info	159929	Windows LSA Protection Status
Info	92431	User Shell Folders Settings
Info	10400	Microsoft Windows SMB Registry Remotely Accessible
Info	125835	Microsoft Remote Desktop Connection Installed
Info	52001	WMI QuickFixEngineering (QFE) Enumeration
Info	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
Info	56468	Time of Last System Startup
Info	63080	Microsoft Windows Mounted Devices
Info	171860	Curl Installed (Windows)
Info	24269	WMI Available
Info	92370	Microsoft Windows ARP Table
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	92435	UserAssist Execution History
Info	42897	SMB Registry : Start the Registry Service during the scan (WMI)
Info	24272	Network Interfaces Enumeration (WMI)
Info	277650	Remote Services Not Using Post-Quantum Ciphers
Info	20811	Microsoft Windows Installed Software Enumeration (credentialed check)
Info	126527	Microsoft Windows SAM user enumeration
Info	70329	Microsoft Windows Process Information
Info	151440	Microsoft Windows Print Spooler Service Enabled
Info	38689	Microsoft Windows SMB Last Logged On User Disclosure
Info	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
Info	58181	Windows DNS Server Enumeration

Info	204960	Windows System Driver Enumeration (Windows)
Info	93962	Microsoft Security Rollup Enumeration
Info	62042	SMB QuickFixEngineering (QFE) Enumeration
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	162560	Microsoft Internet Explorer Installed
Info	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
Info	23974	Microsoft Windows SMB Share Hosting Office Files
Info	148541	Windows Language Settings Detection
Info	10736	DCE Services Enumeration
Info	92424	MUICache Program Execution History
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	55472	Device Hostname
Info	92429	Recycle Bin Files
Info	42898	SMB Registry : Stop the Registry Service after the scan (WMI)
Info	66424	Microsoft Malicious Software Removal Tool Installed
Info	100871	Microsoft Windows SMB Versions Supported (remote check)
Info	34220	Netstat Portscanner (WMI)
Info	86420	Ethernet MAC Addresses
Info	11936	OS Identification
Info	11011	Microsoft Windows SMB Service Detection
Info	21643	SSL Cipher Suites Supported
Info	92423	Windows Explorer Recently Executed Programs
Info	70331	Microsoft Windows Process Module Information
Info	10456	Microsoft Windows SMB Service Enumeration
Info	103871	Microsoft Windows Network Adapters
Info	182962	libcurl Installed (Windows)
Info	117885	Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	131023	Windows Defender Installed
Info	64582	Netstat Connection Information

Info	34252	Microsoft Windows Remote Listeners Enumeration (WMI)
Info	34096	BIOS Info (WMI)
Info	48763	Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting
Info	24270	Computer Manufacturer Information (WMI)
Info	77668	Windows Prefetch Folder
Info	10396	Microsoft Windows SMB Shares Access
Info	298387	Shor's Harvest Now Decrypt Later
Info	10902	Microsoft Windows 'Administrators' Group User List
Info	159817	Windows Credential Guard Status
Info	72482	Windows Display Driver Enumeration
Info	160576	Windows Services Registry ACL
Info	92421	Internet Explorer Typed URLs
Info	54615	Device Type
Info	200493	Microsoft Windows Start Menu Software Version Enumeration
Info	160486	Server Message Block (SMB) Protocol Version Detection
Info	10863	SSL Certificate Information
Info	51351	Microsoft .NET Framework Detection
Info	11777	Microsoft Windows SMB Share Hosting Possibly Copyrighted Material
Info	51187	WMI Encryptable Volume Enumeration
Info	45590	Common Platform Enumeration (CPE)
Info	92415	Application Compatibility Cache
Info	92373	Microsoft Windows SMB Sessions
Info	168980	Enumerate the PATH Variables
Info	156899	SSL/TLS Recommended Cipher Suites
Info	92369	Microsoft Windows Time Zone Information
Info	178102	Microsoft Windows Installed Software Version Enumeration
Info	92371	Microsoft Windows DNS Cache
Info	10287	Traceroute Information
Info	187318	Microsoft Windows Installed
Info	71246	Enumerate Local Group Memberships
Info	92364	Microsoft Windows Environment Variables

Info	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
Info	72684	Enumerate Users via WMI
Info	138603	Microsoft OneDrive Installed
Info	16193	Antivirus Software Check
Info	171410	IP Assignment Method Detection
Info	34097	BIOS Info (SMB)
Info	10394	Microsoft Windows SMB Log In Possible
Info	92368	Microsoft Windows Scripting Host Settings
Info	280146	Microsoft Azure Guest Agent Installed (Windows)
Info	161502	Microsoft Windows Logged On Users
Info	117887	OS Security Patch Assessment Available
Info	209654	OS Fingerprints Detected
Info	161691	The Microsoft Windows Support Diagnostic Tool (MSDT) RCE Workaround Detection (CVE-2022-30190)
Info	171956	Windows Enumerate Accounts

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 20% of the vulnerabilities on the network:

Action to take	Vulns	Assets
Microsoft Teams for Desktop < 25122.1415.3698.6812 Remote Code Execution (August 2025): Upgrade to Microsoft Teams for Desktop version 25122.1415.3698.6812 or later via the Microsoft Store.	1	1

Audits FAILED

WN11-00-000020 - Secure Boot must be enabled on Windows 11 systems.

Info

Secure Boot is a standard that ensures systems boot only to a trusted operating system. Secure Boot is required to support additional security features in Windows 11, including virtualization-based Security and Credential Guard. If Secure Boot is turned off, these security features will not function.

Solution

Enable Secure Boot in the system firmware.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8(1)
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14

ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8(1)
NESA	T7.4.1
NIAV2	NS5d
NIAV2	NS6b
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253257r1117271_rule
STIG-ID	WN11-00-000020
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253257

Assets

vm-win11-stig-s

```
'False'
```

WN11-00-000031 - Windows 11 systems must use a BitLocker PIN for pre-boot authentication.

Info

If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running. Pre-boot authentication prevents unauthorized users from accessing encrypted drives.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> BitLocker Drive Encryption >> Operating System Drives 'Require additional authentication at startup' to 'Enabled' with 'Configure TPM Startup PIN:' set to 'Require startup PIN with TPM' or with 'Configure TPM startup key and PIN:' set to 'Require startup key and PIN with TPM'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.16
800-171R3	03.13.08
800-53	SC-28(1)
800-53R5	SC-28(1)
CAT	I
CCI	CCI-002476
CN-L3	8.1.4.7(b)
CN-L3	8.1.4.8(b)
CSF	PR.DS-1
CSF2.0	PR.DS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.33
ITSG-33	SC-28(1)
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1
QCSC-V1	5.2.2

QCSC-V1	6.2
RULE-ID	SV-253260r958872_rule
STIG-ID	WN11-00-000031
TBA-FIISB	28.1
VULN-ID	V-253260

Assets

vm-win11-stig-s

```
The following AND condition has failed:
{
 UseAdvancedStartup:
 Remote value: NULL
 Policy value: 1
}
```

WN11-00-000032 - Windows 11 systems must use a BitLocker PIN with a minimum length of six digits for pre-boot authentication.

Info

If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running. Pre-boot authentication prevents unauthorized users from accessing encrypted drives. Increasing the pin length requires a greater number of guesses for an attacker.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> BitLocker Drive Encryption >> Operating System Drives 'Configure minimum PIN length for startup' to 'Enabled' with 'Minimum characters:' set to '6' or greater.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	IA-8
800-53R5	IA-8
CAT	II
CCI	CCI-000804
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-8
ITSG-33	IA-8a.
NESA	T4.3.1
NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253261r958504_rule

STIG-ID	WN11-00-000032
SWIFT-CSCV1	2.8
VULN-ID	V-253261

Assets

vm-win11-stig-s

```
NULL
```

WN11-00-000090 - Accounts must be configured to require password expiration.

Info

Passwords that do not expire increase exposure with a greater probability of being discovered or cracked.

Solution

Configure all passwords to expire.
Run 'Computer Management'.
Navigate to System Tools >> Local Users and Groups >> Users.
Double-click each active account.
Ensure 'Password never expires' is not checked on all active accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.07d.
800-53	IA-5(1)(d)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000199
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(d)
NESA	T5.2.3
NIAV2	AM20

NIAV2	AM21
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253273r1051040_rule
STIG-ID	WN11-00-000090
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-253273

Assets

vm-win11-stig-s

```
'Name       : Administrator
SID        : S-1-5-21-2746855186-1286860024-2359785572-1000
RunspaceId : 44ff50f3-d2f9-4a1b-bc57-18bdbfe705b1

Name       : Guest
SID        : S-1-5-21-2746855186-1286860024-2359785572-501
RunspaceId : 44ff50f3-d2f9-4a1b-bc57-18bdbfe705b1'
```

WN11-00-000135 - A host-based firewall must be installed and enabled on the system.

Info

A firewall provides a line of defense against attack, allowing or blocking inbound and outbound connections based on a set of rules.

Solution

Install and enable a host-based firewall on the system.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253281r991589_rule
STIG-ID	WN11-00-000135
SWIFT-CSCV1	2.3
VULN-ID	V-253281

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Domain:
 Remote value: NULL
 Policy value: 1


-------------------------
```

```
FAILED - PrivateProfile:
 Remote value: NULL
 Policy value: 1


-------------------------
FAILED - PublicProfile:
 Remote value: NULL
 Policy value: 1
```

WN11-00-000150 - Structured Exception Handling Overwrite Protection (SEHOP) must be enabled.

Info

Attackers are constantly looking for vulnerabilities in systems and applications. Structured Exception Handling Overwrite Protection (SEHOP) blocks exploits that use the Structured Exception Handling overwrite technique, a common buffer overflow attack.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' to 'Enabled'.
This policy setting requires the installation of the SecGuide custom templates included with the STIG package. 'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SI-16
800-53R5	SI-16
CAT	I
CCI	CCI-002824
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
RULE-ID	SV-253284r958928_rule
STIG-ID	WN11-00-000150
VULN-ID	V-253284

Assets

vm-win11-stig-s

NULL

WN11-00-000155 - The Windows PowerShell 2.0 feature must be disabled on the system.

Info

Windows PowerShell 5.0 added advanced logging features which can provide additional detail when malware has been run on a system. Disabling the Windows PowerShell 2.0 mitigates against a downgrade attack that evades the Windows PowerShell 5.0 script block logging feature.

Solution

Disable 'Windows PowerShell 2.0' on the system.
Run 'Windows PowerShell' with elevated privileges (run as administrator).
Enter the following:
Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root
This command must disable both 'MicrosoftWindowsPowerShellV2Root' and 'MicrosoftWindowsPowerShellV2' which correspond to 'Windows PowerShell 2.0' and 'Windows PowerShell 2.0 Engine' respectively in 'Turn Windows features on or off'.
Alternately:
Search for 'Features'.
Select 'Turn Windows features on or off'.
De-select 'Windows PowerShell 2.0'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2

RULE-ID	SV-253285r958478_rule
STIG-ID	WN11-00-000155
SWIFT-CSCV1	2.3
VULN-ID	V-253285

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - PowerShellv2:
 POWERSHELL_NO_RESULT: powershell command returned no result



-------------------------
FAILED - PowerShellv2Root:
 POWERSHELL_NO_RESULT: powershell command returned no result
```

WN11-00-000175 - The Secondary Logon service must be disabled on Windows 11.

Info

The Secondary Logon service provides a means for entering alternate credentials, typically used to run commands with elevated privileges. Using privileged credentials in a standard user session can expose those credentials to theft.

Solution

Configure the 'Secondary Logon' service 'Startup Type' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253289r958478_rule
STIG-ID	WN11-00-000175
SWIFT-CSCV1	2.3
VULN-ID	V-253289

Assets

vm-win11-stig-s

```
'manual'
```

WN11-AC-000005 - Windows 11 account lockout duration must be configured to 15 minutes or greater.

Info

The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the amount of time that an account will remain locked after the specified number of failed logon attempts.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> 'Account lockout duration' to '15' minutes or greater.
A value of '0' is also acceptable, requiring an administrator to unlock the account.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.8
800-171R3	03.01.08b.
800-53	AC-7b.
800-53R5	AC-7b.
CAT	II
CCI	CCI-002238
CN-L3	7.1.2.7(f)
CN-L3	7.1.3.1(c)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-7b.
NESA	T5.5.1
NIAV2	AM24
PCI-DSSV3.2.1	8.1.7
PCI-DSSV4.0	8.3.4
RULE-ID	SV-253297r958736_rule
STIG-ID	WN11-AC-000005
TBA-FIISB	36.2.4
TBA-FIISB	45.1.2
VULN-ID	V-253297

Assets

vm-win11-stig-s

10

WN11-AC-000010 - The number of allowed bad logon attempts must be configured to three or less.

Info

The account lockout feature, when enabled, prevents brute-force password attacks on the system. The higher this value is, the less effective the account lockout feature will be in protecting the local system. The number of bad logon attempts must be reasonably small to minimize the possibility of a successful password attack, while allowing for honest errors made during a normal user logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> 'Account lockout threshold' to '3' or less invalid logon attempts (excluding '0' which is unacceptable).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.8
800-171R3	03.01.08a.
800-53	AC-7a.
800-53R5	AC-7a.
CAT	II
CCI	CCI-000044
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-7a.
NESA	T5.5.1
NIAV2	AM24
PCI-DSSV3.2.1	8.1.6
PCI-DSSV4.0	8.3.4
RULE-ID	SV-253298r958388_rule
STIG-ID	WN11-AC-000010
TBA-FIISB	45.1.2
TBA-FIISB	45.2.1
TBA-FIISB	45.2.2
VULN-ID	V-253298

Assets

vm-win11-stig-s

10

WN11-AC-000015 - The period of time before the bad logon counter is reset must be configured to 15 minutes.

Info

The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that must pass after failed logon attempts before the counter is reset to 0. The smaller this value is, the less effective the account lockout feature will be in protecting the local system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> 'Reset account lockout counter after' to '15' minutes.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.8
800-171R3	03.01.08a.
800-53	AC-7a.
800-53R5	AC-7a.
CAT	II
CCI	CCI-000044
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-7a.
NESA	T5.5.1
NIAV2	AM24
PCI-DSSV3.2.1	8.1.6
PCI-DSSV4.0	8.3.4
RULE-ID	SV-253299r958388_rule
STIG-ID	WN11-AC-000015
TBA-FIISB	45.1.2
TBA-FIISB	45.2.1
TBA-FIISB	45.2.2
VULN-ID	V-253299

Assets

vm-win11-stig-s

10

WN11-AC-000020 - The password history must be configured to 24 passwords remembered.

Info

A system is more vulnerable to unauthorized access when system users recycle the same password several times without being required to change a password to a unique password on a regularly scheduled basis. This enables users to effectively negate the purpose of mandating periodic password changes. The default value is 24 for Windows domain systems. DOD has decided this is the appropriate value for all Windows systems.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> 'Enforce password history' to '24' passwords remembered.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.7
800-171R3	03.05.07b.
800-53	IA-5(1)(b)
800-53R5	IA-5(1)(b)
CAT	II
CCI	CCI-004061
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(b)
NESA	T5.2.3
NIAV2	AM22d
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253300r1000103_rule

STIG-ID	WN11-AC-000020
SWIFT-CSCV1	4.1
VULN-ID	V-253300

Assets

vm-win11-stig-s

0

WN11-AC-000030 - The minimum password age must be configured to at least 1 day.

Info

Permitting passwords to be changed in immediate succession within the same day allows users to cycle passwords through their history database. This enables users to effectively negate the purpose of mandating periodic password changes.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> 'Minimum Password Age' to at least '1' day.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.07d.
800-53	IA-5(1)(d)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000198
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(d)
NESA	T5.2.3
NIAV2	AM20
NIAV2	AM21

QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253302r1051043_rule
STIG-ID	WN11-AC-000030
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-253302

Assets

vm-win11-stig-s

0

WN11-AC-000035 - Passwords must, at a minimum, be 14 characters.

Info

Information systems not protected with strong password schemes (including passwords of minimum length) provide the opportunity for anyone to crack the password, thus gaining access to the system and compromising the device, information, or the local network.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> 'Minimum password length' to '14' characters.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.7
800-171R3	03.05.07a.
800-53	IA-5(1)(a)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000205
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(a)
NESA	T5.2.3
NIAV2	AM19a
NIAV2	AM19b

NIAV2	AM19c
NIAV2	AM19d
NIAV2	AM22a
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253303r1051044_rule
STIG-ID	WN11-AC-000035
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.1
TBA-FIISB	26.2.4
VULN-ID	V-253303

Assets

vm-win11-stig-s

```
0
```

WN11-AC-000040 - The built-in Microsoft password complexity filter must be enabled.

Info

The use of complex passwords increases their strength against guessing and brute-force attacks. This setting configures the system to verify that newly created passwords conform to the Windows password complexity policy.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> 'Password must meet complexity requirements' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.7
800-171R3	03.05.07a.
800-53	IA-5(1)(a)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000192
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(a)
NESA	T5.2.3
NIAV2	AM19a
NIAV2	AM19b

NIAV2	AM19c
NIAV2	AM19d
NIAV2	AM22a
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253304r1051045_rule
STIG-ID	WN11-AC-000040
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.1
TBA-FIISB	26.2.4
VULN-ID	V-253304

Assets

vm-win11-stig-s

```
'disabled'
```

WN11-AU-000005 - The system must be configured to audit Account Logon - Credential Validation failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Credential validation records events related to validation tests on credentials for a user account logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Logon >> 'Audit Credential Validation' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253306r991570_rule
STIG-ID	WN11-AU-000005
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253306

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000010 - The system must be configured to audit Account Logon - Credential Validation successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Credential validation records events related to validation tests on credentials for a user account logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Logon >> 'Audit Credential Validation' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253307r991570_rule
STIG-ID	WN11-AU-000010
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253307

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000035 - The system must be configured to audit Account Management - User Account Management failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
User Account Management records events such as creating, changing, deleting, renaming, disabling, or enabling user accounts.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Management >> 'Audit User Account Management' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SI-11b.
800-53R5	SI-11b.
CAT	II
CCI	CCI-001314
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-11c.
RULE-ID	SV-253309r958566_rule
STIG-ID	WN11-AU-000035
VULN-ID	V-253309

Assets

vm-win11-stig-s

```
'success'
```

WN11-AU-000045 - The system must be configured to audit Detailed Tracking - PNP Activity successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Plug and Play activity records events related to the successful connection of external devices.

Solution

Computer Configuration >> Windows Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Detailed Tracking >> 'Audit PNP Activity' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171	3.4.5
800-171R3	03.03.03a.
800-171R3	03.04.05
800-53	AU-12c.
800-53	CM-5(1)
800-53R5	AU-12c.
800-53R5	CM-5(1)(b)
CAT	II
CCI	CCI-000172
CCI	CCI-001814
CCI	CCI-003938
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7

CSF	PR.IP-1
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.4
ISO-27001-2022	A.8.9
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.19
ISO-27001-2022	A.8.31
ISO-27001-2022	A.8.32
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
ITSG-33	CM-5(1)
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.6.1
NESA	T7.5.3
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2

QCSC-V1	7.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253311r1051047_rule
STIG-ID	WN11-AU-000045
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253311

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000050 - The system must be configured to audit Detailed Tracking - Process Creation successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Process creation records events related to the creation of a process and the source.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Detailed Tracking >> 'Audit Process Creation' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171	3.4.5
800-171R3	03.03.03a.
800-171R3	03.04.05
800-53	AU-12c.
800-53	CM-5(1)
800-53R5	AU-12c.
800-53R5	CM-5(1)(b)
CAT	II
CCI	CCI-000172
CCI	CCI-001814
CCI	CCI-003938
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7

CSF	PR.IP-1
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.4
ISO-27001-2022	A.8.9
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.19
ISO-27001-2022	A.8.31
ISO-27001-2022	A.8.32
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
ITSG-33	CM-5(1)
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.6.1
NESA	T7.5.3
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2

QCSC-V1	7.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253312r1051048_rule
STIG-ID	WN11-AU-000050
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253312

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000054 - The system must be configured to audit Logon/Logoff - Account Lockout failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Account Lockout events can be used to identify potentially malicious logon attempts.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> 'Audit Account Lockout' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253313r991578_rule
STIG-ID	WN11-AU-000054
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253313

Assets

vm-win11-stig-s

```
'success'
```

WN11-AU-000060 - The system must be configured to audit Logon/Logoff - Group Membership successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Group Membership records information related to the group membership of a user's logon token.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> 'Audit Group Membership' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253314r991570_rule
STIG-ID	WN11-AU-000060
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253314

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000081 - Windows 11 must be configured to audit Object Access - File Share failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Auditing file shares records events related to connection to shares on a system including system shares such as C$.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit File Share' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253319r991572_rule
STIG-ID	WN11-AU-000081
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253319

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000082 - Windows 11 must be configured to audit Object Access - File Share successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Auditing file shares records events related to connection to shares on a system including system shares such as C$.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit File Share' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253320r991572_rule
STIG-ID	WN11-AU-000082
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253320

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000083 - Windows 11 must be configured to audit Object Access - Other Object Access Events successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Auditing for other object access records events related to the management of task scheduler jobs and COM+ objects.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit Other Object Access Events' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253321r991572_rule
STIG-ID	WN11-AU-000083
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253321

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000084 - Windows 11 must be configured to audit Object Access - Other Object Access Events failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Auditing for other object access records events related to the management of task scheduler jobs and COM+ objects.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit Other Object Access Events' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253322r991572_rule
STIG-ID	WN11-AU-000084
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253322

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000085 - The system must be configured to audit Object Access - Removable Storage failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Auditing object access for removable media records events related to access attempts on file system objects on removable storage devices.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit Removable Storage' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253323r991583_rule
STIG-ID	WN11-AU-000085
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253323

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000090 - The system must be configured to audit Object Access - Removable Storage successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Auditing object access for removable media records events related to access attempts on file system objects on removable storage devices.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit Removable Storage' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04

DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253324r991583_rule
STIG-ID	WN11-AU-000090
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253324

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000107 - The system must be configured to audit Policy Change - Authorization Policy Change successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Authorization Policy Change records events related to changes in user rights, such as create a token object.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> 'Audit Authorization Policy Change' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253327r991572_rule
STIG-ID	WN11-AU-000107
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253327

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000110 - The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Sensitive Privilege Use records events related to use of sensitive privileges, such as 'Act as part of the operating system' or 'Debug programs'.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Privilege Use >> 'Audit Sensitive Privilege Use' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07b.
800-53	AC-6(9)
800-53R5	AC-6(9)
CAT	II
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253328r958732_rule
STIG-ID	WN11-AU-000110
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253328

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000115 - The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Sensitive Privilege Use records events related to use of sensitive privileges, such as 'Act as part of the operating system' or 'Debug programs'.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Privilege Use >> 'Audit Sensitive Privilege Use' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04

DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253329r991575_rule
STIG-ID	WN11-AU-000115
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253329

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000120 - The system must be configured to audit System - IPsec Driver failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
IPsec Driver records events related to the IPsec Driver such as dropped packets.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> 'Audit IPsec Driver' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253330r991586_rule
STIG-ID	WN11-AU-000120
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253330

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000150 - The system must be configured to audit System - Security System Extension successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Security System Extension records events related to extension code being loaded by the security subsystem.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> 'Audit Security System Extension' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253334r991575_rule
STIG-ID	WN11-AU-000150
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253334

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000500 - The Application event log size must be configured to 32768 KB or greater.

Info

Inadequate log size will cause the log to fill up quickly. This may prevent audit events from being recorded properly and require frequent attention by administrative personnel.

Solution

If the system is configured to send audit records directly to an audit server, this is NA. This must be documented with the ISSO.
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Event Log Service >> Application >> 'Specify the maximum log file size (KB)' to 'Enabled' with a 'Maximum Log Size (KB)' of '32768' or greater.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	AU-4
800-53R5	AU-4
CAT	II
CCI	CCI-001849
CSF	PR.DS-4
CSF	PR.PT-1
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.6
ITSG-33	AU-4
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253337r958752_rule
STIG-ID	WN11-AU-000500
VULN-ID	V-253337

Assets

vm-win11-stig-s

```
NULL
```

WN11-AU-000505 - The Security event log size must be configured to 1024000 KB or greater.

Info

Inadequate log size will cause the log to fill up quickly. This may prevent audit events from being recorded properly and require frequent attention by administrative personnel.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Event Log Service >> Security >> 'Specify the maximum log file size (KB)' to 'Enabled' with a 'Maximum Log Size (KB)' of '1024000' or greater.
If the system is configured to send audit records directly to an audit server, this must be documented with the ISSO.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	AU-4
800-53R5	AU-4
CAT	II
CCI	CCI-001849
CSF	PR.DS-4
CSF	PR.PT-1
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.6
ITSG-33	AU-4
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253338r958752_rule
STIG-ID	WN11-AU-000505
VULN-ID	V-253338

Assets

vm-win11-stig-s

```
NULL
```

WN11-AU-000510 - The System event log size must be configured to 32768 KB or greater.

Info

Inadequate log size will cause the log to fill up quickly. This may prevent audit events from being recorded properly and require frequent attention by administrative personnel.

Solution

If the system is configured to send audit records directly to an audit server, this is NA. This must be documented with the ISSO.
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Event Log Service >> System >> 'Specify the maximum log file size (KB)' to 'Enabled' with a 'Maximum Log Size (KB)' of '32768' or greater.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	AU-4
800-53R5	AU-4
CAT	II
CCI	CCI-001849
CSF	PR.DS-4
CSF	PR.PT-1
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.6
ITSG-33	AU-4
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253339r958752_rule
STIG-ID	WN11-AU-000510
VULN-ID	V-253339

Assets

vm-win11-stig-s

```
NULL
```

WN11-AU-000550 - Windows 11 must be configured to audit Other Policy Change Events Successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Other Policy Change Events contains events about EFS Data Recovery Agent policy changes, changes in Windows Filtering Platform filter, status on Security policy settings updates for local Group Policy settings, Central Access Policy changes, and detailed troubleshooting events for Cryptographic Next Generation (CNG) operations.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change>> 'Audit Other Policy Change Events' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253343r958412_rule
STIG-ID	WN11-AU-000550
SWIFT-CSCV1	6.4
VULN-ID	V-253343

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000555 - Windows 11 must be configured to audit Other Policy Change Events Failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Other Policy Change Events contains events about EFS Data Recovery Agent policy changes, changes in Windows Filtering Platform filter, status on Security policy settings updates for local Group Policy settings, Central Access Policy changes, and detailed troubleshooting events for Cryptographic Next Generation (CNG) operations.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change>> 'Audit Other Policy Change Events' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253344r958412_rule
STIG-ID	WN11-AU-000555
SWIFT-CSCV1	6.4
VULN-ID	V-253344

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000560 - Windows 11 must be configured to audit other Logon/Logoff Events Successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Other Logon/Logoff Events determines whether Windows generates audit events for other logon or logoff events. Logon events are essential to understanding user activity and detecting potential attacks.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> 'Audit Other Logon/Logoff Events' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2
NIAV2	AM34a

NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253345r958412_rule
STIG-ID	WN11-AU-000560
SWIFT-CSCV1	6.4
VULN-ID	V-253345

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000565 - Windows 11 must be configured to audit other Logon/Logoff Events Failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Other Logon/Logoff Events determines whether Windows generates audit events for other logon or logoff events. Logon events are essential to understanding user activity and detecting potential attacks.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> 'Audit Other Logon/Logoff Events' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2
NIAV2	AM34a

NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253346r958412_rule
STIG-ID	WN11-AU-000565
SWIFT-CSCV1	6.4
VULN-ID	V-253346

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000570 - Windows 11 must be configured to audit Detailed File Share Failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Detailed File Share allows the user to audit attempts to access files and folders on a shared folder.
The Detailed File Share setting logs an event every time a file or folder is accessed, whereas the File Share setting only records one event for any connection established between a client and file share. Detailed File Share audit events include detailed information about the permissions or other criteria used to grant or deny access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> Audit Detailed File Share' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253347r958412_rule
STIG-ID	WN11-AU-000570
SWIFT-CSCV1	6.4
VULN-ID	V-253347

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000575 - Windows 11 must be configured to audit MPSSVC Rule-Level Policy Change Successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit MPSSVC Rule-Level Policy Change determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe).

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> Audit MPSSVC Rule-Level Policy Change' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253348r958412_rule
STIG-ID	WN11-AU-000575
SWIFT-CSCV1	6.4
VULN-ID	V-253348

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000580 - Windows 11 must be configured to audit MPSSVC Rule-Level Policy Change Failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit MPSSVC Rule-Level Policy Change determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe).

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> Audit MPSSVC Rule-Level Policy Change' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253349r958412_rule
STIG-ID	WN11-AU-000580
SWIFT-CSCV1	6.4
VULN-ID	V-253349

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000581 - Windows 11 must be configured to audit file system failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. Credential validation records events related to validation tests on credentials for a user account logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit File System' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-278926r1135296_rule
STIG-ID	WN11-AU-000581
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-278926

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000582 - Windows 11 must be configured to audit file system successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. Credential validation records events related to validation tests on credentials for a user account logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit File System' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-278927r1135299_rule
STIG-ID	WN11-AU-000582
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-278927

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000583 - Windows 11 must be configured to audit handle manipulation failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. Credential validation records events related to validation tests on credentials for a user account logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit Handle Manipulation' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-278928r1135302_rule
STIG-ID	WN11-AU-000583
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-278928

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000584 - Windows 11 must be configured to audit handle manipulation successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. Credential validation records events related to validation tests on credentials for a user account logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit Handle Manipulation' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-278929r1135305_rule
STIG-ID	WN11-AU-000584
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-278929

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000585 - Windows 11 must have command line process auditing events enabled for failures.

Info

When this policy setting is enabled, the operating system generates audit events when a process fails to start and the name of the program or user that created it.
These audit events can assist in understanding how a computer is being used and tracking user activity.

Solution

Go to Computer Configuration >> Windows Settings >>Security Settings>> Advanced Audit Policy Configuration >> System Audit Policies >> Detailed Tracking >> Set 'Audit Process Creation' to 'Failure'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07b.
800-53	AC-6(9)
800-53R5	AC-6(9)
CAT	II
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2

NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-257770r958412_rule
STIG-ID	WN11-AU-000585
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-257770

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000586 - Windows 11 must be configured to audit registry successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. Credential validation records events related to validation tests on credentials for a user account logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit Registry' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-278931r1135311_rule
STIG-ID	WN11-AU-000586
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-278931

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000587 - Windows 11 must be configured to audit sensitive privilege use successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. Credential validation records events related to validation tests on credentials for a user account logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Privilege Use >> Audit Sensitive Privilege Use with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-278932r1141916_rule
STIG-ID	WN11-AU-000587
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-278932

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000588 - Windows 11 must be configured to audit sensitive privilege use failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. Credential validation records events related to validation tests on credentials for a user account logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Privilege Use >> Audit Sensitive Privilege Use with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-278933r1141919_rule
STIG-ID	WN11-AU-000588
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-278933

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-AU-000589 - Windows 11 must be configured to audit registry failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. Credential validation records events related to validation tests on credentials for a user account logon.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit Registry' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-278930r1135308_rule
STIG-ID	WN11-AU-000589
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-278930

Assets

vm-win11-stig-s

```
'no auditing'
```

WN11-CC-000039 - Run as different user must be removed from context menus.

Info

The 'Run as different user' selection from context menus allows the use of credentials other than the currently logged on user. Using privileged credentials in a standard user session can expose those credentials to theft. Removing this option from context menus helps prevent this from occurring.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'Remove 'Run as Different User' from context menus' to 'Enabled'.
This policy setting requires the installation of the SecGuide custom templates included with the STIG package. 'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253359r958478_rule
STIG-ID	WN11-CC-000039

SWIFT-CSCV1	2.3
VULN-ID	V-253359

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - batfile:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Classes\Batfile\Shell\Runasuser
reg_item: SuppressionPolicy


-------------------------
FAILED - cmdfile:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Classes\Cmdfile\Shell\Runasuser
reg_item: SuppressionPolicy


-------------------------
FAILED - exefile:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Classes\Exefile\Shell\Runasuser
reg_item: SuppressionPolicy


-------------------------
FAILED - mscfile:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Classes\Mscfile\Shell\Runasuser
reg_item: SuppressionPolicy
```

WN11-CC-000050 - Hardened UNC Paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.

Info

Additional security requirements are applied to Universal Naming Convention (UNC) paths specified in Hardened UNC paths before allowing access them. This aids in preventing tampering with or spoofing of connections to these paths.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Network Provider >> 'Hardened UNC Paths' to 'Enabled' with at least the following configured in 'Hardened UNC Paths:' (click the 'Show' button to display).
Value Name: *\SYSVOL Value: RequireMutualAuthentication=1, RequireIntegrity=1
Value Name: *\NETLOGON Value: RequireMutualAuthentication=1, RequireIntegrity=1

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253362r991589_rule
STIG-ID	WN11-CC-000050
SWIFT-CSCV1	2.3
VULN-ID	V-253362

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
```

```
FAILED - SYSVOL:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths
reg_item: \\*\SYSVOL


-------------------------
FAILED - NETLOGON:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths
reg_item: \\*\NETLOGON
```

WN11-CC-000070 - Virtualization-based Security must be enabled on Windows 11 with the platform security level configured to Secure Boot or Secure Boot with DMA Protection.

Info

Virtualization-based Security (VBS) provides the platform for the additional security features, Credential Guard and virtualization-based protection of code integrity. Secure Boot is the minimum security level with DMA protection providing additional memory protection. DMA Protection requires a CPU that supports input/output memory management unit (IOMMU).

Solution

Virtualization-based security, including Credential Guard, currently cannot be implemented in virtual desktop implementations (VDI) due to specific supporting requirements including a TPM, UEFI with Secure Boot, and the capability to run the Hyper-V feature within the virtual desktop.
For VDIs where the virtual desktop instance is deleted or refreshed upon logoff, this is NA.
Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Device Guard >> 'Turn On virtualization-based Security' to 'Enabled' with 'Secure Boot' or 'Secure Boot and DMA Protection' selected for 'Select Platform Security Level:'.
A Microsoft article on Credential Guard system requirement can be found at the following link.
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard-requirements

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253369r991589_rule
STIG-ID	WN11-CC-000070
SWIFT-CSCV1	2.3
VULN-ID	V-253369

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - RequiredSecurityProperties:
 WMI_CMD_EXEC_FAILED: Could not execute command

Error: Failed to connect to the 'ADMIN$' share.



-------------------------
FAILED - VirtualizationBasedSecurityStatus:
 WMI_CMD_EXEC_FAILED: Could not execute command

Error: Failed to connect to the 'ADMIN$' share.
```

WN11-CC-000210 - The Microsoft Defender SmartScreen for Explorer must be enabled.

Info

Microsoft Defender SmartScreen helps protect systems from programs downloaded from the internet that may be malicious. Enabling Microsoft Defender SmartScreen will warn or prevent users from running potentially malicious programs.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Configure Windows Defender SmartScreen' to 'Enabled' with 'Warn and prevent bypass' selected. Windows 11 includes duplicate policies for this setting. It can also be configured under Computer Configuration >> Administrative Templates >> Windows Components >> Windows Defender SmartScreen >> Explorer.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253395r958478_rule
STIG-ID	WN11-CC-000210
SWIFT-CSCV1	2.3

VULN-ID V-253395

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - EnableSmartScreen:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Policies\Microsoft\Windows\System
reg_item: EnableSmartScreen


-------------------------
FAILED - ShellSmartScreenLevel:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Policies\Microsoft\Windows\System
reg_item: ShellSmartScreenLevel
```

WN11-PK-000005 - The DoD Root CA certificates must be installed in the Trusted Root Store.

Info

To ensure secure DoD websites and DoD-signed code are properly validated, the system must trust the DoD Root Certificate Authorities (CAs). The DoD root certificates will ensure that the trust chain is established for server certificates issued from the DoD CAs.

Solution

Install the DoD Root CA certificates.
DoD Root CA 3 DoD Root CA 4 DoD Root CA 5 DoD Root CA 6
The InstallRoot tool is available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. PKI can be found at https://crl.gds.disa.mil/.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.12
800-53	IA-5(2)(a)
800-53R5	IA-5(2)(b)(1)
CAT	II
CCI	CCI-000185
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(2)(a)
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253427r958448_rule
STIG-ID	WN11-PK-000005
VULN-ID	V-253427

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Root CA 4:
 WMI_CMD_EXEC_FAILED: Could not execute command

Error: Failed to connect to the 'ADMIN$' share.



-------------------------
FAILED - Root CA 6:
 WMI_CMD_EXEC_FAILED: Could not execute command

Error: Failed to connect to the 'ADMIN$' share.



-------------------------
FAILED - Root CA 5:
 WMI_CMD_EXEC_FAILED: Could not execute command

Error: Failed to connect to the 'ADMIN$' share.



-------------------------
FAILED - Root CA 3:
 WMI_CMD_EXEC_FAILED: Could not execute command

Error: Failed to connect to the 'ADMIN$' share.
```

WN11-PK-000020 - The US DOD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

Info

To ensure users do not experience denial of service when performing certificate-based authentication to DOD websites due to the system chaining to a root other than DOD Root CAs, the US DOD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificate Store. This requirement only applies to unclassified systems.

Solution

Install the US DOD CCEB Interoperability Root CA cross-certificate on unclassified systems.
Issued To - Issued By - Thumbprint 9B74964506C7ED9138070D08D5F8B969866560C8 NotAfter: 7/18/2025 9:56:22 AM Issued To: DOD Root CA 6 Issued By: US DOD CCEB Interoperability Root CA 2 Thumbprint: D471CA32F7A692CE6CBB6196BD3377FE4DBCD106 NotAfter: 7/18/2026
The certificates can be installed using the InstallRoot tool. The tool and user guide are available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. Certificate bundles published by the PKI can be found at https://crl.gds.disa.mil/.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.15
800-171R3	03.13.15
800-53	SC-23(5)
800-53R5	SC-23(5)
CAT	II
CCI	CCI-002470
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-23
ITSG-33	SC-23a.
NESA	T4.5.1
QCSC-V1	5.2.1
RULE-ID	SV-253430r1081058_rule
STIG-ID	WN11-PK-000020
VULN-ID	V-253430

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Root CA 3:
 WMI_CMD_EXEC_FAILED: Could not execute command

Error: Failed to connect to the 'ADMIN$' share.
```

```
-------------------------
FAILED - Root CA 6:
 WMI_CMD_EXEC_FAILED: Could not execute command

Error: Failed to connect to the 'ADMIN$' share.
```

WN11-RG-000005 - Default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained.

Info

The registry is integral to the function, security, and stability of the Windows system. Changing the system's registry permissions allows the possibility of unauthorized and anonymous modification to the operating system.

Solution

Maintain the default permissions for the HKEY_LOCAL_MACHINE registry hive.
The default permissions of the higher level keys are noted below.
HKEY_LOCAL_MACHINE\SECURITY Type - 'Allow' for all Inherited from - 'None' for all Principal - Access - Applies to SYSTEM - Full Control - This key and subkeys Administrators - Special - This key and subkeys
HKEY_LOCAL_MACHINE\SOFTWARE Type - 'Allow' for all Inherited from - 'None' for all Principal - Access - Applies to Users - Read - This key and subkeys Administrators - Full Control - This key and subkeys SYSTEM - Full Control - This key and subkeys CREATOR OWNER - Full Control - This key and subkeys ALL APPLICATION PACKAGES - Read - This key and subkeys
HKEY_LOCAL_MACHINE\SYSTEM Type - 'Allow' for all Inherited from - 'None' for all Principal - Access - Applies to Users - Read - This key and subkeys Administrators - Full Control - This key and subkeys SYSTEM - Full Control - This key and subkeys CREATOR OWNER - Full Control - This key and subkeys ALL APPLICATION PACKAGES - Read - This key and subkeys
Microsoft has also given read permission to the SOFTWARE and SYSTEM registry keys in later versions of Windows 11 to the following SID.
S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2

ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253431r958726_rule
STIG-ID	WN11-RG-000005
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253431

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - HKEY_LOCAL_MACHINE\SECURITY:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Security


-------------------------
FAILED - HKEY_LOCAL_MACHINE\SOFTWARE:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$
```

```
reg_key: HKLM\Software


-------------------------
FAILED - HKEY_LOCAL_MACHINE\SYSTEM:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\System
```

WN11-SO-000280 - Passwords for enabled local Administrator accounts must be changed at least every 60 days.

Info

The longer a password is in use, the greater the opportunity for someone to gain unauthorized knowledge of the password. A local Administrator account is not generally used and its password may not be changed as frequently as necessary. Changing the password for enabled Administrator accounts on a regular basis will limit its exposure. Windows LAPS must be used to change the built-in Administrator account password.

Solution

Change the enabled local Administrator account password at least every 60 days.
Windows LAPS must be used to change the built-in Administrator account password. Domain-joined and nondomain-joined systems can configure this to occur more frequently. LAPS will change the password every 30 days by default. More information is available at:
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/by-popular-demand-windows-laps-available-now/ba-p/3788747 https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview#windows-laps-supported-platforms-and-azure-ad-laps-preview-status

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.07d.
800-53	IA-5(1)(d)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000199
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3

ITSG-33	IA-5(1)(d)
NESA	T5.2.3
NIAV2	AM20
NIAV2	AM21
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253476r1051060_rule
STIG-ID	WN11-SO-000280
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-253476

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Password last set date for Admin account.:
 WMI_CMD_EXEC_FAILED: Could not execute command

Error: Failed to connect to the 'ADMIN$' share.



-------------------------
FAILED - LAPS password age configured.:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\LAPS
reg_item: PasswordAgeDays


-------------------------
FAILED - LAPS password length configured.:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\LAPS
reg_item: PasswordLength


-------------------------
FAILED - LAPS password complexity configured.:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$

reg_key: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\LAPS
reg_item: PasswordComplexity


-------------------------
FAILED - LAPS name of administrator account enabled.:
 IPC_ERROR_SHARE_CONNECT: an error happened while connecting to IPC$
```

Audits SKIPPED

Audits PASSED

DISA_STIG_Microsoft_Windows_11_v2r5.audit from DISA Microsoft Windows 11 STIG v2r5

Info

Solution

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - Windows 11 is installed:
 Remote value: '26200'
 Policy value: '2[26][0-9]{3}'


-------------------------
PASSED - Windows 11 installation type:
 Remote value: 'Client'
 Policy value: 'Client'
```

WN11-00-000005 - Domain-joined systems must use Windows 11 Enterprise Edition 64-bit version.

Info

Features such as Credential Guard use virtualization-based security to protect information that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Virtualization-based security and Credential Guard are only available with Windows 11 Enterprise 64-bit version.

Solution

Use Windows 11 Enterprise 64-bit version for domain-joined systems.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253254r991589_rule
STIG-ID	WN11-00-000005
SWIFT-CSCV1	2.3
VULN-ID	V-253254

Assets

vm-win11-stig-s

PASSED

WN11-00-000010 - Windows 11 domain-joined systems must have a Trusted Platform Module (TPM) enabled.

Info

Credential Guard uses virtualization-based security to protect information that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Without a TPM enabled and ready for use, Credential Guard keys are stored in a less secure method using software.

Solution

For standalone systems, this is NA.
Virtualization-based security, including Credential Guard, currently cannot be implemented in virtual desktop implementations (VDI) due to specific supporting requirements including a TPM, UEFI with Secure Boot, and the capability to run the Hyper-V feature within the virtual desktop.
For VDIs where the virtual desktop instance is deleted or refreshed upon logoff, this is NA.
Ensure domain-joined systems must have a TPM that is configured for use. (Versions 2.0 support Credential Guard.)
The TPM must be enabled in the firmware.
Run 'tpm.msc' for configuration options in Windows.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8(1)
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8(1)
NESA	T7.4.1
NIAV2	NS5d
NIAV2	NS6b
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253255r1117271_rule
STIG-ID	WN11-00-000010
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253255

Assets

vm-win11-stig-s

PASSED

WN11-00-000040 - Windows 11 systems must be maintained at a supported servicing level.

Info

Windows 11 is maintained by Microsoft at servicing levels for specific periods of time to support Windows as a Service. Systems at unsupported servicing levels or releases will not receive security updates for new vulnerabilities which leaves them subject to exploitation.
New versions with feature updates are planned to be released on a semi-annual basis with an estimated support timeframe of 18 to 30 months depending on the release. Support for previously released versions has been extended for Enterprise editions.
A separate servicing branch intended for special purpose systems is the Long-Term Servicing Channel (LTSC, formerly Branch - LTSB) which will receive security updates for 10 years but excludes feature updates.

Solution

Update systems on the Semi-Annual Channel to 'Microsoft Windows 11 Version 22H2 (OS Build 22621.380)' or greater.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253263r1016364_rule
STIG-ID	WN11-00-000040
SWIFT-CSCV1	2.3
VULN-ID	V-253263

Assets

vm-win11-stig-s

```
'26200'
```

WN11-00-000045 - The Windows 11 system must use an antivirus program.

Info

Malicious software can establish a base on individual desktops and servers. Employing an automated mechanism to detect this type of software will aid in elimination of the software from the operating system.

Solution

Install Microsoft Defender Antivirus or a third-party antivirus solution.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253264r991589_rule
STIG-ID	WN11-00-000045
SWIFT-CSCV1	2.3
VULN-ID	V-253264

Assets

vm-win11-stig-s

```
One of the following must pass to satisfy this requirement:

-------------------------
PASSED - Microsoft Defender Antivirus is installed:
 Remote value: 'Status      : Running
DisplayName : Microsoft Defender Antivirus Network Inspection Service
RunspaceId  : 3deaff51-22f3-428d-ba97-377c15b76beb

Status      : Running
```

```
DisplayName : Microsoft Defender Antivirus Service
RunspaceId  : 3deaff51-22f3-428d-ba97-377c15b76beb

PASS'
 Policy value: '^PASS$'


-------------------------
FAILED - Symantec Antivirus is installed:
 Remote value: 'FAIL - Symantec Antivirus not found'
 Policy value: '^PASS$'


-------------------------
FAILED - McAfee Antivirus is installed:
 Remote value: 'FAIL - McAfee Antivirus not found'
 Policy value: '^PASS$'
```

WN11-00-000050 - Local volumes must be formatted using NTFS.

Info

The ability to set access permissions and auditing is critical to maintaining the security and proper access controls of a system. To support this, volumes must be formatted using the NTFS file system.

Solution

Format all local volumes to use NTFS.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	I
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20

ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253265r1137691_rule
STIG-ID	WN11-00-000050
TBA-FIISB	31.1
VULN-ID	V-253265

Assets

vm-win11-stig-s

```
'None'
```

WN11-00-000075 - Only accounts responsible for the backup operations must be members of the Backup Operators group.

Info

Backup Operators are able to read and write to any file in the system, regardless of the rights assigned to it. Backup and restore rights permit users to circumvent the file access restrictions present on NTFS disk drives for backup and restore purposes. Members of the Backup Operators group must have separate logon accounts for performing backup duties.

Solution

Create separate accounts for backup operations for users with this privilege.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253270r991589_rule
STIG-ID	WN11-00-000075
SWIFT-CSCV1	2.3
VULN-ID	V-253270

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - Check if no accounts are members of the Backup Operators group.:
 Remote value: 'PASS: No accounts are part of the Backup Operators group.'
```

```
Policy value: 'PASS: No accounts are part of the Backup Operators group.'
```

WN11-00-000080 - Only authorized user accounts must be allowed to create or run virtual machines on Windows 11 systems.

Info

Allowing other operating systems to run on a secure system may allow users to circumvent security. For Hyper-V, preventing unauthorized users from being assigned to the Hyper-V Administrators group will prevent them from accessing or creating virtual machines on the system. The Hyper-V Hypervisor is used by virtualization-based Security features such as Credential Guard on Windows 11; however, it is not the full Hyper-V installation.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

For Hyper-V, remove any unauthorized groups or user accounts from the 'Hyper-V Administrators' group.
For hosted hypervisors other than Hyper-V, restrict access to create or run virtual machines to authorized user accounts only.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3(4)
800-53R5	AC-3(4)
CAT	II
CCI	CCI-002165
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33

ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3(4)
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253271r958702_rule
STIG-ID	WN11-00-000080
TBA-FIISB	31.1
VULN-ID	V-253271

Assets

vm-win11-stig-s

```
'No entries found'
```

WN11-00-000085 - Standard local user accounts must not exist on a system in a domain.

Info

To minimize potential points of attack, local user accounts, other than built-in accounts and local administrator accounts, must not exist on a workstation in a domain. Users must log on to workstations in a domain with their domain accounts.

Solution

Limit local user accounts on domain-joined systems. Remove any unauthorized local accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253272r991589_rule
STIG-ID	WN11-00-000085
SWIFT-CSCV1	2.3
VULN-ID	V-253272

Assets

vm-win11-stig-s

PASSED

WN11-00-000095 - Permissions for system files and directories must conform to minimum requirements.

Info

Changing the system's file and directory permissions allows the possibility of unauthorized and anonymous modification to the operating system and installed applications.

Solution

Maintain the default file system permissions and configure the Security Option: 'Network access: Let everyone permissions apply to anonymous users' to 'Disabled' (WN11-SO-000160).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3(4)
800-53R5	AC-3(4)
CAT	II
CCI	CCI-002165
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18

ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3(4)
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253274r1016661_rule
STIG-ID	WN11-00-000095
TBA-FIISB	31.1
VULN-ID	V-253274

Assets

vm-win11-stig-s

PASSED

WN11-00-000100 - Internet Information System (IIS) or its subcomponents must not be installed on a workstation.

Info

IIS is not installed by default. Installation of Internet Information System (IIS) may allow unauthorized internet services to be hosted. Websites must only be hosted on servers that have been designed for that purpose and can be adequately secured.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Uninstall 'Internet Information Services' or 'Internet Information Services Hostable Web Core' from the system.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	I
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253275r958478_rule
STIG-ID	WN11-00-000100
SWIFT-CSCV1	2.3

VULN-ID V-253275

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - IIS-WebServer:
 Remote value: ''
 Policy value: '^Manual Review Required$'


-------------------------
PASSED - IIS-HostableWebCore:
 Remote value: ''
 Policy value: '^Manual Review Required$'
```

WN11-00-000105 - Simple Network Management Protocol (SNMP) must not be installed on the system.

Info

'SNMP' is not installed by default. Some protocols and services do not support required security features, such as encrypting passwords or traffic.

Solution

Uninstall 'Simple Network Management Protocol (SNMP)' from the system.
Run 'Programs and Features'.
Select 'Turn Windows Features on or off'.
De-select 'Simple Network Management Protocol (SNMP)'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06b.
800-53	CM-7b.
800-53R5	CM-7b.
CAT	II
CCI	CCI-000382
CN-L3	7.1.3.5(c)
CN-L3	7.1.3.7(d)
CN-L3	8.1.4.4(b)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS13b
NIAV2	SS14a
NIAV2	SS14c
PCI-DSSV3.2.1	2.2.2
PCI-DSSV4.0	2.2.4
QCSC-V1	3.2

RULE-ID	SV-253276r958480_rule
STIG-ID	WN11-00-000105
SWIFT-CSCV1	2.3
VULN-ID	V-253276

Assets

vm-win11-stig-s

```
'%windir%\System32\snmp.exe_file_does_not_exist'
```

WN11-00-000110 - Simple TCP/IP Services must not be installed on the system.

Info

'Simple TCP/IP Services' is not installed by default. Some protocols and services do not support required security features, such as encrypting passwords or traffic.

Solution

Uninstall 'Simple TCPIP Services (i.e. echo, daytime etc.)' from the system.
Run 'Programs and Features'.
Select 'Turn Windows Features on or off'.
De-select 'Simple TCPIP Services (i.e. echo, daytime etc.)'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253277r958478_rule
STIG-ID	WN11-00-000110
SWIFT-CSCV1	2.3

VULN-ID	V-253277

Assets

vm-win11-stig-s

```
'HKLM\System\CurrentControlSet\Services\Simptcp_registry_does_not_exist'
```

WN11-00-000115 - The Telnet Client must not be installed on the system.

Info

The 'Telnet Client' is not installed by default. Some protocols and services do not support required security features, such as encrypting passwords or traffic.

Solution

Uninstall 'Telnet Client' from the system.
Run 'Programs and Features'.
Select 'Turn Windows Features on or off'.
De-select 'Telnet Client'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06b.
800-53	CM-7b.
800-53R5	CM-7b.
CAT	II
CCI	CCI-000382
CN-L3	7.1.3.5(c)
CN-L3	7.1.3.7(d)
CN-L3	8.1.4.4(b)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS13b
NIAV2	SS14a
NIAV2	SS14c
PCI-DSSV3.2.1	2.2.2
PCI-DSSV4.0	2.2.4
QCSC-V1	3.2

RULE-ID	SV-253278r958480_rule
STIG-ID	WN11-00-000115
SWIFT-CSCV1	2.3
VULN-ID	V-253278

Assets

vm-win11-stig-s

```
'%windir%\System32\telnet.exe_file_does_not_exist'
```

WN11-00-000120 - The TFTP Client must not be installed on the system.

Info

The 'TFTP Client' is not installed by default. Some protocols and services do not support required security features, such as encrypting passwords or traffic.

Solution

Uninstall 'TFTP Client' from the system.
Run 'Programs and Features'.
Select 'Turn Windows Features on or off'.
De-select 'TFTP Client'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06b.
800-53	CM-7b.
800-53R5	CM-7b.
CAT	II
CCI	CCI-000382
CN-L3	7.1.3.5(c)
CN-L3	7.1.3.7(d)
CN-L3	8.1.4.4(b)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS13b
NIAV2	SS14a
NIAV2	SS14c
PCI-DSSV3.2.1	2.2.2
PCI-DSSV4.0	2.2.4
QCSC-V1	3.2

RULE-ID	SV-253279r958480_rule
STIG-ID	WN11-00-000120
SWIFT-CSCV1	2.3
VULN-ID	V-253279

Assets

vm-win11-stig-s

```
'%windir%\System32\TFTP.exe_file_does_not_exist'
```

WN11-00-000125 - Copilot must be disabled for Windows 11.

Info

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Turning off this capability will prevent potentially sensitive information from being sent outside the enterprise and uncontrolled updates to the system.

Solution

Open PowerShell as an administrator. Run the following command:
Get-AppxPackage -AllUsers *CoPilot* | Remove-AppxPackage -AllUsers

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06b.
800-53	CM-7b.
800-53R5	CM-7b.
CAT	II
CCI	CCI-000382
CN-L3	7.1.3.5(c)
CN-L3	7.1.3.7(d)
CN-L3	8.1.4.4(b)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS13b
NIAV2	SS14a
NIAV2	SS14c
PCI-DSSV3.2.1	2.2.2
PCI-DSSV4.0	2.2.4
QCSC-V1	3.2
RULE-ID	SV-268317r1135320_rule

STIG-ID	WN11-00-000125
SWIFT-CSCV1	2.3
VULN-ID	V-268317

Assets

vm-win11-stig-s

```
'Pass - No Copilot AppxPackages detected for any users'
```

WN11-00-000160 - The Server Message Block (SMB) v1 protocol must be disabled on the system.

Info

SMBv1 is a legacy protocol that uses the MD5 algorithm as part of SMB. MD5 is known to be vulnerable to a number of attacks such as collision and preimage attacks as well as not being FIPS compliant.
Disabling SMBv1 support may prevent access to file or print sharing resources with systems or devices that only support SMBv1. File shares and print services hosted on Windows Server 2003 are an example, however Windows Server 2003 is no longer a supported operating system. Some older Network Attached Storage (NAS) devices may only support SMBv1.

Solution

Disable the SMBv1 protocol.
Run 'Windows PowerShell' with elevated privileges (run as administrator).
Enter the following:
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
Alternately:
Search for 'Features'.
Select 'Turn Windows features on or off'.
De-select 'SMB 1.0/CIFS File Sharing Support'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2

RULE-ID	SV-253286r958478_rule
STIG-ID	WN11-00-000160
SWIFT-CSCV1	2.3
VULN-ID	V-253286

Assets

vm-win11-stig-s

```
'State : Disabled'
```

WN11-00-000165 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.

Info

SMBv1 is a legacy protocol that uses the MD5 algorithm as part of SMB. MD5 is known to be vulnerable to a number of attacks such as collision and preimage attacks as well as not being FIPS compliant.
Disabling SMBv1 support may prevent access to file or print sharing resources with systems or devices that only support SMBv1. File shares and print services hosted on Windows Server 2003 are an example, however Windows Server 2003 is no longer a supported operating system. Some older network attached devices may only support SMBv1.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'Configure SMBv1 Server' to 'Disabled'.
This policy setting requires the installation of the SecGuide custom templates included with the STIG package. 'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories, respectively.
The system must be restarted for the change to take effect.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253287r958478_rule

STIG-ID	WN11-00-000165
SWIFT-CSCV1	2.3
VULN-ID	V-253287

Assets

vm-win11-stig-s

PASSED

WN11-00-000170 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.

Info

SMBv1 is a legacy protocol that uses the MD5 algorithm as part of SMB. MD5 is known to be vulnerable to a number of attacks such as collision and preimage attacks as well as not being FIPS compliant.
Disabling SMBv1 support may prevent access to file or print sharing resources with systems or devices that only support SMBv1. File shares and print services hosted on Windows Server 2003 are an example, however Windows Server 2003 is no longer a supported operating system. Some older network attached devices may only support SMBv1.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'Configure SMBv1 client driver' to 'Enabled' with 'Disable driver (recommended)' selected for 'Configure MrxSmb10 driver'.
This policy setting requires the installation of the SecGuide custom templates included with the STIG package. 'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories, respectively.
The system must be restarted for the changes to take effect.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2

RULE-ID	SV-253288r958478_rule
STIG-ID	WN11-00-000170
SWIFT-CSCV1	2.3
VULN-ID	V-253288

Assets

vm-win11-stig-s

PASSED

WN11-00-000210 - Bluetooth must be turned off unless approved by the organization.

Info

If not configured properly, Bluetooth may allow rogue devices to communicate with a system. If a rogue device is paired with a system, there is potential for sensitive information to be compromised.

Solution

Turn off Bluetooth radios not organizationally approved. Establish an organizational policy for the use of Bluetooth.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253291r958478_rule
STIG-ID	WN11-00-000210
SWIFT-CSCV1	2.3
VULN-ID	V-253291

Assets

vm-win11-stig-s

```
'No entries found'
```

WN11-00-000220 - Bluetooth must be turned off when not in use.

Info

If not configured properly, Bluetooth may allow rogue devices to communicate with a system. If a rogue device is paired with a system, there is potential for sensitive information to be compromised.

Solution

Turn off Bluetooth radios when not in use. Establish an organizational policy for the use of Bluetooth to include training of personnel.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253292r958478_rule
STIG-ID	WN11-00-000220
SWIFT-CSCV1	2.3
VULN-ID	V-253292

Assets

vm-win11-stig-s

```
'No entries found'
```

WN11-00-000395 - Windows 11 must not have portproxy enabled or in use.

Info

Having portproxy enabled or configured in Windows 10 could allow a man-in-the-middle attack.

Solution

Contact the Administrator to run 'netsh interface portproxy delete' with elevation. Remove any enabled portproxies that may be configured.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-257592r991589_rule
STIG-ID	WN11-00-000395
SWIFT-CSCV1	2.3
VULN-ID	V-257592

Assets

vm-win11-stig-s

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - netsh:
 Remote value: 'Not found'
 Policy value: 'Not found'


-------------------------
PASSED - PortProxy:
 Remote value: 'HKLM\SYSTEM\CurrentControlSet\Services\PortProxy
\v4tov4\tcp_registry_does_not_exist'
 Policy value: 'HKLM\SYSTEM\CurrentControlSet\Services\PortProxy\v4tov4\tcp'
```

WN11-AC-000025 - The maximum password age must be configured to 60 days or less.

Info

The longer a password is in use, the greater the opportunity for someone to gain unauthorized knowledge of the passwords. Scheduled changing of passwords hinders the ability of unauthorized system users to crack passwords and gain access to a system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> 'Maximum Password Age' to '60' days or less (excluding '0' which is unacceptable).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.07d.
800-53	IA-5(1)(d)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000199
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(d)
NESA	T5.2.3
NIAV2	AM20
NIAV2	AM21

QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253301r1051042_rule
STIG-ID	WN11-AC-000025
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-253301

Assets

vm-win11-stig-s

42

WN11-AC-000045 - Reversible password encryption must be disabled.

Info

Storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords. For this reason, this policy must never be enabled.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> 'Store passwords using reversible encryption' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.10
800-171R3	03.05.07c.
800-53	IA-5(1)(c)
800-53R5	IA-5(1)(d)
CAT	I
CCI	CCI-000196
CCI	CCI-004062
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)(c)
NESA	T5.2.3
NIAV2	CY6
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253305r1051046_rule
STIG-ID	WN11-AC-000045

SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-253305

Assets

vm-win11-stig-s

```
'disabled'
```

WN11-AU-000030 - The system must be configured to audit Account Management - Security Group Management successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Security Group Management records events such as creating, deleting or changing of security groups, including changes in group members.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Management >> 'Audit Security Group Management' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03
800-53	AU-12(3)
800-53R5	AU-12(3)
CAT	II
CCI	CCI-001914
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-12
PCI-DSSV3.2.1	10.1

QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253308r971541_rule
STIG-ID	WN11-AU-000030
SWIFT-CSCV1	6.4
VULN-ID	V-253308

Assets

vm-win11-stig-s

```
'success'
```

WN11-AU-000040 - The system must be configured to audit Account Management - User Account Management successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
User Account Management records events such as creating, changing, deleting, renaming, disabling, or enabling user accounts.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Management >> 'Audit User Account Management' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.01
800-53	AC-2(4)
800-53R5	AC-2(4)
CAT	II
CCI	CCI-001403
CN-L3	7.1.3.2(d)
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	PR.AA-01
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18

ISO-27001-2022	A.8.2
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2(4)
NESA	T5.2.2
NIAV2	AM9a
NIAV2	AM9b
NIAV2	AM9c
NIAV2	AM9d
NIAV2	AM9e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-253310r991551_rule
STIG-ID	WN11-AU-000040
TBA-FIISB	36.2.3
VULN-ID	V-253310

Assets

vm-win11-stig-s

```
'success'
```

WN11-AU-000065 - The system must be configured to audit Logon/Logoff - Logoff successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Logoff records user logoffs. If this is an interactive logoff, it is recorded on the local system. If it is to a network share, it is recorded on the system accessed.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> 'Audit Logoff' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.12
800-171R3	03.01.12
800-53	AC-17(1)
800-53R5	AC-17(1)
CAT	II
CCI	CCI-000067
CN-L3	8.1.4.4(c)
CN-L3	8.1.10.6(i)
CSF	PR.AC-3
CSF	PR.PT-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.8.16
ISO/IEC-27001	A.6.2.2
ITSG-33	AC-17(1)
NESA	T5.4.4
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2

RULE-ID	SV-253315r958406_rule
STIG-ID	WN11-AU-000065
SWIFT-CSCV1	2.6
VULN-ID	V-253315

Assets

vm-win11-stig-s

```
'success'
```

WN11-AU-000070 - The system must be configured to audit Logon/Logoff - Logon failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Logon records user logons. If this is an interactive logon, it is recorded on the local system. If it is to a network share, it is recorded on the system accessed.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> 'Audit Logon' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253316r991581_rule
STIG-ID	WN11-AU-000070
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253316

Assets

vm-win11-stig-s

```
'success, failure'
```

WN11-AU-000075 - The system must be configured to audit Logon/Logoff - Logon successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Logon records user logons. If this is an interactive logon, it is recorded on the local system. If it is to a network share, it is recorded on the system accessed.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> 'Audit Logon' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253317r991581_rule
STIG-ID	WN11-AU-000075
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253317

Assets

vm-win11-stig-s

```
'success, failure'
```

WN11-AU-000080 - The system must be configured to audit Logon/Logoff - Special Logon successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Special Logon records special logons which have administrative privileges and can be used to elevate processes.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> 'Audit Special Logon' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253318r991578_rule
STIG-ID	WN11-AU-000080
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253318

Assets

vm-win11-stig-s

```
'success'
```

WN11-AU-000100 - The system must be configured to audit Policy Change - Audit Policy Change successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Policy Change records events related to changes in audit policy.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> 'Audit Policy Change' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253325r991572_rule
STIG-ID	WN11-AU-000100
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253325

Assets

vm-win11-stig-s

```
'success'
```

WN11-AU-000105 - The system must be configured to audit Policy Change - Authentication Policy Change successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Authentication Policy Change records events related to changes in authentication policy including Kerberos policy and Trust changes.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> 'Audit Authentication Policy Change' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04

DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253326r991572_rule
STIG-ID	WN11-AU-000105
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253326

Assets

vm-win11-stig-s

```
'success'
```

WN11-AU-000130 - The system must be configured to audit System - Other System Events successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Other System Events records information related to cryptographic key operations and the Windows Firewall service.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> 'Audit Other System Events' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253331r991579_rule
STIG-ID	WN11-AU-000130
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253331

Assets

vm-win11-stig-s

```
'success, failure'
```

WN11-AU-000135 - The system must be configured to audit System - Other System Events failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Other System Events records information related to cryptographic key operations and the Windows Firewall service.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> 'Audit Other System Events' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253332r991579_rule
STIG-ID	WN11-AU-000135
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253332

Assets

vm-win11-stig-s

```
'success, failure'
```

WN11-AU-000140 - The system must be configured to audit System - Security State Change successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Security State Change records events related to changes in the security state, such as startup and shutdown of the system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> 'Audit Security State Change' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253333r991575_rule
STIG-ID	WN11-AU-000140
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253333

Assets

vm-win11-stig-s

```
'success'
```

WN11-AU-000155 - The system must be configured to audit System - System Integrity failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
System Integrity records events related to violations of integrity to the security subsystem.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> 'Audit System Integrity' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253335r991573_rule
STIG-ID	WN11-AU-000155
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253335

Assets

vm-win11-stig-s

```
'success, failure'
```

WN11-AU-000160 - The system must be configured to audit System - System Integrity successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
System Integrity records events related to violations of integrity to the security subsystem.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> 'Audit System Integrity' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253336r991573_rule
STIG-ID	WN11-AU-000160
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253336

Assets

vm-win11-stig-s

```
'success, failure'
```

WN11-AU-000515 - Windows 11 permissions for the Application event log must prevent access by non-privileged accounts.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. The Application event log may be susceptible to tampering if proper permissions are not applied.

Solution

Ensure the permissions on the Application event log (Application.evtx) are configured to prevent standard user accounts or groups from having access. The default permissions listed below satisfy this requirement.
Eventlog - Full Control SYSTEM - Full Control Administrators - Full Control
The default location is the '%SystemRoot%\SYSTEM32\WINEVT\LOGS' directory.
If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as 'NT Service\Eventlog'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.8
800-171R3	03.03.08
800-53	AU-9
800-53R5	AU-9a.
CAT	II
CCI	CCI-000162
CN-L3	7.1.2.3(d)
CN-L3	7.1.3.3(f)
CN-L3	8.1.3.5(c)
CN-L3	8.1.4.3(c)
CSF	PR.PT-1
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.2
ITSG-33	AU-9
NESA	M5.2.3

NESA	M5.5.2
NESA	T3.6.4
NESA	T8.2.9
NIAV2	SM5
NIAV2	SM6
PCI-DSSV3.2.1	10.5
PCI-DSSV3.2.1	10.5.2
PCI-DSSV4.0	10.3.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253340r958434_rule
STIG-ID	WN11-AU-000515
VULN-ID	V-253340

Assets

vm-win11-stig-s

```
'C:\Windows\System32\winevt\Logs\Application.evtx NT SERVICE\EventLog:(I)(F)
                                                  NT AUTHORITY\SYSTEM:(I)(F)
                                                  BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files

STATUS: PASSED'
```

WN11-AU-000520 - Windows 11 permissions for the Security event log must prevent access by non-privileged accounts.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. The Security event log may disclose sensitive information or be susceptible to tampering if proper permissions are not applied.

Solution

Ensure the permissions on the Security event log (Security.evtx) are configured to prevent standard user accounts or groups from having access. The default permissions listed below satisfy this requirement.
Eventlog - Full Control SYSTEM - Full Control Administrators - Full Control
The default location is the '%SystemRoot%\SYSTEM32\WINEVT\LOGS' directory.
If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as 'NT Service\Eventlog'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.8
800-171R3	03.03.08
800-53	AU-9
800-53R5	AU-9a.
CAT	II
CCI	CCI-000162
CN-L3	7.1.2.3(d)
CN-L3	7.1.3.3(f)
CN-L3	8.1.3.5(c)
CN-L3	8.1.4.3(c)
CSF	PR.PT-1
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.2
ITSG-33	AU-9
NESA	M5.2.3

NESA	M5.5.2
NESA	T3.6.4
NESA	T8.2.9
NIAV2	SM5
NIAV2	SM6
PCI-DSSV3.2.1	10.5
PCI-DSSV3.2.1	10.5.2
PCI-DSSV4.0	10.3.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253341r958434_rule
STIG-ID	WN11-AU-000520
VULN-ID	V-253341

Assets

vm-win11-stig-s

```
'C:\Windows\System32\winevt\Logs\Security.evtx NT SERVICE\EventLog:(I)(F)
                                               NT AUTHORITY\SYSTEM:(I)(F)
                                               BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files

STATUS: PASSED'
```

WN11-AU-000525 - Windows 11 permissions for the System event log must prevent access by non-privileged accounts.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. The System event log may be susceptible to tampering if proper permissions are not applied.

Solution

Ensure the permissions on the System event log (System.evtx) are configured to prevent standard user accounts or groups from having access. The default permissions listed below satisfy this requirement.
Eventlog - Full Control SYSTEM - Full Control Administrators - Full Control
The default location is the '%SystemRoot%\SYSTEM32\WINEVT\LOGS' directory.
If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as 'NT Service\Eventlog'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.8
800-171R3	03.03.08
800-53	AU-9
800-53R5	AU-9a.
CAT	II
CCI	CCI-000162
CN-L3	7.1.2.3(d)
CN-L3	7.1.3.3(f)
CN-L3	8.1.3.5(c)
CN-L3	8.1.4.3(c)
CSF	PR.PT-1
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.2
ITSG-33	AU-9
NESA	M5.2.3

NESA	M5.5.2
NESA	T3.6.4
NESA	T8.2.9
NIAV2	SM5
NIAV2	SM6
PCI-DSSV3.2.1	10.5
PCI-DSSV3.2.1	10.5.2
PCI-DSSV4.0	10.3.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253342r958434_rule
STIG-ID	WN11-AU-000525
VULN-ID	V-253342

Assets

vm-win11-stig-s

```
'C:\Windows\System32\winevt\Logs\System.evtx NT SERVICE\EventLog:(I)(F)
                                             NT AUTHORITY\SYSTEM:(I)(F)
                                             BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files

STATUS: PASSED'
```

WN11-CC-000005 - Camera access from the lock screen must be disabled.

Info

Enabling camera access from the lock screen could allow for unauthorized use. Requiring logon will ensure the device is only used by authorized personnel.

Solution

If the device does not have a camera, this is NA.
Configure the policy value for Computer Configuration >> Administrative Templates >> Control Panel >> Personalization >> 'Prevent enabling lock screen camera' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253350r958478_rule
STIG-ID	WN11-CC-000005
SWIFT-CSCV1	2.3
VULN-ID	V-253350

Assets

vm-win11-stig-s

PASSED

WN11-CC-000007 - Windows 11 must cover or disable the built-in or attached camera when not in use.

Info

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.
Failing to disconnect from collaborative computing devices (i.e. cameras) can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure that participants actually carry out the disconnect activity without having to go through complex and tedious procedures.
Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Solution

If the camera is not disconnected or covered, the following registry entry is required.
Registry Hive: HKEY_LOCAL_MACHINE RegistryPath\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\webcam
Value Name: Value Value Data: Deny

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2

RULE-ID	SV-253351r1106508_rule
STIG-ID	WN11-CC-000007
SWIFT-CSCV1	2.3
VULN-ID	V-253351

Assets

vm-win11-stig-s

PASSED

WN11-CC-000037 - Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.

Info

A compromised local administrator account can provide means for an attacker to move laterally between domain systems.
With User Account Control enabled, filtering the privileged token for built-in administrator accounts will prevent the elevated privileges of these accounts from being used over the network.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'Apply UAC restrictions to local accounts on network logons' to 'Enabled'.
This policy setting requires the installation of the SecGuide custom templates included with the STIG package. 'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253357r958518_rule
STIG-ID	WN11-CC-000037
VULN-ID	V-253357

Assets

vm-win11-stig-s

PASSED

WN11-CC-000063 - Windows 11 systems must use either Group Policy or an approved Mobile Device Management (MDM) product to enforce STIG compliance.

Info

Without Windows 11 systems being managed, devices could be rogue and become targets of an attacker.

Solution

Configure the Windows 11 system to use either Group Policy or an approved MDM product to enforce STIG compliance.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-268318r1135322_rule
STIG-ID	WN11-CC-000063
SWIFT-CSCV1	2.3
VULN-ID	V-268318

Assets

vm-win11-stig-s

PASSED

WN11-CC-000075 - Credential Guard must be running on Windows 11 domain-joined systems.

Info

Credential Guard uses virtualization-based security to protect information that could be used in credential theft attacks if compromised. This authentication information, which was stored in the Local Security Authority (LSA) in previous versions of Windows, is isolated from the rest of operating system and can only be accessed by privileged system software.

Solution

Virtualization-based security, including Credential Guard, currently cannot be implemented in virtual desktop implementations (VDI) due to specific supporting requirements including a TPM, UEFI with Secure Boot, and the capability to run the Hyper-V feature within the virtual desktop.
For VDIs where the virtual desktop instance is deleted or refreshed upon logoff, this is NA.
For VDIs with persistent desktops, this may be downgraded to a CAT II only where administrators have specific tokens for the VDI. Administrator accounts on virtual desktops must only be used on systems in the VDI; they may not have administrative privileges on any other systems such as servers and physical workstations.
Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Device Guard >> 'Turn On virtualization-based Security' to 'Enabled' with 'Enabled with UEFI lock' selected for 'Credential Guard Configuration:'.
A Microsoft TechNet article on Credential Guard, including system requirement details, can be found at the following link:
https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253370r991589_rule
STIG-ID	WN11-CC-000075

SWIFT-CSCV1	2.3
VULN-ID	V-253370

Assets

vm-win11-stig-s

PASSED

WN11-CC-000080 - Virtualization-based protection of code integrity must be enabled.

Info

Virtualization-based protection of code integrity enforces kernel mode memory protections as well as protecting Code Integrity validation paths. This isolates the processes from the rest of the operating system and can only be accessed by privileged system software.

Solution

Virtualization-based security currently cannot be implemented in virtual desktop implementations (VDI) due to specific supporting requirements including a TPM, UEFI with Secure Boot, and the capability to run the Hyper-V feature within the virtual desktop.
For VDIs where the virtual desktop instance is deleted or refreshed upon logoff, this is NA.
Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Device Guard >> 'Turn On virtualization-based Security' to 'Enabled' with 'Enabled with UEFI lock' or 'Enabled without lock' selected for 'virtualization-based Protection of Code Integrity:'.
'Enabled with UEFI lock' is preferred as more secure, however it cannot be turned off remotely through a group policy change if there is an issue.
'Enabled without lock' will allow this to be turned off remotely while testing for issues.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253371r991589_rule
STIG-ID	WN11-CC-000080
SWIFT-CSCV1	2.3
VULN-ID	V-253371

Assets

vm-win11-stig-s

PASSED

WN11-CC-000115 - Systems must at least attempt device authentication using certificates.

Info

Using certificates to authenticate devices to the domain provides increased security over passwords. By default systems will attempt to authenticate using certificates and fall back to passwords if the domain controller does not support certificates for devices. This may also be configured to always use certificates for device authentication.

Solution

This requirement is applicable to domain-joined systems, for standalone systems this is NA.
The default behavior for 'Support device authentication using certificate' is 'Automatic'.
To correct this, configured the policy value for Computer Configuration >> Administrative Templates >> System >> Kerberos >> 'Support device authentication using certificate' to 'Not Configured or 'Enabled' with either option selected in 'Device authentication behavior using certificate:'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253377r991589_rule
STIG-ID	WN11-CC-000115
SWIFT-CSCV1	2.3
VULN-ID	V-253377

Assets

vm-win11-stig-s

PASSED

WN11-CC-000130 - Local users on domain-joined computers must not be enumerated.

Info

The username is one part of logon credentials that could be used to gain access to a system. Preventing the enumeration of users limits this information to authorized personnel.

Solution

This requirement is applicable to domain-joined systems, for standalone systems this is NA.
Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Logon >> 'Enumerate local users on domain-joined computers' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253379r958478_rule
STIG-ID	WN11-CC-000130
SWIFT-CSCV1	2.3
VULN-ID	V-253379

Assets

vm-win11-stig-s

PASSED

WN11-SO-000085 - Caching of logon credentials must be limited.

Info

The default Windows configuration caches the last logon credentials for users who log on interactively to a system. This feature is provided for system availability reasons, such as the user's machine being disconnected from the network or domain controllers being unavailable. Even though the credential cache is well-protected, if a system is attacked, an unauthorized individual may isolate the password to a domain user account using a password-cracking program and gain access to the domain.

Solution

This is the default configuration for this setting (10 logons to cache).
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '10' logons or less.
This setting only applies to domain-joined systems, however, it is configured by default on all systems.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253447r991589_rule
STIG-ID	WN11-SO-000085
SWIFT-CSCV1	2.3
VULN-ID	V-253447

Assets

vm-win11-stig-s

PASSED

WN11-SO-000160 - The system must be configured to prevent anonymous users from having the same rights as the Everyone group.

Info

Access by anonymous users must be restricted. If this setting is enabled, then anonymous users have the same rights and permissions as the built-in Everyone group. Anonymous users must not have these permissions or rights.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253455r991589_rule
STIG-ID	WN11-SO-000160
SWIFT-CSCV1	2.3
VULN-ID	V-253455

Assets

vm-win11-stig-s

0

WN11-SO-000251 - Windows 11 must use multifactor authentication for local and network access to privileged and nonprivileged accounts.

Info

Without the use of multifactor authentication, the ease of access to privileged and nonprivileged functions is greatly increased.
All domain accounts must be enabled for multifactor authentication with the exception of local emergency accounts.
Multifactor authentication requires using two or more factors to achieve authentication.
Factors include:
1) Something a user knows (e.g., password/PIN);
2) Something a user has (e.g., cryptographic identification device, token); and
3) Something a user is (e.g., biometric).
A privileged account is defined as an information system account with authorizations of a privileged user.
Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet).
Local access is defined as access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
The DoD CAC with DoD-approved PKI is an example of multifactor authentication.
Satisfies: SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

Solution

For nondomain joined systems, configuring Windows Hello for sign-on options would be suggested based on the organization's needs and capabilities.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.3
800-171R3	03.05.03
800-53	IA-2(1)
800-53R5	IA-2(1)
CAT	II
CCI	CCI-000765
CN-L3	7.1.2.7(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-2(1)
NESA	T5.4.2

NIAV2	AM36
NIAV2	VL3c
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253470r1106510_rule
STIG-ID	WN11-SO-000251
SWIFT-CSCV1	1.2
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-253470

Assets

vm-win11-stig-s

PASSED

WN11-UR-000075 - The 'Deny log on as a batch job' user right on domain-joined workstations must be configured to prevent access from highly privileged domain accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Deny log on as a batch job' right defines accounts that are prevented from logging on to the system as a batch job, such as Task Scheduler.
In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks which could lead to the compromise of an entire domain.

Solution

This requirement is applicable to domain-joined systems, for standalone systems this is NA.
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on as a batch job' to include the following:
Domain Systems Only:
Enterprise Admin Group Domain Admin Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253492r1137691_rule
STIG-ID	WN11-UR-000075
TBA-FIISB	31.1
VULN-ID	V-253492

Assets

vm-win11-stig-s

PASSED

WN11-UR-000080 - The 'Deny log on as a service' user right on Windows 11 domain-joined workstations must be configured to prevent access from highly privileged domain accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Deny log on as a service' right defines accounts that are denied log on as a service.
In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks which could lead to the compromise of an entire domain.
Incorrect configurations could prevent services from starting and result in a DoS.

Solution

This requirement is applicable to domain-joined systems, for standalone systems this is NA.
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on as a service' to include the following:
Domain Systems Only:
Enterprise Admins Group Domain Admins Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253493r1137691_rule
STIG-ID	WN11-UR-000080
TBA-FIISB	31.1
VULN-ID	V-253493

Assets

vm-win11-stig-s

PASSED

Audits INFO,WARNING,ERROR

WN11-00-000015 - Windows 11 systems must have Unified Extensible Firmware Interface (UEFI) firmware and be configured to run in UEFI mode, not Legacy BIOS.

Info

UEFI provides additional security features in comparison to legacy BIOS firmware, including Secure Boot. UEFI is required to support additional security features in Windows 11, including virtualization-based Security and Credential Guard. Systems with UEFI that are operating in Legacy BIOS mode will not support these security features.

Solution

Configure UEFI firmware to run in UEFI mode, not Legacy BIOS mode.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8(1)
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14

ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8(1)
NESA	T7.4.1
NIAV2	NS5d
NIAV2	NS6b
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253256r1117271_rule
STIG-ID	WN11-00-000015
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253256

Assets

vm-win11-stig-s

WN11-00-000025 - Windows 11 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: Continuously, where ESS is used; 30 days, for any additional internal network scans not covered by ESS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).

Info

An approved tool for continuous network scanning must be installed and configured to run.
Without the use of automated mechanisms to scan for security flaws on a continuous and/or periodic basis, the operating system or other system components may remain vulnerable to the exploits presented by undetected software flaws.
To support this requirement, the operating system may have an integrated solution incorporating continuous scanning using ESS and periodic scanning using other tools, as specified in the requirement.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Install DOD-approved ESS software and ensure it is operating continuously.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253258r1000099_rule
STIG-ID	WN11-00-000025
SWIFT-CSCV1	2.3
VULN-ID	V-253258

Assets

vm-win11-stig-s

WN11-00-000030 - Windows 11 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.

Info

If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Enable full disk encryption on all information systems (including SIPRNet) using BitLocker.
BitLocker, included in Windows, can be enabled in the Control Panel under 'BitLocker Drive Encryption' as well as other management tools.
Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and satisfies the pre-boot authentication requirements (WN11-00-000031 and WN11-00-000032).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.16
800-171R3	03.13.08
800-53	SC-28(1)
800-53R5	SC-28(1)
CAT	I
CCI	CCI-002475
CN-L3	8.1.4.7(b)
CN-L3	8.1.4.8(b)
CSF	PR.DS-1
CSF2.0	PR.DS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.33
ITSG-33	SC-28(1)
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1

QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253259r958870_rule
STIG-ID	WN11-00-000030
TBA-FIISB	28.1
VULN-ID	V-253259

Assets

vm-win11-stig-s

```
'VolumeType       : OperatingSystem
MountPoint       : C:
ProtectionStatus : Off

VolumeType       : Data
MountPoint       : D:
ProtectionStatus : Off



Some disks not encrypted.'
```

WN11-00-000035 - The operating system must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

Info

Utilizing an allowlist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities.
The organization must identify authorized software programs and only permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as allowlisting.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure an application allowlisting program to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.
Configuration of allowlisting applications will vary by the program. AppLocker is an allowlisting application built into Windows 11 Enterprise.
If AppLocker is used, it is configured through group policy in Computer Configuration >> Windows Settings >> Security Settings >> Application Control Policies >> AppLocker.
Implementation guidance for AppLocker is available in the NSA paper 'Application allowlisting using Microsoft AppLocker' at the following link:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-policies-deployment-guide

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.8
800-171R3	03.04.08b.
800-53	CM-7(5)(b)
800-53R5	CM-7(5)(b)
CAT	II
CCI	CCI-001774
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.19
ISO/IEC-27001	A.12.5.1
ISO/IEC-27001	A.12.6.2
ITSG-33	CM-7
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2

QCSC-V1	3.2
RULE-ID	SV-253262r958808_rule
STIG-ID	WN11-00-000035
SWIFT-CSCV1	2.3
TBA-FIISB	44.2.2
TBA-FIISB	49.2.3
VULN-ID	V-253262

Assets

vm-win11-stig-s

```
'<AppLockerPolicy Version="1" />'
```

WN11-00-000055 - Alternate operating systems must not be permitted on the same system.

Info

Allowing other operating systems to run on a secure system may allow security to be circumvented.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Ensure Windows 11 is the only operating system on a device. Remove alternate operating systems.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253266r991589_rule
STIG-ID	WN11-00-000055
SWIFT-CSCV1	2.3
VULN-ID	V-253266

Assets

vm-win11-stig-s

WN11-00-000060 - Non-system-created file shares on a system must limit access to groups that require it.

Info

Shares which provide network access, must not exist on a workstation except for system-created administrative shares, and could potentially expose sensitive information. If a share is necessary, share permissions, as well as NTFS permissions, must be reconfigured to give the minimum access to those accounts that require it.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

If a non-system-created share is required on a system, configure the share and NTFS permissions to limit access to the specific groups or accounts that require it.
Remove any unnecessary non-system-created shares.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.4
800-171R3	03.13.04
800-53	SC-4
800-53R5	SC-4
CAT	II
CCI	CCI-001090
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-253267r1137695_rule
STIG-ID	WN11-00-000060
VULN-ID	V-253267

Assets

vm-win11-stig-s

WN11-00-000065 - Unused accounts must be disabled or removed from the system after 35 days of inactivity.

Info

Outdated or unused accounts provide penetration points that may go undetected. Inactive accounts must be deleted if no longer necessary or, if still required, disable until needed.
Satisfies: SRG-OS-000468-GPOS-00212, SRG-OS-000118-GPOS-00060
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Review local accounts and verify their necessity. Disable or delete any active accounts that have not been used in the last 35 days.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171	3.5.5
800-171	3.5.6
800-171R3	03.03.03a.
800-171R3	03.05.05
800-53	AU-12c.
800-53	IA-4e.
800-53R5	AC-2(3)(a)
800-53R5	AU-12c.
CAT	III
CCI	CCI-000172
CCI	CCI-000795
CCI	CCI-003627
CN-L3	7.1.2.7(b)
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3

CSF	DE.CM-7
CSF	PR.AC-1
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-01
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(b)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
ITSG-33	IA-4e.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	8.1.4
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	8.2.6
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

RULE-ID	SV-253268r1051039_rule
STIG-ID	WN11-00-000065
SWIFT-CSCV1	5
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253268

Assets

vm-win11-stig-s

WN11-00-000070 - Only accounts responsible for the administration of a system must have Administrator rights on the system.

Info

An account that does not have Administrator duties must not have Administrator rights. Such rights would allow the account to bypass or modify required security restrictions on that machine and make it vulnerable to attack.
System administrators must log on to systems only using accounts with the minimum level of authority necessary.
For domain-joined workstations, the Domain Admins group must be replaced by a domain workstation administrator group (see V-36434 in the Active Directory Domain STIG). Restricting highly privileged accounts from the local Administrators group helps mitigate the risk of privilege escalation resulting from credential theft attacks.
Standard user accounts must not be members of the local administrators group.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure the system to include only administrator groups or accounts that are responsible for the system in the local Administrators group.
For domain-joined workstations, the Domain Admins group must be replaced by a domain workstation administrator group.
Remove any standard user accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3(4)
800-53R5	AC-3(4)
CAT	I
CCI	CCI-002165
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3(4)
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253269r958702_rule
STIG-ID	WN11-00-000070
TBA-FIISB	31.1
VULN-ID	V-253269

Assets

vm-win11-stig-s

```
'Finding: vm-win11-stig-s\Guest is a standard user account in the local Administrators group.
Finding: vm-win11-stig-s\tazdevil4 is a standard user account in the local Administrators group.'
```

WN11-00-000130 - Software certificate installation files must be removed from Windows 11.

Info

Use of software certificates and their accompanying installation files for end users to access resources is less secure than the use of hardware-based certificates.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Remove any certificate installation files (*.p12 and *.pfx) found on a system.
Note: This does not apply to server-based applications that have a requirement for .p12 certificate files (e.g., Oracle Wallet Manager) or Adobe PreFlight certificate files.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253280r991589_rule
STIG-ID	WN11-00-000130
SWIFT-CSCV1	2.3
VULN-ID	V-253280

Assets

vm-win11-stig-s

WN11-00-000140 - Inbound exceptions to the firewall on Windows 11 domain workstations must only allow authorized remote management hosts.

Info

Allowing inbound access to domain workstations from other systems may allow lateral movement across systems if credentials are compromised. Limiting inbound connections only from authorized remote management systems will help limit this exposure.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure firewall exceptions to inbound connections on domain workstations to include only authorized remote management hosts.
Configure only inbound connection exceptions for authorized remote management hosts.
Computer Configuration >> Windows Settings >> Security Settings >> Windows Defender Firewall with Advanced Security >> Windows Defender Firewall with Advanced Security >> Inbound Rules (this link will be in the right pane)
For any inbound rules that allow connections, configure the Scope for Remote IP address to those of authorized remote management hosts. This may be defined as an IP address, subnet or range. Apply the rule to all firewall profiles.
If a third-party firewall is used, configure inbound exceptions to only include authorized remote management hosts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253282r991593_rule
STIG-ID	WN11-00-000140
SWIFT-CSCV1	2.3
VULN-ID	V-253282

```
 'DisplayName : Wi-Fi Direct Spooler Use (In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - IPv6 (IPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Delivery Optimization (UDP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Router Advertisement (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Dynamic Host Configuration Protocol (DHCP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery (WSD-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery for Teredo (SSDP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Wi-Fi Direct Scan Service Use (In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery (WSD-In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery (WSD Events-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Remote Assistance (DCOM-In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery (WSD EventsSecure-In)
Enabled     : True
Direction   : Inbound

DisplayName : Remote Assistance (RA Server TCP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery (UPnP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Microsoft Media Foundation Network Source IN [UDP 5004-5009]
Enabled     : True
Direction   : Inbound
```

```
DisplayName : Delivery Optimization (TCP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Router Solicitation (ICMPv6-In)
Enabled     : True
Direction [...]
```

WN11-00-000190 - Orphaned security identifiers (SIDs) must be removed from user rights on Windows 11.

Info

Accounts or groups given rights on a system may show up as unresolved SIDs for various reasons including deletion of the accounts or groups. If the account or group objects are reanimated, there is a potential they may still have rights no longer intended. Valid domain accounts or groups may also show up as unresolved SIDs if a connection to the domain cannot be established for some reason.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Remove any unresolved SIDs found in User Rights assignments and determined to not be for currently valid accounts or groups by removing the accounts or groups from the appropriate group policy.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253290r991589_rule
STIG-ID	WN11-00-000190
SWIFT-CSCV1	2.3
VULN-ID	V-253290

Assets

vm-win11-stig-s

WN11-00-000230 - The system must notify the user when a Bluetooth device attempts to connect.

Info

If not configured properly, Bluetooth may allow rogue devices to communicate with a system. If a rogue device is paired with a system, there is potential for sensitive information to be compromised.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure Bluetooth to notify users if devices attempt to connect.
View Bluetooth Settings.
Ensure 'Alert me when a new Bluetooth device wants to connect' is checked.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253293r991589_rule
STIG-ID	WN11-00-000230
SWIFT-CSCV1	2.3
VULN-ID	V-253293

Assets

vm-win11-stig-s

```
Non-compliant items:
  HKU\S-1-5-21-2746855186-1286860024-2359785572-500\Software\Microsoft
\BluetoothAuthenticationAgent - 2
```

WN11-00-000240 - Administrative accounts must not be used with applications that access the internet, such as web browsers, or with potential internet sources, such as email.

Info

Using applications that access the internet or have potential internet sources using administrative privileges exposes a system to compromise. If a flaw in an application is exploited while running as a privileged user, the entire system could be compromised. Web browsers and email are common attack vectors for introducing malicious code and must not be run with an administrative account.
Since administrative accounts may generally change or work around technical restrictions for running a web browser or other applications, it is essential that policy requires administrative accounts to not access the internet or use applications, such as email.
The policy must define specific exceptions for local service administration. These exceptions may include HTTP(S)-based tools that are used for the administration of the local system, services, or attached devices.
Technical means such as application allowlisting can be used to enforce the policy to ensure compliance.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Establish and enforce a policy that prohibits administrative accounts from using applications that access the internet, such as web browsers, or with potential internet sources, such as email. Define specific exceptions for local service administration. These exceptions may include HTTP(S)-based tools that are used for the administration of the local system, services, or attached devices.
Implement technical measures where feasible such as removal of applications or use of application allowlisting to restrict the use of applications that can access the internet.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253294r991589_rule
STIG-ID	WN11-00-000240

SWIFT-CSCV1	2.3
VULN-ID	V-253294

Assets

vm-win11-stig-s

WN11-00-000250 - Windows 11 nonpersistent VM sessions must not exceed 24 hours.

Info

For virtual desktop implementations (VDIs) where the virtual desktop instance is deleted or refreshed upon logoff, the organization must enforce that sessions be terminated within 24 hours. This would ensure any data stored on the VM that is not encrypted or covered by Credential Guard is deleted.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Set nonpersistent VM sessions to not exceed 24 hours.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.16
800-171R3	03.13.08
800-53	SC-28
800-53R5	SC-28
CAT	II
CCI	CCI-001199
CN-L3	8.1.4.7(b)
CN-L3	8.1.4.8(b)
CSF	PR.DS-1
CSF2.0	PR.DS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.33
ITSG-33	SC-28
ITSG-33	SC-28a.
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1
QCSC-V1	5.2.2

QCSC-V1	6.2
RULE-ID	SV-253295r958552_rule
STIG-ID	WN11-00-000250
VULN-ID	V-253295

Assets

vm-win11-stig-s

WN11-00-000260 - The Windows 11 time service must synchronize with an appropriate DOD time source.

Info

The Windows Time Service controls time synchronization settings. Time synchronization is essential for authentication and auditing purposes. If the Windows Time Service is used, it must synchronize with a secure, authorized time source. Domain-joined systems are automatically configured to synchronize with domain controllers. If an NTP server is configured, it must synchronize with a secure, authorized time source.

Solution

Configure the system to synchronize time with an appropriate DOD time source.
Domain-joined systems use NT5DS to synchronize time from other systems in the domain by default.
If the system needs to be configured to an NTP server, configure the system to point to an authorized time server by setting the policy value for Computer Configuration >> Administrative Templates >> System >> Windows Time Service >> Time Providers >> 'Configure Windows NTP Client' to 'Enabled', and configure the 'NtpServer' field to point to an appropriate DOD time server.
The US Naval Observatory operates stratum 1 time servers, identified at https://www.cnmoc.usff.navy.mil/Our-Commands/United-States-Naval-Observatory/Precise-Time-Department/Network-Time-Protocol-NTP/. Time synchronization will occur through a hierarchy of time servers down to the local level. Clients and lower-level servers will synchronize with an authorized time server in the hierarchy.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.7
800-171R3	03.03.07
800-53	AU-8(1)(a)
800-53R5	SC-45(1)(a)
CAT	III
CCI	CCI-001891
CCI	CCI-004923
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.17
ISO/IEC-27001	A.12.4.4
ITSG-33	AU-8(1)
NESA	T3.6.7
NIAV2	NS44
NIAV2	NS45

NIAV2	NS46
NIAV2	NS47
PCI-DSSV3.2.1	10.4
PCI-DSSV3.2.1	10.4.1
PCI-DSSV3.2.1	10.4.3
PCI-DSSV4.0	10.6
PCI-DSSV4.0	10.6.1
PCI-DSSV4.0	10.6.2
PCI-DSSV4.0	10.6.3
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253296r1051041_rule
STIG-ID	WN11-00-000260
TBA-FIISB	37.4
VULN-ID	V-253296

Assets
vm-win11-stig-s

WN11-CC-000010 - The display of slide shows on the lock screen must be disabled.

Info

Slide shows that are displayed on the lock screen could display sensitive information to unauthorized personnel. Turning off this feature will limit access to the information to a logged on user.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Control Panel >> Personalization >> 'Prevent enabling lock screen slide show' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253352r958478_rule
STIG-ID	WN11-CC-000010
SWIFT-CSCV1	2.3
VULN-ID	V-253352

Assets

vm-win11-stig-s

WN11-CC-000020 - IPv6 source routing must be configured to highest protection.

Info

Configuring the system to disable IPv6 source routing protects against spoofing.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'.
This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. 'MSS-Legacy.admx' and 'MSS-Legacy.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253353r991589_rule
STIG-ID	WN11-CC-000020
SWIFT-CSCV1	2.3
VULN-ID	V-253353

Assets

vm-win11-stig-s

WN11-CC-000025 - The system must be configured to prevent IP source routing.

Info

Configuring the system to disable IP source routing protects against spoofing.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'.
This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. 'MSS-Legacy.admx' and 'MSS-Legacy.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253354r991589_rule
STIG-ID	WN11-CC-000025
SWIFT-CSCV1	2.3
VULN-ID	V-253354

Assets

vm-win11-stig-s

WN11-CC-000030 - The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.

Info

Allowing ICMP redirect of routes can lead to traffic not being routed properly. When disabled, this forces ICMP to be routed via shortest path first.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' to 'Disabled'.
This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. 'MSS-Legacy.admx' and 'MSS-Legacy.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253355r991589_rule
STIG-ID	WN11-CC-000030
SWIFT-CSCV1	2.3
VULN-ID	V-253355

Assets

vm-win11-stig-s

WN11-CC-000035 - The system must be configured to ignore NetBIOS name release requests except from WINS servers.

Info

Configuring the system to ignore name release requests, except from WINS servers, prevents a denial of service (DoS) attack. The DoS consists of sending a NetBIOS name release request to the server for each entry in the server's cache, causing a response delay in the normal operation of the servers WINS resolution capability.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' to 'Enabled'.
This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. 'MSS-Legacy.admx' and 'MSS-Legacy.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SC-5
800-53R5	SC-5a.
CAT	III
CCI	CCI-002385
CSF	DE.CM-1
CSF	PR.DS-4
CSF2.0	DE.CM-01
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-5
ITSG-33	SC-5a.
NESA	T3.3.1
NIAV2	GS8e
NIAV2	GS10c
QCSC-V1	8.2.1
RULE-ID	SV-253356r958902_rule
STIG-ID	WN11-CC-000035
VULN-ID	V-253356

Assets

vm-win11-stig-s

WN11-CC-000038 - WDigest Authentication must be disabled.

Info

When the WDigest Authentication protocol is enabled, plain text passwords are stored in the Local Security Authority Subsystem Service (LSASS) exposing them to theft. WDigest is disabled by default in Windows 11. This setting ensures this is enforced.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'WDigest Authentication (disabling may require KB2871997)' to 'Disabled'.
The patch referenced in the policy title is not required for Windows 11.
This policy setting requires the installation of the SecGuide custom templates included with the STIG package. 'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253358r958478_rule
STIG-ID	WN11-CC-000038

SWIFT-CSCV1	2.3
VULN-ID	V-253358

Assets

vm-win11-stig-s

WN11-CC-000040 - Insecure logons to an SMB server must be disabled.

Info

Insecure guest logons allow unauthenticated access to shared folders. Shared resources on a system must require authentication to establish proper access.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Lanman Workstation >> 'Enable insecure guest logons' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253360r991589_rule
STIG-ID	WN11-CC-000040
SWIFT-CSCV1	2.3
VULN-ID	V-253360

Assets

vm-win11-stig-s

WN11-CC-000044 - Internet connection sharing must be disabled.

Info

Internet connection sharing makes it possible for an existing internet connection, such as through wireless, to be shared and used by other systems essentially creating a mobile hotspot. This exposes the system sharing the connection to others with potentially malicious purpose.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Network Connections >> 'Prohibit use of Internet Connection Sharing on your DNS domain network' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253361r958478_rule
STIG-ID	WN11-CC-000044
SWIFT-CSCV1	2.3
VULN-ID	V-253361

Assets

vm-win11-stig-s

WN11-CC-000052 - Windows 11 must be configured to prioritize ECC Curves with longer key lengths first.

Info

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. By default Windows uses ECC curves with shorter key lengths first. Requiring ECC curves with longer key lengths to be prioritized first helps ensure more secure algorithms are used.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> SSL Configuration Settings >> 'ECC Curve Order' to 'Enabled' with 'ECC Curve Order:' including the following in the order listed: NistP384 NistP256

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	IA-7
800-53R5	IA-7
CAT	II
CCI	CCI-000803
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
ITSG-33	IA-7
ITSG-33	IA-7a.
NESA	M5.2.1
NESA	M5.2.6
NESA	M5.3.1
NESA	T7.4.1
QCSC-V1	13.2
RULE-ID	SV-253363r971535_rule
STIG-ID	WN11-CC-000052
VULN-ID	V-253363

Assets

vm-win11-stig-s

WN11-CC-000055 - Simultaneous connections to the internet or a Windows domain must be limited.

Info

Multiple network connections can provide additional attack vectors to a system and must be limited. The 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' setting prevents systems from automatically establishing multiple connections. When both wired and wireless connections are available, for example, the less preferred connection (typically wireless) will be disconnected.

Solution

The default behavior for 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is 'Enabled'.
If this needs to be corrected, configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Windows Connection Manager >> 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' to 'Enabled'. Under 'Options', set 'Minimize Policy Options' to '3 = Prevent Wi-Fi When on Ethernet'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53R5	SC-8
CAT	II
CCI	CCI-002418
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)

ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ITSG-33	SC-8
ITSG-33	SC-8a.
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253364r958358_rule
STIG-ID	WN11-CC-000055
VULN-ID	V-253364

Assets

vm-win11-stig-s

WN11-CC-000060 - Connections to non-domain networks when connected to a domain authenticated network must be blocked.

Info

Multiple network connections can provide additional attack vectors to a system and must be limited. When connected to a domain, communication must go through the domain connection.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Windows Connection Manager >> 'Prohibit connection to non-domain networks when connected to domain authenticated network' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253365r991589_rule
STIG-ID	WN11-CC-000060
SWIFT-CSCV1	2.3
VULN-ID	V-253365

Assets

vm-win11-stig-s

WN11-CC-000065 - Wi-Fi Sense must be disabled.

Info

Wi-Fi Sense automatically connects the system to known hotspots and networks that contacts have shared. It also allows the sharing of the system's known networks to contacts. Automatically connecting to hotspots and shared networks can expose a system to unsecured or potentially malicious systems.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> WLAN Service >> WLAN Settings>> 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253366r991589_rule
STIG-ID	WN11-CC-000065
SWIFT-CSCV1	2.3
VULN-ID	V-253366

Assets

vm-win11-stig-s

WN11-CC-000066 - Command line data must be included in process creation events.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Enabling 'Include command line data for process creation events' will record the command line information with the process creation events in the log. This can provide additional detail when malware has run on a system.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Audit Process Creation >> 'Include command line in process creation events' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02b.
800-53	AU-3(1)
800-53R5	AU-3(1)
CAT	II
CCI	CCI-000135
CN-L3	7.1.3.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3(1)
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d

NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253367r958422_rule
STIG-ID	WN11-CC-000066
SWIFT-CSCV1	6.4
VULN-ID	V-253367

Assets

vm-win11-stig-s

WN11-CC-000068 - Windows 11 must be configured to enable Remote host allows delegation of non-exportable credentials.

Info

An exportable version of credentials is provided to remote hosts when using credential delegation which exposes them to theft on the remote host. Restricted Admin mode or Remote Credential Guard allow delegation of non-exportable credentials providing additional protection of the credentials. Enabling this configures the host to support Restricted Admin mode or Remote Credential Guard.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Credentials Delegation >> 'Remote host allows delegation of non-exportable credentials' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253368r991589_rule
STIG-ID	WN11-CC-000068
SWIFT-CSCV1	2.3
VULN-ID	V-253368

Assets

vm-win11-stig-s

WN11-CC-000085 - Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers.

Info

The default behavior is for Early Launch Antimalware - Boot-Start Driver Initialization policy is to enforce 'Good, unknown and bad but critical' (preventing 'bad'). By being launched first by the kernel, ELAM (Early Launch Antimalware) is ensured to be launched before any third-party software, and is therefore able to detect malware in the boot process and prevent it from initializing.

Solution

Ensure that Early Launch Antimalware - Boot-Start Driver Initialization policy is set to enforce 'Good, unknown and bad but critical' (preventing 'bad').
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> System >> Early Launch Antimalware >> 'Boot-Start Driver Initialization Policy' to 'Enabled with 'Good, unknown and bad but critical' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253372r991589_rule
STIG-ID	WN11-CC-000085
SWIFT-CSCV1	2.3
VULN-ID	V-253372

Assets

vm-win11-stig-s

WN11-CC-000090 - Group Policy objects must be reprocessed even if they have not changed.

Info

Enabling this setting and then selecting the 'Process even if the Group Policy objects have not changed' option ensures that the policies will be reprocessed even if none have been changed. This way, any unauthorized changes are forced to match the domain-based group policy settings again.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Group Policy >> 'Configure registry policy processing' to 'Enabled' and select the option 'Process even if the Group Policy objects have not changed'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253373r991589_rule
STIG-ID	WN11-CC-000090
SWIFT-CSCV1	2.3
VULN-ID	V-253373

Assets

vm-win11-stig-s

WN11-CC-000100 - Downloading print driver packages over HTTP must be prevented.

Info

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Turning off this capability will prevent potentially sensitive information from being sent outside the enterprise and uncontrolled updates to the system. This setting prevents the computer from downloading print driver packages over HTTP.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Internet Communication Management >> Internet Communication settings >> 'Turn off downloading of print drivers over HTTP' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253374r958478_rule
STIG-ID	WN11-CC-000100
SWIFT-CSCV1	2.3

VULN-ID	V-253374

Assets

vm-win11-stig-s

WN11-CC-000105 - Web publishing and online ordering wizards must be prevented from downloading a list of providers.

Info

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Turning off this capability will prevent potentially sensitive information from being sent outside the enterprise and uncontrolled updates to the system. This setting prevents Windows from downloading a list of providers for the Web publishing and online ordering wizards.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Internet Communication Management >> Internet Communication settings >> 'Turn off Internet download for Web publishing and online ordering wizards' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253375r958478_rule
STIG-ID	WN11-CC-000105

SWIFT-CSCV1	2.3
VULN-ID	V-253375

Assets

vm-win11-stig-s

WN11-CC-000110 - Printing over HTTP must be prevented.

Info

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Turning off this capability will prevent potentially sensitive information from being sent outside the enterprise and uncontrolled updates to the system. This setting prevents the client computer from printing over HTTP, which allows the computer to print to printers on the intranet as well as the internet.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Internet Communication Management >> Internet Communication settings >> 'Turn off printing over HTTP' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253376r958478_rule
STIG-ID	WN11-CC-000110
SWIFT-CSCV1	2.3

VULN-ID	V-253376

Assets

vm-win11-stig-s

WN11-CC-000120 - The network selection user interface (UI) must not be displayed on the logon screen.

Info

Enabling interaction with the network selection UI allows users to change connections to available networks without signing into Windows.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Logon >> 'Do not display network selection UI' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253378r958478_rule
STIG-ID	WN11-CC-000120
SWIFT-CSCV1	2.3
VULN-ID	V-253378

Assets

vm-win11-stig-s

WN11-CC-000145 - Users must be prompted for a password on resume from sleep (on battery).

Info

Authentication must always be required when accessing a system. This setting ensures the user is prompted for a password on resume from sleep (on battery).

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Power Management >> Sleep Settings >> 'Require a password when a computer wakes (on battery)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253380r1051049_rule
STIG-ID	WN11-CC-000145
VULN-ID	V-253380

Assets

vm-win11-stig-s

WN11-CC-000150 - The user must be prompted for a password on resume from sleep (plugged in).

Info

Authentication must always be required when accessing a system. This setting ensures the user is prompted for a password on resume from sleep (plugged in).

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Power Management >> Sleep Settings >> 'Require a password when a computer wakes (plugged in)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253381r1051050_rule
STIG-ID	WN11-CC-000150
VULN-ID	V-253381

Assets

vm-win11-stig-s

WN11-CC-000155 - Solicited Remote Assistance must not be allowed.

Info

Remote assistance allows another user to view or take control of the local session of a user. Solicited assistance is help that is specifically requested by the local user. This may allow unauthorized parties access to the resources on the computer.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Remote Assistance >> 'Configure Solicited Remote Assistance' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.4
800-171R3	03.13.04
800-53	SC-4
800-53R5	SC-4
CAT	I
CCI	CCI-001090
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-253382r1137695_rule
STIG-ID	WN11-CC-000155
VULN-ID	V-253382

Assets

vm-win11-stig-s

WN11-CC-000165 - Unauthenticated RPC clients must be restricted from connecting to the RPC server.

Info

Configuring RPC to restrict unauthenticated RPC clients from connecting to the RPC server will prevent anonymous connections.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Remote Procedure Call >> 'Restrict Unauthenticated RPC clients' to 'Enabled' and 'Authenticated'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171R3	03.05.02
800-53	IA-3(1)
800-53R5	IA-3(1)
CAT	II
CCI	CCI-001967
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-3(1)
NESA	T5.4.3
QCSC-V1	13.2
RULE-ID	SV-253383r971545_rule
STIG-ID	WN11-CC-000165
TBA-FIISB	27.1
VULN-ID	V-253383

Assets

vm-win11-stig-s

WN11-CC-000170 - The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.

Info

Control of credentials and the system must be maintained within the enterprise. Enabling this setting allows enterprise credentials to be used with modern style apps that support this, instead of Microsoft accounts.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> App Runtime >> 'Allow Microsoft accounts to be optional' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253384r991589_rule
STIG-ID	WN11-CC-000170
SWIFT-CSCV1	2.3
VULN-ID	V-253384

Assets

vm-win11-stig-s

WN11-CC-000175 - The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.

Info

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Turning off this capability will prevent potentially sensitive information from being sent outside the enterprise and uncontrolled updates to the system. This setting will prevent the Program Inventory from collecting data about a system and sending the information to Microsoft.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Application Compatibility >> 'Turn off Inventory Collector' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	III
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253385r958478_rule
STIG-ID	WN11-CC-000175
SWIFT-CSCV1	2.3

VULN-ID	V-253385

Assets

vm-win11-stig-s

WN11-CC-000180 - Autoplay must be turned off for non-volume devices.

Info

Allowing autoplay to execute may introduce malicious code to a system. Autoplay begins reading from a drive as soon as media is inserted in the drive. As a result, the setup file of programs or music on audio media may start. This setting will disable autoplay for non-volume devices (such as Media Transfer Protocol (MTP) devices).

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> AutoPlay Policies >> 'Disallow Autoplay for non-volume devices' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.7
800-171R3	03.04.06
800-53	CM-7(2)
800-53R5	CM-7(2)
CAT	I
CCI	CCI-001764
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7(2)
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
QCSC-V1	3.2
RULE-ID	SV-253386r958804_rule
STIG-ID	WN11-CC-000180
SWIFT-CSCV1	2.3
VULN-ID	V-253386

Assets

vm-win11-stig-s

WN11-CC-000185 - The default autorun behavior must be configured to prevent autorun commands.

Info

Allowing autorun commands to execute may introduce malicious code to a system. Configuring this setting prevents autorun commands from executing.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> AutoPlay Policies >> 'Set the default behavior for AutoRun' to 'Enabled:Do not execute any autorun commands'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.7
800-171R3	03.04.06
800-53	CM-7(2)
800-53R5	CM-7(2)
CAT	I
CCI	CCI-001764
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7(2)
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
QCSC-V1	3.2
RULE-ID	SV-253387r958804_rule
STIG-ID	WN11-CC-000185
SWIFT-CSCV1	2.3
VULN-ID	V-253387

Assets

vm-win11-stig-s

WN11-CC-000190 - Autoplay must be disabled for all drives.

Info

Allowing autoplay to execute may introduce malicious code to a system. Autoplay begins reading from a drive as soon as media is inserted in the drive. As a result, the setup file of programs or music on audio media may start. By default, autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive) and on network drives. If this policy is enabled, autoplay can be disabled on all drives.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> AutoPlay Policies >> 'Turn off AutoPlay' to 'Enabled:All Drives'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.7
800-171R3	03.04.06
800-53	CM-7(2)
800-53R5	CM-7(2)
CAT	I
CCI	CCI-001764
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7(2)
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
QCSC-V1	3.2
RULE-ID	SV-253388r958804_rule
STIG-ID	WN11-CC-000190
SWIFT-CSCV1	2.3
VULN-ID	V-253388

Assets

vm-win11-stig-s

WN11-CC-000195 - Enhanced anti-spoofing for facial recognition must be enabled on Windows 11.

Info

Enhanced anti-spoofing provides additional protections when using facial recognition with devices that support it.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Biometrics >> Facial Features >> 'Configure enhanced anti-spoofing' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253389r991589_rule
STIG-ID	WN11-CC-000195
SWIFT-CSCV1	2.3
VULN-ID	V-253389

Assets

vm-win11-stig-s

WN11-CC-000197 - Microsoft consumer experiences must be turned off.

Info

Microsoft consumer experiences provides suggestions and notifications to users, which may include the installation of Windows Store apps. Organizations may control the execution of applications through other means such as allowlisting. Turning off Microsoft consumer experiences will help prevent the unwanted installation of suggested applications.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Cloud Content >> 'Turn off Microsoft consumer experiences' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	III
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253390r958478_rule
STIG-ID	WN11-CC-000197
SWIFT-CSCV1	2.3

VULN-ID	V-253390

Assets

vm-win11-stig-s

WN11-CC-000200 - Administrator accounts must not be enumerated during elevation.

Info

Enumeration of administrator accounts when elevating can provide part of the logon information to an unauthorized user. This setting configures the system to always require users to type in a username and password to elevate a running application.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Credential User Interface >> 'Enumerate administrator accounts on elevation' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253391r958518_rule
STIG-ID	WN11-CC-000200
VULN-ID	V-253391

Assets

vm-win11-stig-s

WN11-CC-000204 - Enhanced diagnostic data must be limited to the minimum required to support Windows Analytics.

Info

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Limiting this capability will prevent potentially sensitive information from being sent outside the enterprise. The 'Enhanced' level for telemetry includes additional information beyond 'Security' and 'Basic' on how Windows and apps are used and advanced reliability data. Windows Analytics can use a 'limited enhanced' level to provide information such as health data for devices.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Data Collection and Preview Builds >> 'Limit optional diagnostic data for Windows Analytics' to 'Enabled' with 'Enable Desktop Analytics collection' selected in 'Options:'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253392r991589_rule
STIG-ID	WN11-CC-000204
SWIFT-CSCV1	2.3
VULN-ID	V-253392

Assets

vm-win11-stig-s

WN11-CC-000205 - Windows Telemetry must not be configured to Full.

Info

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Limiting this capability will prevent potentially sensitive information from being sent outside the enterprise. The 'Security' option for Telemetry configures the lowest amount of data, effectively none outside of the Malicious Software Removal Tool (MSRT), Defender and telemetry client settings. 'Basic' sends basic diagnostic and usage data and may be required to support some Microsoft services. 'Enhanced' includes additional information on how Windows and apps are used and advanced reliability data. Windows Analytics can use a 'limited enhanced' level to provide information such as health data for devices.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Data Collection and Preview Builds >> 'Allow Diagnostic Data' to 'Enabled' with 'Send required diagnostic data' selected in 'Options:'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SI-11a.
800-53R5	SI-11a.
CAT	II
CCI	CCI-001312
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-11b.
RULE-ID	SV-253393r958564_rule
STIG-ID	WN11-CC-000205
VULN-ID	V-253393

Assets

vm-win11-stig-s

WN11-CC-000206 - Windows Update must not obtain updates from other PCs on the internet.

Info

Windows 11 allows Windows Update to obtain updates from additional sources instead of Microsoft. In addition to Microsoft, updates can be obtained from and sent to PCs on the local network as well as on the Internet. This is part of the Windows Update trusted process, however to minimize outside exposure, obtaining updates from or sending to systems on the internet must be prevented.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Delivery Optimization >> 'Download Mode' to 'Enabled' with any option except 'Internet' selected.
Acceptable selections include:
Bypass (100) Group (2) HTTP only (0) LAN (1) Simple (99)
.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253394r991589_rule
STIG-ID	WN11-CC-000206
SWIFT-CSCV1	2.3
VULN-ID	V-253394

Assets

vm-win11-stig-s

WN11-CC-000215 - Explorer Data Execution Prevention must be enabled.

Info

Data Execution Prevention (DEP) provides additional protection by performing checks on memory to help prevent malicious code from running. This setting will prevent Data Execution Prevention from being turned off for File Explorer.

Solution

The default behavior is for data execution prevention to be turned on for file explorer.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Turn off Data Execution Prevention for Explorer' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SI-16
800-53R5	SI-16
CAT	II
CCI	CCI-002824
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
RULE-ID	SV-253396r958928_rule
STIG-ID	WN11-CC-000215
VULN-ID	V-253396

Assets

vm-win11-stig-s

WN11-CC-000220 - File Explorer heap termination on corruption must be disabled.

Info

Legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Disabling this feature will prevent this.

Solution

The default behavior is for File Explorer heap termination on corruption to be enabled.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Turn off heap termination on corruption' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SC-5
800-53R5	SC-5a.
CAT	III
CCI	CCI-002385
CSF	DE.CM-1
CSF	PR.DS-4
CSF2.0	DE.CM-01
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-5
ITSG-33	SC-5a.
NESA	T3.3.1
NIAV2	GS8e
NIAV2	GS10c
QCSC-V1	8.2.1
RULE-ID	SV-253397r958902_rule
STIG-ID	WN11-CC-000220
VULN-ID	V-253397

Assets

vm-win11-stig-s

WN11-CC-000225 - File Explorer shell protocol must run in protected mode.

Info

The shell protocol will limit the set of folders applications can open when run in protected mode. Restricting files an application can open, to a limited set of folders, increases the security of Windows.

Solution

The default behavior is for shell protected mode to be turned on for file explorer.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Turn off shell protocol protected mode' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253398r991589_rule
STIG-ID	WN11-CC-000225
SWIFT-CSCV1	2.3
VULN-ID	V-253398

Assets

vm-win11-stig-s

WN11-CC-000252 - Windows 11 must be configured to disable Windows Game Recording and Broadcasting.

Info

Windows Game Recording and Broadcasting is intended for use with games; however, it could potentially record screen shots of other applications and expose sensitive data. Disabling the feature will prevent this from occurring.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Game Recording and Broadcasting >> 'Enables or disables Windows Game Recording and Broadcasting' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253399r958478_rule
STIG-ID	WN11-CC-000252
SWIFT-CSCV1	2.3

VULN-ID	V-253399

Assets

vm-win11-stig-s

WN11-CC-000255 - The use of a hardware security device with Windows Hello for Business must be enabled.

Info

The use of a Trusted Platform Module (TPM) to store keys for Windows Hello for Business provides additional security. Keys stored in the TPM may only be used on that system while keys stored using software are more susceptible to compromise and could be used on other systems.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Hello for Business >> 'Use a hardware security device' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253400r991589_rule
STIG-ID	WN11-CC-000255
SWIFT-CSCV1	2.3
VULN-ID	V-253400

Assets

vm-win11-stig-s

WN11-CC-000260 - Windows 11 must be configured to require a minimum pin length of six characters or greater.

Info

Windows allows the use of PINs as well as biometrics for authentication without sending a password to a network or website where it could be compromised. Longer minimum PIN lengths increase the available combinations an attacker would have to attempt. Shorter minimum length significantly reduces the strength.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> PIN Complexity >> 'Minimum PIN length' to '6' or greater.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253401r991589_rule
STIG-ID	WN11-CC-000260
SWIFT-CSCV1	2.3
VULN-ID	V-253401

Assets

vm-win11-stig-s

WN11-CC-000270 - Passwords must not be saved in the Remote Desktop Client.

Info

Saving passwords in the Remote Desktop Client could allow an unauthorized user to establish a remote desktop session to another system. The system must be configured to prevent users from saving passwords in the Remote Desktop Client.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Connection Client >> 'Do not allow passwords to be saved' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253402r1051051_rule
STIG-ID	WN11-CC-000270
VULN-ID	V-253402

Assets

vm-win11-stig-s

WN11-CC-000275 - Local drives must be prevented from sharing with Remote Desktop Session Hosts.

Info

Preventing users from sharing the local drives on their client computers to Remote Session Hosts that they access helps reduce possible exposure of sensitive data.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Device and Resource Redirection >> 'Do not allow drive redirection' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.4
800-171R3	03.13.04
800-53	SC-4
800-53R5	SC-4
CAT	II
CCI	CCI-001090
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-253403r1137695_rule
STIG-ID	WN11-CC-000275
VULN-ID	V-253403

Assets

vm-win11-stig-s

WN11-CC-000280 - Remote Desktop Services must always prompt a client for passwords upon connection.

Info

This setting controls the ability of users to supply passwords automatically as part of their remote desktop connection. Disabling this setting would allow anyone to use the stored credentials in a connection item to connect to the terminal server.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security >> 'Always prompt for password upon connection' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253404r1051052_rule
STIG-ID	WN11-CC-000280
VULN-ID	V-253404

Assets

vm-win11-stig-s

WN11-CC-000285 - The Remote Desktop Session Host must require secure RPC communications.

Info

Allowing unsecure RPC communication exposes the system to man in the middle attacks and data disclosure attacks. A man in the middle attack occurs when an intruder captures packets between a client and server and modifies them before allowing the packets to be exchanged. Usually the attacker will modify the information in the packets in an attempt to cause either the client or server to reveal sensitive information.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security 'Require secure RPC communication' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.13
800-171R3	03.13.08
800-53	AC-17(2)
800-53R5	AC-17(2)
CAT	II
CCI	CCI-001453
CN-L3	7.1.2.7(g)
CN-L3	7.1.3.1(d)
CN-L3	8.1.4.1(c)
CSF	PR.AC-3
CSF	PR.PT-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.6.7
ISO/IEC-27001	A.6.2.2
ITSG-33	AC-17(2)
NESA	T5.4.2
NIAV2	AM37
PCI-DSSV3.2.1	2.3

PCI-DSSV4.0	2.2.7
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
RULE-ID	SV-253405r991554_rule
STIG-ID	WN11-CC-000285
SWIFT-CSCV1	2.6
VULN-ID	V-253405

Assets

vm-win11-stig-s

WN11-CC-000290 - Remote Desktop Services must be configured with the client connection encryption set to the required level.

Info

Remote connections must be encrypted to prevent interception of data or sensitive information. Selecting 'High Level' will ensure encryption of Remote Desktop Services sessions in both directions.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security >> 'Set client connection encryption level' to 'Enabled' and 'High Level'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.13
800-171R3	03.13.08
800-53	AC-17(2)
800-53R5	AC-17(2)
CAT	II
CCI	CCI-000068
CN-L3	7.1.2.7(g)
CN-L3	7.1.3.1(d)
CN-L3	8.1.4.1(c)
CSF	PR.AC-3
CSF	PR.PT-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.6.7
ISO/IEC-27001	A.6.2.2
ITSG-33	AC-17(2)
NESA	T5.4.2
NIAV2	AM37
PCI-DSSV3.2.1	2.3

PCI-DSSV4.0	2.2.7
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
RULE-ID	SV-253406r958408_rule
STIG-ID	WN11-CC-000290
SWIFT-CSCV1	2.6
VULN-ID	V-253406

Assets

vm-win11-stig-s

WN11-CC-000295 - Attachments must be prevented from being downloaded from RSS feeds.

Info

Attachments from RSS feeds may not be secure. This setting will prevent attachments from being downloaded from RSS feeds.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> RSS Feeds >> 'Prevent downloading of enclosures' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253407r991589_rule
STIG-ID	WN11-CC-000295
SWIFT-CSCV1	2.3
VULN-ID	V-253407

Assets

vm-win11-stig-s

WN11-CC-000300 - Basic authentication for RSS feeds over HTTP must not be used.

Info

Basic authentication uses plain text passwords that could be used to compromise a system.

Solution

The default behavior is for the Windows RSS platform to not use Basic authentication over HTTP connections. To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> RSS Feeds >> 'Turn on Basic feed authentication over HTTP' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253408r958478_rule
STIG-ID	WN11-CC-000300
SWIFT-CSCV1	2.3
VULN-ID	V-253408

Assets

vm-win11-stig-s

WN11-CC-000305 - Indexing of encrypted files must be turned off.

Info

Indexing of encrypted files may expose sensitive data. This setting prevents encrypted files from being indexed.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Search >> 'Allow indexing of encrypted files' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253409r958478_rule
STIG-ID	WN11-CC-000305
SWIFT-CSCV1	2.3
VULN-ID	V-253409

Assets

vm-win11-stig-s

WN11-CC-000310 - Users must be prevented from changing installation options.

Info

Installation options for applications are typically controlled by administrators. This setting prevents users from changing installation options that may bypass security features.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> 'Allow user control over installs' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.9
800-53	CM-11(2)
800-53R5	CM-11(2)
CAT	II
CCI	CCI-001812
CCI	CCI-003980
CSF	DE.CM-3
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
CSF2.0	PR.PS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.19
ISO/IEC-27001	A.12.6.2
QCSC-V1	8.2.1
RULE-ID	SV-253410r1051053_rule
STIG-ID	WN11-CC-000310
SWIFT-CSCV1	5.1
VULN-ID	V-253410

Assets

vm-win11-stig-s

WN11-CC-000315 - The Windows Installer feature 'Always install with elevated privileges' must be disabled.

Info

Standard user accounts must not be granted elevated privileges. Enabling Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> 'Always install with elevated privileges' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.9
800-53	CM-11(2)
800-53R5	CM-11(2)
CAT	I
CCI	CCI-001812
CCI	CCI-003980
CSF	DE.CM-3
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
CSF2.0	PR.PS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.19
ISO/IEC-27001	A.12.6.2
QCSC-V1	8.2.1
RULE-ID	SV-253411r1051054_rule
STIG-ID	WN11-CC-000315
SWIFT-CSCV1	5.1
VULN-ID	V-253411

Assets

vm-win11-stig-s

WN11-CC-000320 - Users must be notified if a web-based program attempts to install software.

Info

Web-based programs may attempt to install malicious software on a system. Ensuring users are notified if a web-based program attempts to install software allows them to refuse the installation.

Solution

The default behavior is for Internet Explorer to warn users and select whether to allow or refuse installation when a web-based program attempts to install software on the system.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> 'Prevent Internet Explorer security prompt for Windows Installer scripts' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253412r991589_rule
STIG-ID	WN11-CC-000320
SWIFT-CSCV1	2.3
VULN-ID	V-253412

Assets

vm-win11-stig-s

WN11-CC-000325 - Automatically signing in the last interactive user after a system-initiated restart must be disabled.

Info

Windows can be configured to automatically sign the user back in after a Windows Update restart. Some protections are in place to help ensure this is done in a secure fashion; however, disabling this will prevent the caching of credentials for this purpose and also ensure the user is aware of the restart.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Logon Options >> 'Sign-in last interactive user automatically after a system-initiated restart' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253413r991591_rule
STIG-ID	WN11-CC-000325
SWIFT-CSCV1	2.3
VULN-ID	V-253413

Assets

vm-win11-stig-s

WN11-CC-000326 - PowerShell script block logging must be enabled on Windows 11.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Enabling PowerShell script block logging will record detailed information from the processing of PowerShell commands and scripts. This can provide additional detail when malware has run on a system.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows PowerShell >> 'Turn on PowerShell Script Block Logging' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02b.
800-53	AU-3(1)
800-53R5	AU-3(1)
CAT	II
CCI	CCI-000135
CN-L3	7.1.3.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3(1)
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d

NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253414r958422_rule
STIG-ID	WN11-CC-000326
SWIFT-CSCV1	6.4
VULN-ID	V-253414

Assets

vm-win11-stig-s

WN11-CC-000327 - PowerShell Transcription must be enabled on Windows 11.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Enabling PowerShell Transcription will record detailed information from the processing of PowerShell commands and scripts. This can provide additional detail when malware has run on a system.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows PowerShell >> 'Turn on PowerShell Transcription' to 'Enabled'.
Specify the Transcript output directory to point to a Central Log Server or another secure location to prevent user access.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3e.
CAT	II
CCI	CCI-000134
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253415r958420_rule
STIG-ID	WN11-CC-000327
SWIFT-CSCV1	6.4
VULN-ID	V-253415

Assets

vm-win11-stig-s

WN11-CC-000330 - The Windows Remote Management (WinRM) client must not use Basic authentication.

Info

Basic authentication uses plain text passwords that could be used to compromise a system.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> 'Allow Basic authentication' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.7.5
800-171R3	03.07.05b.
800-53	MA-4c.
800-53R5	MA-4c.
CAT	I
CCI	CCI-000877
CSF	PR.MA-2
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	MA-4c.
NESA	T2.3.4
NESA	T5.4.4
QCSC-V1	5.2.2
RULE-ID	SV-253416r958510_rule
STIG-ID	WN11-CC-000330
TBA-FIISB	45.2.3
VULN-ID	V-253416

Assets

vm-win11-stig-s

WN11-CC-000335 - The Windows Remote Management (WinRM) client must not allow unencrypted traffic.

Info

Unencrypted remote access to a system can allow sensitive information to be compromised. Windows remote management connections must be encrypted to prevent this.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> 'Allow unencrypted traffic' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.7.5
800-171R3	03.07.05
800-53	MA-4(6)
800-53R5	MA-4(6)
CAT	II
CCI	CCI-002890
CSF	PR.MA-2
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	MA-4(6)
NESA	T2.3.4
NESA	T5.4.4
QCSC-V1	5.2.2
RULE-ID	SV-253417r958848_rule
STIG-ID	WN11-CC-000335
SWIFT-CSCV1	2.6
TBA-FIISB	45.2.3
VULN-ID	V-253417

Assets

vm-win11-stig-s

WN11-CC-000345 - The Windows Remote Management (WinRM) service must not use Basic authentication.

Info

Basic authentication uses plain text passwords that could be used to compromise a system.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> 'Allow Basic authentication' to 'Disabled'.
Severity Override Guidance: The AO can allow the severity override if they have reviewed the overall protection. This would only be allowed temporarily for implementation as documented and approved.
....
Allowing Basic authentication to be used for the sole creation of Office 365 DoD tenants.
....
A documented mechanism and or script that can disable Basic authentication once administration completes.
....
Use of a Privileged Access Workstation (PAW) and adherence to the Clean Source principle for administration.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.7.5
800-171R3	03.07.05b.
800-53	MA-4c.
800-53R5	MA-4c.
CAT	I
CCI	CCI-000877
CSF	PR.MA-2
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	MA-4c.
NESA	T2.3.4
NESA	T5.4.4
QCSC-V1	5.2.2
RULE-ID	SV-253418r958510_rule
STIG-ID	WN11-CC-000345
TBA-FIISB	45.2.3
VULN-ID	V-253418

Assets

vm-win11-stig-s

WN11-CC-000350 - The Windows Remote Management (WinRM) service must not allow unencrypted traffic.

Info

Unencrypted remote access to a system can allow sensitive information to be compromised. Windows remote management connections must be encrypted to prevent this.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> 'Allow unencrypted traffic' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.7.5
800-171R3	03.07.05
800-53	MA-4(6)
800-53R5	MA-4(6)
CAT	II
CCI	CCI-003123
CSF	PR.MA-2
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	MA-4(6)
NESA	T2.3.4
NESA	T5.4.4
QCSC-V1	5.2.2
RULE-ID	SV-253419r958850_rule
STIG-ID	WN11-CC-000350
SWIFT-CSCV1	2.6
TBA-FIISB	45.2.3
VULN-ID	V-253419

Assets

vm-win11-stig-s

WN11-CC-000355 - The Windows Remote Management (WinRM) service must not store RunAs credentials.

Info

Storage of administrative credentials could allow unauthorized access. Disallowing the storage of RunAs credentials for Windows Remote Management will prevent them from being used with plug-ins.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> 'Disallow WinRM from storing RunAs credentials' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253420r1051055_rule
STIG-ID	WN11-CC-000355
VULN-ID	V-253420

Assets

vm-win11-stig-s

WN11-CC-000360 - The Windows Remote Management (WinRM) client must not use Digest authentication.

Info

Digest authentication is not as strong as other options and may be subject to man-in-the-middle attacks.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> 'Disallow Digest authentication' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.7.5
800-171R3	03.07.05b.
800-53	MA-4c.
800-53R5	MA-4c.
CAT	II
CCI	CCI-000877
CSF	PR.MA-2
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	MA-4c.
NESA	T2.3.4
NESA	T5.4.4
QCSC-V1	5.2.2
RULE-ID	SV-253421r958510_rule
STIG-ID	WN11-CC-000360
TBA-FIISB	45.2.3
VULN-ID	V-253421

Assets

vm-win11-stig-s

WN11-CC-000365 - Windows 11 must be configured to prevent Windows apps from being activated by voice while the system is locked.

Info

Allowing Windows apps to be activated by voice from the lock screen could allow for unauthorized use. Requiring logon will ensure the apps are only used by authorized personnel.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> App Privacy >> 'Let Windows apps activate with voice while the system is locked' to 'Enabled' with Default for all Apps: set to Force Deny.
The requirement is NA if the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> App Privacy >> 'Let Windows apps activate with voice' is configured to 'Enabled' with Default for all Apps: set to Force Deny.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.10
800-171R3	03.01.10b.
800-53	AC-11b.
800-53R5	AC-11b.
CAT	II
CCI	CCI-000056
CN-L3	8.1.4.1(b)
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO-27001-2022	A.7.7
ISO-27001-2022	A.8.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-11b.
NIAV2	AM23e
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8
RULE-ID	SV-253422r958400_rule
STIG-ID	WN11-CC-000365
VULN-ID	V-253422

Assets

vm-win11-stig-s

WN11-CC-000370 - The convenience PIN for Windows 11 must be disabled.

Info

This policy controls whether a domain user can sign in using a convenience PIN to prevent enabling (Password Stuffer).

Solution

Disable the convenience PIN sign-in.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> System >> Logon >> Set 'Turn on convenience PIN sign-in' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253423r958478_rule
STIG-ID	WN11-CC-000370
SWIFT-CSCV1	2.3
VULN-ID	V-253423

Assets

vm-win11-stig-s

WN11-CC-000385 - Windows Ink Workspace must be configured to disallow access above the lock.

Info

This action secures Windows Ink, which contains applications and features oriented toward pen computing.

Solution

Disable the convenience PIN sign-in.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Ink Workspace >> Set 'Allow Windows Ink Workspace' to 'Enabled and set Options 'On, but disallow access above lock'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.10
800-171R3	03.01.10
800-53	AC-11(1)
800-53R5	AC-11(1)
CAT	II
CCI	CCI-000060
CN-L3	8.1.4.1(b)
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO-27001-2022	A.7.7
ISO-27001-2022	A.8.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-11(1)
NIAV2	AM23c
NIAV2	AM23d
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8
RULE-ID	SV-253424r958404_rule
STIG-ID	WN11-CC-000385
VULN-ID	V-253424

Assets

vm-win11-stig-s

WN11-CC-000390 - Windows 11 must be configured to prevent users from receiving suggestions for third-party or additional applications.

Info

Windows spotlight features may suggest apps and content from third-party software publishers in addition to Microsoft apps and content.

Solution

Configure the policy value for User Configuration >> Administrative Templates. >> Windows Components >> Cloud Content >> 'Do not suggest third-party content in Windows spotlight' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	III
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253425r958478_rule
STIG-ID	WN11-CC-000390
SWIFT-CSCV1	2.3
VULN-ID	V-253425

Assets
vm-win11-stig-s

WN11-CC-000391 - Internet Explorer must be disabled for Windows 11.

Info

Internet Explorer 11 (IE11) is not supported on Windows 11 semi-annual channel.

Solution

For Windows 11 semi-annual channel, remove or disable the IE11 application.
To disable IE11 as a standalone browser:
Set the policy value for 'Computer Configuration/Administrative Templates/Windows Components/Internet Explorer/Disable Internet Explorer 11 as a standalone browser' to 'Enabled' with the option value set to 'Never'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-256893r958552_rule
STIG-ID	WN11-CC-000391
SWIFT-CSCV1	2.3
VULN-ID	V-256893

Assets

vm-win11-stig-s

WN11-EP-000310 - Windows 11 Kernel (Direct Memory Access) DMA Protection must be enabled.

Info

Kernel DMA Protection to protect PCs against drive-by Direct Memory Access (DMA) attacks using PCI hot plug devices connected to Thunderbolt 3 ports. Drive-by DMA attacks can lead to disclosure of sensitive information residing on a PC, or even injection of malware that allows attackers to bypass the lock screen or control PCs remotely.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Kernel DMA Protection >> 'Enumeration policy for external devices incompatible with Kernel DMA Protection' to 'Enabled' with 'Enumeration Policy' set to 'Block All'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253426r991580_rule
STIG-ID	WN11-EP-000310
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253426

Assets

vm-win11-stig-s

WN11-PK-000010 - The External Root CA certificates must be installed in the Trusted Root Store on unclassified systems.

Info

To ensure secure websites protected with External Certificate Authority (ECA) server certificates are properly validated, the system must trust the ECA Root CAs. The ECA root certificates will ensure the trust chain is established for server certificates issued from the External CAs. This requirement only applies to unclassified systems.

Solution

Install the ECA Root CA certificates on unclassified systems.
ECA Root CA 4
The InstallRoot tool is available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. PKI can be found at https://crl.gds.disa.mil/.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.12
800-53	IA-5(2)(a)
800-53R5	IA-5(2)(b)(1)
CAT	II
CCI	CCI-000185
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(2)(a)
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253428r958448_rule
STIG-ID	WN11-PK-000010

VULN-ID	V-253428

Assets

vm-win11-stig-s

WN11-PK-000015 - The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

Info

To ensure users do not experience denial of service when performing certificate-based authentication to DoD websites due to the system chaining to a root other than DoD Root CAs, the DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificate Store. This requirement only applies to unclassified systems.

Solution

Install the DoD Interoperability Root CA cross-certificates on unclassified systems.
Issued To - Issued By - Thumbprint DoD Root CA 3 - DoD Interoperability Root CA 2 - 49CBE933151872E17C8EAE7F0ABA97FB610F6477
The certificates can be installed using the InstallRoot tool. The tool and user guide are available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. Certificate bundles published by the PKI can be found at https://crl.gds.disa.mil/.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.15
800-171R3	03.13.15
800-53	SC-23(5)
800-53R5	SC-23(5)
CAT	II
CCI	CCI-002470
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-23
ITSG-33	SC-23a.
NESA	T4.5.1
QCSC-V1	5.2.1
RULE-ID	SV-253429r958448_rule
STIG-ID	WN11-PK-000015
VULN-ID	V-253429

Assets

vm-win11-stig-s

WN11-SO-000005 - The built-in administrator account must be disabled.

Info

The built-in administrator account is a well-known account subject to attack. It also provides no accountability to individual administrators on a system. It must be disabled to prevent its use.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Accounts: Administrator account status' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.1
800-171R3	03.05.01a.
800-53	IA-2
800-53R5	IA-2
CAT	II
CCI	CCI-000764
CN-L3	7.1.3.1(a)
CN-L3	7.1.3.1(e)
CN-L3	8.1.4.1(a)
CN-L3	8.1.4.2(a)
CN-L3	8.5.4.1(a)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-2
ITSG-33	IA-2a.
NESA	T2.3.8
NESA	T5.3.1

NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2
NESA	T5.5.3
NIAV2	AM2
NIAV2	AM8
NIAV2	AM14b
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253432r958482_rule
STIG-ID	WN11-SO-000005
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-253432

Assets

vm-win11-stig-s

WN11-SO-000010 - The built-in guest account must be disabled.

Info

A system faces an increased vulnerability threat if the built-in guest account is not disabled. This account is a known account that exists on all Windows systems and cannot be deleted. This account is initialized during the installation of the operating system with no password assigned.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Accounts: Guest account status' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	IA-8
800-53R5	IA-8
CAT	II
CCI	CCI-000804
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-8
ITSG-33	IA-8a.
NESA	T4.3.1
NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253433r958504_rule
STIG-ID	WN11-SO-000010
SWIFT-CSCV1	2.8

VULN-ID	V-253433

Assets

vm-win11-stig-s

WN11-SO-000015 - Local accounts with blank passwords must be restricted to prevent access from the network.

Info

An account without a password can allow unauthorized access to a system as only the username would be required. Password policies must prevent accounts with blank passwords from existing on a system. However, if a local account with a blank password did exist, enabling this setting will prevent network access, limiting the account to local console logon only.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253434r991589_rule
STIG-ID	WN11-SO-000015
SWIFT-CSCV1	2.3
VULN-ID	V-253434

Assets

vm-win11-stig-s

WN11-SO-000020 - The built-in administrator account must be renamed.

Info

The built-in administrator account is a well-known account subject to attack. Renaming this account to an unidentified name improves the protection of this account and the system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Accounts: Rename administrator account' to a name other than 'Administrator'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253435r991589_rule
STIG-ID	WN11-SO-000020
SWIFT-CSCV1	2.3
VULN-ID	V-253435

Assets

vm-win11-stig-s

WN11-SO-000025 - The built-in guest account must be renamed.

Info

The built-in guest account is a well-known user account on all Windows systems and, as initially installed, does not require a password. This can allow access to system resources by unauthorized users. Renaming this account to an unidentified name improves the protection of this account and the system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Accounts: Rename guest account' to a name other than 'Guest'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253436r991589_rule
STIG-ID	WN11-SO-000025
SWIFT-CSCV1	2.3
VULN-ID	V-253436

Assets

vm-win11-stig-s

WN11-SO-000030 - Audit policy using subcategories must be enabled.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. This setting allows administrators to enable more precise auditing capabilities.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12a.
800-53R5	AU-12a.
CAT	II
CCI	CCI-000169
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-12a.
PCI-DSSV3.2.1	10.1

QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253437r958442_rule
STIG-ID	WN11-SO-000030
SWIFT-CSCV1	6.4
VULN-ID	V-253437

Assets

vm-win11-stig-s

WN11-SO-000035 - Outgoing secure channel traffic must be encrypted or signed.

Info

Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but not all information is encrypted. If this policy is enabled, outgoing secure channel traffic will be encrypted and signed.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Domain member: Digitally encrypt or sign secure channel data (always)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53	SC-8(1)
800-53R5	SC-8
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002418
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)

HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8
ITSG-33	SC-8a.
ITSG-33	SC-8(1)
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS5d
NIAV2	NS6b
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253438r958908_rule
STIG-ID	WN11-SO-000035

SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253438

Assets

vm-win11-stig-s

WN11-SO-000040 - Outgoing secure channel traffic must be encrypted.

Info

Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but not all information is encrypted. If this policy is enabled, outgoing secure channel traffic will be encrypted.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Domain member: Digitally encrypt secure channel data (when possible)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53	SC-8(1)
800-53R5	SC-8
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002418
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)

HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8
ITSG-33	SC-8a.
ITSG-33	SC-8(1)
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS5d
NIAV2	NS6b
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253439r958908_rule
STIG-ID	WN11-SO-000040

SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253439

Assets

vm-win11-stig-s

WN11-SO-000045 - Outgoing secure channel traffic must be signed.

Info

Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked. If this policy is enabled, outgoing secure channel traffic will be signed.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Domain member: Digitally sign secure channel data (when possible)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53	SC-8(1)
800-53R5	SC-8
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002418
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)

HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8
ITSG-33	SC-8a.
ITSG-33	SC-8(1)
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS5d
NIAV2	NS6b
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253440r958908_rule
STIG-ID	WN11-SO-000045

SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253440

Assets

vm-win11-stig-s

WN11-SO-000050 - The computer account password must not be prevented from being reset.

Info

Computer account passwords are changed automatically on a regular basis. Disabling automatic password changes can make the system more vulnerable to malicious access. Frequent password changes can be a significant safeguard for the system. A new password for the computer account will be generated every 30 days.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Domain member: Disable machine account password changes' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253441r991589_rule
STIG-ID	WN11-SO-000050
SWIFT-CSCV1	2.3
VULN-ID	V-253441

Assets

vm-win11-stig-s

WN11-SO-000055 - The maximum age for machine account passwords must be configured to 30 days or less.

Info

Computer account passwords are changed automatically on a regular basis. This setting controls the maximum password age that a machine account may have. This setting must be set to no more than 30 days, ensuring the machine changes its password monthly.

Solution

This is the default configuration for this setting (30 days).
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Domain member: Maximum machine account password age' to '30' or less (excluding 0 which is unacceptable).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253442r991589_rule
STIG-ID	WN11-SO-000055
SWIFT-CSCV1	2.3
VULN-ID	V-253442

Assets

vm-win11-stig-s

WN11-SO-000060 - The system must be configured to require a strong session key.

Info

A computer connecting to a domain controller will establish a secure channel. Requiring strong session keys enforces 128-bit encryption between systems.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Domain member: Require strong (Windows 2000 or Later) session key' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53R5	SC-8
CAT	II
CCI	CCI-002418
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14

ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ITSG-33	SC-8
ITSG-33	SC-8a.
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253443r958908_rule
STIG-ID	WN11-SO-000060
VULN-ID	V-253443

Assets

vm-win11-stig-s

WN11-SO-000070 - The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.

Info

Unattended systems are susceptible to unauthorized use and must be locked when unattended. The screen saver must be set at a maximum of 15 minutes and be password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer.
Satisfies: SRG-OS-000279-GPOS-00109, SRG-OS-000163-GPOS-00072

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Interactive logon: Machine inactivity limit' to '900' seconds' or less, excluding '0' which is effectively disabled.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.11
800-171	3.13.9
800-171R3	03.01.11
800-171R3	03.13.09
800-53	AC-12
800-53	SC-10
800-53R5	AC-12
800-53R5	SC-10
CAT	II
CCI	CCI-001133
CCI	CCI-002361
CN-L3	7.1.2.2(d)
CN-L3	7.1.3.7(b)
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO-27001-2022	A.8.20
ITSG-33	AC-12
ITSG-33	SC-10

ITSG-33	SC-10a.
NESA	T2.3.8
NESA	T4.5.1
NESA	T5.5.1
NIAV2	NS49
RULE-ID	SV-253444r958636_rule
STIG-ID	WN11-SO-000070
SWIFT-CSCV1	2.6
VULN-ID	V-253444

Assets

vm-win11-stig-s

WN11-SO-000075 - The required legal notice must be configured to display before console logon.

Info

Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.
Satisfies: SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088, SRG-OS-000024-GPOS-00007

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Interactive logon: Message text for users attempting to log on' to the following.
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.8
800-171	3.1.9
800-171R3	03.01.08a.
800-171R3	03.01.09
800-53	AC-7a.
800-53	AC-8a.
800-53	AC-8b.
800-53R5	AC-7a.
800-53R5	AC-8a.
800-53R5	AC-8b.
CAT	II
CCI	CCI-000044
CCI	CCI-000048
CCI	CCI-000050
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-7a.
ITSG-33	AC-8a.
ITSG-33	AC-8b.
NESA	M5.2.5
NESA	T5.5.1
NIAV2	AM10a
NIAV2	AM10b
NIAV2	AM10c
NIAV2	AM10d
NIAV2	AM10e
NIAV2	AM10f
NIAV2	AM24
PCI-DSSV3.2.1	8.1.6
PCI-DSSV4.0	8.3.4
RULE-ID	SV-253445r958392_rule
STIG-ID	WN11-SO-000075
TBA-FIISB	45.1.2
TBA-FIISB	45.2.1
TBA-FIISB	45.2.2
TBA-FIISB	45.2.4
VULN-ID	V-253445

Assets

vm-win11-stig-s

WN11-SO-000080 - The Windows message title for the legal notice must be configured.

Info

Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Interactive logon: Message title for users attempting to log on' to 'DoD Notice and Consent Banner', 'US Department of Defense Warning Statement', or a site-defined equivalent.
If a site-defined title is used, it can in no case contravene or modify the language of the banner text required in WN11-SO-000075.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.9
800-171R3	03.01.09
800-53	AC-8a.
800-53	AC-8c.1.
800-53	AC-8c.2.
800-53	AC-8c.3.
800-53R5	AC-8a.
800-53R5	AC-8c.1.
800-53R5	AC-8c.2.
800-53R5	AC-8c.3.
CAT	III
CCI	CCI-000048
CCI	CCI-001384
CCI	CCI-001385
CCI	CCI-001386
CCI	CCI-001387
CCI	CCI-001388
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-8a.
ITSG-33	AC-8c.a.

ITSG-33	AC-8c.b.
ITSG-33	AC-8c.c.
NESA	M5.2.5
NESA	T5.5.1
NIAV2	AM10a
NIAV2	AM10b
NIAV2	AM10c
NIAV2	AM10d
NIAV2	AM10e
RULE-ID	SV-253446r958586_rule
STIG-ID	WN11-SO-000080
TBA-FIISB	45.2.4
VULN-ID	V-253446

Assets

vm-win11-stig-s

WN11-SO-000095 - The Smart Card removal option must be configured to Force Logoff or Lock Workstation.

Info

Unattended systems are susceptible to unauthorized use and must be locked. Configuring a system to lock when a smart card is removed will ensure the system is inaccessible when unattended.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Interactive logon: Smart card removal behavior' to 'Lock Workstation' or 'Force Logoff'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253448r991589_rule
STIG-ID	WN11-SO-000095
SWIFT-CSCV1	2.3
VULN-ID	V-253448

Assets

vm-win11-stig-s

WN11-SO-000100 - The Windows SMB client must be configured to always perform SMB packet signing.

Info

The server message block (SMB) protocol provides the basis for many network operations. Digitally signed SMB packets aid in preventing man-in-the-middle attacks. If this policy is enabled, the SMB client will only communicate with an SMB server that performs SMB packet signing.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53R5	SC-8
CAT	II
CCI	CCI-002418
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10

ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ITSG-33	SC-8
ITSG-33	SC-8a.
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253449r958908_rule
STIG-ID	WN11-SO-000100
VULN-ID	V-253449

Assets

vm-win11-stig-s

WN11-SO-000110 - Unencrypted passwords must not be sent to third-party SMB Servers.

Info

Some non-Microsoft SMB servers only support unencrypted (plain text) password authentication. Sending plain text passwords across the network, when authenticating to an SMB server, reduces the overall security of the environment. Check with the vendor of the SMB server to see if there is a way to support encrypted password authentication.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.10
800-171R3	03.05.07c.
800-53	IA-5(1)(c)
800-53R5	IA-5(1)(c)
CAT	II
CCI	CCI-000197
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)(c)
NESA	T5.2.3
NIAV2	CY6
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253450r987796_rule
STIG-ID	WN11-SO-000110

SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-253450

Assets

vm-win11-stig-s

WN11-SO-000120 - The Windows SMB server must be configured to always perform SMB packet signing.

Info

The server message block (SMB) protocol provides the basis for many network operations. Digitally signed SMB packets aid in preventing man-in-the-middle attacks. If this policy is enabled, the SMB server will only communicate with an SMB client that performs SMB packet signing.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Microsoft network server: Digitally sign communications (always)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53R5	SC-8
CAT	II
CCI	CCI-002418
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10

ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ITSG-33	SC-8
ITSG-33	SC-8a.
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253451r958908_rule
STIG-ID	WN11-SO-000120
VULN-ID	V-253451

Assets

vm-win11-stig-s

WN11-SO-000140 - Anonymous SID/Name translation must not be allowed.

Info

Allowing anonymous SID/Name translation can provide sensitive information for accessing a system. Only authorized users must be able to perform such translations.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Allow anonymous SID/Name translation' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253452r991589_rule
STIG-ID	WN11-SO-000140
SWIFT-CSCV1	2.3
VULN-ID	V-253452

Assets

vm-win11-stig-s

WN11-SO-000145 - Anonymous enumeration of SAM accounts must not be allowed.

Info

Anonymous enumeration of SAM accounts allows anonymous log on users (null session connections) to list all accounts names, thus providing a list of potential points to attack the system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253453r991589_rule
STIG-ID	WN11-SO-000145
SWIFT-CSCV1	2.3
VULN-ID	V-253453

Assets

vm-win11-stig-s

WN11-SO-000150 - Anonymous enumeration of shares must be restricted.

Info

Allowing anonymous logon users (null session connections) to list all account names and enumerate all shared resources can provide a map of potential points to attack the system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.4
800-171R3	03.13.04
800-53	SC-4
800-53R5	SC-4
CAT	I
CCI	CCI-001090
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-253454r1137695_rule
STIG-ID	WN11-SO-000150
VULN-ID	V-253454

Assets

vm-win11-stig-s

WN11-SO-000165 - Anonymous access to Named Pipes and Shares must be restricted.

Info

Allowing anonymous access to named pipes or shares provides the potential for unauthorized system access. This setting restricts access to those defined in 'Network access: Named Pipes that can be accessed anonymously' and 'Network access: Shares that can be accessed anonymously', both of which must be blank under other requirements.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.4
800-171R3	03.13.04
800-53	SC-4
800-53R5	SC-4
CAT	I
CCI	CCI-001090
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-253456r1137695_rule
STIG-ID	WN11-SO-000165
VULN-ID	V-253456

Assets

vm-win11-stig-s

WN11-SO-000167 - Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.

Info

The Windows SAM stores users' passwords. Restricting remote rpc connections to the SAM to Administrators helps protect those credentials.

Solution

Navigate to the policy Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Restrict clients allowed to make remote calls to SAM'.
Select 'Edit Security' to configure the 'Security descriptor:'.
Add 'Administrators' in 'Group or user names:' if it is not already listed (this is the default).
Select 'Administrators' in 'Group or user names:'.
Select 'Allow' for 'Remote Access' in 'Permissions for 'Administrators'.
Click 'OK'.
The 'Security descriptor:' must be populated with 'O:BAG:BAD:(A;;RC;;;BA) for the policy to be enforced.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1

NESA	T5.2.2
NESA	T5.4.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253457r1081060_rule
STIG-ID	WN11-SO-000167
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253457

Assets

vm-win11-stig-s

WN11-SO-000180 - NTLM must be prevented from falling back to a Null session.

Info

NTLM sessions that are allowed to fall back to Null (unauthenticated) sessions may gain unauthorized access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253458r991589_rule
STIG-ID	WN11-SO-000180
SWIFT-CSCV1	2.3
VULN-ID	V-253458

Assets

vm-win11-stig-s

WN11-SO-000185 - PKU2U authentication using online identities must be prevented.

Info

PKU2U is a peer-to-peer authentication protocol. This setting prevents online identities from authenticating to domain-joined systems. Authentication will be centrally managed with Windows user accounts.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: Allow PKU2U authentication requests to this computer to use online identities' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253459r991589_rule
STIG-ID	WN11-SO-000185
SWIFT-CSCV1	2.3
VULN-ID	V-253459

Assets

vm-win11-stig-s

WN11-SO-000190 - Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.

Info

Certain encryption types are no longer considered secure. This setting configures a minimum encryption type for Kerberos, preventing the use of the DES and RC4 encryption suites.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: Configure encryption types allowed for Kerberos' to 'Enabled' with only the following selected:
AES128_HMAC_SHA1 AES256_HMAC_SHA1 Future encryption types

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	IA-7
800-53R5	IA-7
CAT	II
CCI	CCI-000803
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
ITSG-33	IA-7
ITSG-33	IA-7a.
NESA	M5.2.1
NESA	M5.2.6
NESA	M5.3.1
NESA	T7.4.1
QCSC-V1	13.2
RULE-ID	SV-253460r971535_rule
STIG-ID	WN11-SO-000190
VULN-ID	V-253460

Assets

vm-win11-stig-s

WN11-SO-000195 - The system must be configured to prevent the storage of the LAN Manager hash of passwords.

Info

The LAN Manager hash uses a weak encryption algorithm and there are several tools available that use this hash to retrieve account passwords. This setting controls whether or not a LAN Manager hash of the password is stored in the SAM the next time the password is changed.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.5.10
800-171R3	03.05.07c.
800-53	IA-5(1)(c)
800-53R5	IA-5(1)(d)
CAT	I
CCI	CCI-000196
CCI	CCI-004062
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)(c)
NESA	T5.2.3
NIAV2	CY6
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253461r1051056_rule

STIG-ID	WN11-SO-000195
SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-253461

Assets

vm-win11-stig-s

WN11-SO-000205 - The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.

Info

The Kerberos v5 authentication protocol is the default for authentication of users who are logging on to domain accounts. NTLM, which is less secure, is retained in later Windows versions for compatibility with clients and servers that are running earlier versions of Windows or applications that still use it. It is also used to authenticate logons to stand-alone computers that are running later versions.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253462r991589_rule
STIG-ID	WN11-SO-000205
SWIFT-CSCV1	2.3
VULN-ID	V-253462

Assets

vm-win11-stig-s

WN11-SO-000210 - The system must be configured to the required LDAP client signing level.

Info

This setting controls the signing requirements for LDAP clients. This setting must be set to Negotiate signing or Require signing, depending on the environment and type of LDAP server in use.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: LDAP client signing requirements' to 'Negotiate signing' at a minimum.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253463r991589_rule
STIG-ID	WN11-SO-000210
SWIFT-CSCV1	2.3
VULN-ID	V-253463

Assets

vm-win11-stig-s

WN11-SO-000215 - The system must be configured to meet the minimum session security requirement for NTLM SSP based clients.

Info

Microsoft has implemented a variety of security support providers for use with RPC sessions. All of the options must be enabled to ensure the maximum security level.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security' and 'Require 128-bit encryption' (all options selected).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253464r991589_rule
STIG-ID	WN11-SO-000215
SWIFT-CSCV1	2.3
VULN-ID	V-253464

Assets

vm-win11-stig-s

WN11-SO-000220 - The system must be configured to meet the minimum session security requirement for NTLM SSP based servers.

Info

Microsoft has implemented a variety of security support providers for use with RPC sessions. All of the options must be enabled to ensure the maximum security level.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security' and 'Require 128-bit encryption' (all options selected).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253465r991589_rule
STIG-ID	WN11-SO-000220
SWIFT-CSCV1	2.3
VULN-ID	V-253465

Assets

vm-win11-stig-s

WN11-SO-000230 - The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.

Info

This setting ensures that the system uses algorithms that are FIPS-compliant for encryption, hashing, and signing. FIPS-compliant algorithms meet specific standards established by the U.S. Government and must be the algorithms used for all OS encryption functions.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.13.11
800-171R3	03.13.11
800-53	SC-13
800-53R5	SC-13b.
CAT	II
CCI	CCI-002450
CSF	PR.DS-5
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.8.24
ISO/IEC-27001	A.10.1.1
ITSG-33	SC-13
ITSG-33	SC-13a.
NESA	M5.2.6
NESA	T7.4.1
NIAV2	CY3

NIAV2	CY4
NIAV2	CY5b
NIAV2	CY5c
NIAV2	CY5d
NIAV2	CY7
NIAV2	NS5e
QCSC-V1	6.2
RULE-ID	SV-253466r1137699_rule
STIG-ID	WN11-SO-000230
VULN-ID	V-253466

Assets

vm-win11-stig-s

WN11-SO-000240 - The default permissions of global system objects must be increased.

Info

Windows systems maintain a global list of shared system resources such as DOS device names, mutexes, and semaphores. Each type of object is created with a default DACL that specifies who can access the objects with what permissions. If this policy is enabled, the default DACL is stronger, allowing non-admin users to read shared objects, but not modify shared objects that they did not create.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic links)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253467r991589_rule
STIG-ID	WN11-SO-000240
SWIFT-CSCV1	2.3
VULN-ID	V-253467

Assets

vm-win11-stig-s

WN11-SO-000245 - User Account Control approval mode for the built-in Administrator must be enabled.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting configures the built-in Administrator account so that it runs in Admin Approval Mode.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253468r1051057_rule
STIG-ID	WN11-SO-000245
VULN-ID	V-253468

Assets

vm-win11-stig-s

WN11-SO-000250 - User Account Control must prompt administrators for consent on the secure desktop.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting configures the elevation requirements for logged on administrators to complete a task that requires raised privileges.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' to 'Prompt for consent on the secure desktop'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253469r958518_rule
STIG-ID	WN11-SO-000250
VULN-ID	V-253469

Assets

vm-win11-stig-s

WN11-SO-000255 - User Account Control must automatically deny elevation requests for standard users.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. Denying elevation requests from standard user accounts requires tasks that need elevation to be initiated by accounts with administrative privileges. This ensures correct accounts are used on the system for privileged tasks to help mitigate credential theft.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Behavior of the elevation prompt for standard users' to 'Automatically deny elevation requests'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253471r1051058_rule
STIG-ID	WN11-SO-000255
VULN-ID	V-253471

Assets

vm-win11-stig-s

WN11-SO-000260 - User Account Control must be configured to detect application installations and prompt for elevation.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting requires Windows to respond to application installation requests by prompting for credentials.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253472r958518_rule
STIG-ID	WN11-SO-000260
VULN-ID	V-253472

Assets

vm-win11-stig-s

WN11-SO-000265 - User Account Control must only elevate UIAccess applications that are installed in secure locations.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting configures Windows to only allow applications installed in a secure location on the file system, such as the Program Files or the Windows\System32 folders, to run with elevated privileges.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253473r958518_rule
STIG-ID	WN11-SO-000265
VULN-ID	V-253473

Assets

vm-win11-stig-s

WN11-SO-000270 - User Account Control must run all administrators in Admin Approval Mode, enabling UAC.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting enables UAC.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253474r1051059_rule
STIG-ID	WN11-SO-000270
VULN-ID	V-253474

Assets

vm-win11-stig-s

WN11-SO-000275 - User Account Control must virtualize file and registry write failures to per-user locations.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting configures non-UAC compliant applications to run in virtualized file and registry entries in per-user locations, allowing them to run.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253475r958518_rule
STIG-ID	WN11-SO-000275
VULN-ID	V-253475

Assets

vm-win11-stig-s

WN11-UC-000015 - Toast notifications to the lock screen must be turned off.

Info

Toast notifications that are displayed on the lock screen could display sensitive information to unauthorized personnel. Turning off this feature will limit access to the information to a logged on user.

Solution

Configure the policy value for User Configuration >> Administrative Templates >> Start Menu and Taskbar >> Notifications >> 'Turn off toast notifications on the lock screen' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	III
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253477r958478_rule
STIG-ID	WN11-UC-000015
SWIFT-CSCV1	2.3
VULN-ID	V-253477

Assets

vm-win11-stig-s

WN11-UC-000020 - Zone information must be preserved when saving attachments.

Info

Preserving zone of origin (internet, intranet, local, restricted) information on file attachments allows Windows to determine risk.

Solution

The default behavior is for Windows to mark file attachments with their zone information.
To correct this, configure the policy value for User Configuration >> Administrative Templates >> Windows Components >> Attachment Manager >> 'Do not preserve zone information in file attachments' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253478r991589_rule
STIG-ID	WN11-UC-000020
SWIFT-CSCV1	2.3
VULN-ID	V-253478

Assets

vm-win11-stig-s

WN11-UR-000005 - The 'Access Credential Manager as a trusted caller' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Access Credential Manager as a trusted caller' user right may be able to retrieve the credentials of other accounts from Credential Manager.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Access Credential Manager as a trusted caller' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253479r958726_rule
STIG-ID	WN11-UR-000005
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253479

Assets

vm-win11-stig-s

WN11-UR-000010 - The 'Access this computer from the network' user right must only be assigned to the Administrators and Remote Desktop Users groups.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Access this computer from the network' user right may access resources on the system, and must be limited to those that require it.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Access this computer from the network' to only include the following groups or accounts: Administrators Remote Desktop Users

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3

ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253480r1137691_rule
STIG-ID	WN11-UR-000010
TBA-FIISB	31.1
VULN-ID	V-253480

Assets

vm-win11-stig-s

WN11-UR-000015 - The 'Act as part of the operating system' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Act as part of the operating system' user right can assume the identity of any user and gain access to resources that user is authorized to access. Any accounts with this right can take complete control of a system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Act as part of the operating system' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	I
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253481r958726_rule
STIG-ID	WN11-UR-000015
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253481

Assets

vm-win11-stig-s

WN11-UR-000025 - The 'Allow log on locally' user right must only be assigned to the Administrators and Users groups.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Allow log on locally' user right can log on interactively to a system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Allow log on locally' to only include the following groups or accounts:
Administrators Users

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3

ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253482r1137691_rule
STIG-ID	WN11-UR-000025
TBA-FIISB	31.1
VULN-ID	V-253482

Assets

vm-win11-stig-s

WN11-UR-000030 - The 'Back up files and directories' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Back up files and directories' user right can circumvent file and directory permissions and could allow access to sensitive data.'

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Back up files and directories' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253483r958726_rule
STIG-ID	WN11-UR-000030
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253483

Assets

vm-win11-stig-s

WN11-UR-000035 - The 'Change the system time' user right must only be assigned to Administrators and Local Service.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Change the system time' user right can change the system time, which can impact authentication, as well as affect time stamps on event log entries.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Change the system time' to only include the following groups or accounts: Administrators LOCAL SERVICE

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253484r958726_rule
STIG-ID	WN11-UR-000035
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253484

Assets

vm-win11-stig-s

WN11-UR-000040 - The 'Create a pagefile' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Create a pagefile' user right can change the size of a pagefile, which could affect system performance.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Create a pagefile' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253485r958726_rule
STIG-ID	WN11-UR-000040
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253485

Assets

vm-win11-stig-s

WN11-UR-000045 - The 'Create a token object' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Create a token object' user right allows a process to create an access token. This could be used to provide elevated rights and compromise a system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Create a token object' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	I
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253486r958726_rule
STIG-ID	WN11-UR-000045
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253486

Assets

vm-win11-stig-s

WN11-UR-000050 - The 'Create global objects' user right must only be assigned to Administrators, Service, Local Service, and Network Service.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Create global objects' user right can create objects that are available to all sessions, which could affect processes in other users' sessions.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Create global objects' to only include the following groups or accounts:
Administrators LOCAL SERVICE NETWORK SERVICE SERVICE

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253487r958726_rule
STIG-ID	WN11-UR-000050
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253487

Assets

vm-win11-stig-s

WN11-UR-000055 - The 'Create permanent shared objects' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Create permanent shared objects' user right could expose sensitive data by creating shared objects.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Create permanent shared objects' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253488r958726_rule
STIG-ID	WN11-UR-000055
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253488

Assets

vm-win11-stig-s

WN11-UR-000060 - The 'Create symbolic links' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Create symbolic links' user right can create pointers to other objects, which could potentially expose the system to attack.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Create symbolic links' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253489r958726_rule
STIG-ID	WN11-UR-000060
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253489

Assets

vm-win11-stig-s

WN11-UR-000065 - The 'Debug programs' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Debug Programs' user right can attach a debugger to any process or to the kernel, providing complete access to sensitive and critical operating system components. This right is given to Administrators in the default configuration.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Debug programs' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	I
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2

NESA	T5.4.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253490r958726_rule
STIG-ID	WN11-UR-000065
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253490

Assets

vm-win11-stig-s

WN11-UR-000070 - The 'Deny access to this computer from the network' user right on workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Deny access to this computer from the network' right defines the accounts that are prevented from logging on from the network.
In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.
Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks.
The Guests group must be assigned this right to prevent unauthenticated access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny access to this computer from the network' to include the following:
Domain Systems Only:
Enterprise Admins group Domain Admins group Local account (see Note below)
All Systems:
Guests group
Privileged Access Workstations (PAWs) dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW requirements.)
Note: 'Local account' is a built-in security group used to assign user rights and permissions to all local accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01

DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253491r1137691_rule
STIG-ID	WN11-UR-000070
TBA-FIISB	31.1
VULN-ID	V-253491

Assets

vm-win11-stig-s

WN11-UR-000085 - The 'Deny log on locally' user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Deny log on locally' right defines accounts that are prevented from logging on interactively.
In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.
The Guests group must be assigned this right to prevent unauthenticated access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on locally' to include the following:
Domain Systems Only:
Enterprise Admins Group Domain Admins Group
Privileged Access Workstations (PAWs) dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW requirements.)
All Systems:
Guests Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253494r1137691_rule
STIG-ID	WN11-UR-000085
TBA-FIISB	31.1
VULN-ID	V-253494

Assets

vm-win11-stig-s

WN11-UR-000090 - The 'Deny log on through Remote Desktop Services' user right on Windows 11 workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Deny log on through Remote Desktop Services' right defines the accounts that are prevented from logging on using Remote Desktop Services.
If Remote Desktop Services is not used by the organization, the Everyone group must be assigned this right to prevent all access.
In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.
Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks.
The Guests group must be assigned this right to prevent unauthenticated access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on through Remote Desktop Services' to include the following:
If Remote Desktop Services is not used by the organization, assign the Everyone group this right to prevent all access.
Domain Systems Only:
Enterprise Admins group Domain Admins group Local account (see Note below)
All Systems:
Guests group
Privileged Access Workstations (PAWs) dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW requirements.)
Note: 'Local account' is a built-in security group used to assign user rights and permissions to all local accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.1
800-171	3.1.12
800-171R3	03.01.02
800-171R3	03.01.12
800-53	AC-3
800-53	AC-17(1)
800-53R5	AC-3
800-53R5	AC-17(1)
CAT	II
CCI	CCI-000213
CCI	CCI-002314
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.4(c)
CN-L3	8.1.4.11(b)

CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(i)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-3
CSF	PR.AC-4
CSF	PR.PT-3
CSF	PR.PT-4
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.2.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-17(1)
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1

NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253495r1137691_rule
STIG-ID	WN11-UR-000090
SWIFT-CSCV1	2.6
TBA-FIISB	31.1
VULN-ID	V-253495

Assets

vm-win11-stig-s

WN11-UR-000095 - The 'Enable computer and user accounts to be trusted for delegation' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Enable computer and user accounts to be trusted for delegation' user right allows the 'Trusted for Delegation' setting to be changed. This could potentially allow unauthorized users to impersonate other users.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Enable computer and user accounts to be trusted for delegation' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253496r958726_rule
STIG-ID	WN11-UR-000095
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253496

Assets

vm-win11-stig-s

WN11-UR-000100 - The 'Force shutdown from a remote system' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Force shutdown from a remote system' user right can remotely shut down a system which could result in a DoS.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Force shutdown from a remote system' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253497r958726_rule
STIG-ID	WN11-UR-000100
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253497

Assets

vm-win11-stig-s

WN11-UR-000110 - The 'Impersonate a client after authentication' user right must only be assigned to Administrators, Service, Local Service, and Network Service.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Impersonate a client after authentication' user right allows a program to impersonate another user or account to run on their behalf. An attacker could potentially use this to elevate privileges.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Impersonate a client after authentication' to only include the following groups or accounts: Administrators LOCAL SERVICE NETWORK SERVICE RESTRICTED SERVICES\PrintSpoolerService SERVICE

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253498r1138526_rule
STIG-ID	WN11-UR-000110
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253498

Assets

vm-win11-stig-s

WN11-UR-000120 - The 'Load and unload device drivers' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Load and unload device drivers' user right allows device drivers to dynamically be loaded on a system by a user.
This could potentially be used to install malicious code by an attacker.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Load and unload device drivers' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253499r958726_rule
STIG-ID	WN11-UR-000120
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253499

Assets

vm-win11-stig-s

WN11-UR-000125 - The 'Lock pages in memory' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Lock pages in memory' user right allows physical memory to be assigned to processes, which could cause performance issues or a DoS.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Lock pages in memory' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253500r958726_rule
STIG-ID	WN11-UR-000125
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253500

Assets

vm-win11-stig-s

WN11-UR-000130 - The 'Manage auditing and security log' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Manage auditing and security log' user right can manage the security log and change auditing configurations. This could be used to clear evidence of tampering.
Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000063-GPOS-00032

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Manage auditing and security log' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.8
800-171R3	03.03.03
800-171R3	03.03.08
800-53	AU-9
800-53	AU-12b.
800-53R5	AU-9a.
800-53R5	AU-12b.
CAT	II
CCI	CCI-000162
CCI	CCI-000171
CN-L3	7.1.2.3(d)
CN-L3	7.1.3.3(f)
CN-L3	8.1.3.5(c)
CN-L3	8.1.4.3(c)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03

CSF2.0	DE.CM-09
CSF2.0	PR.DS-10
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.2
ITSG-33	AU-9
ITSG-33	AU-12b.
NESA	M5.2.3
NESA	M5.5.2
NESA	T3.6.4
NESA	T8.2.9
NIAV2	SM5
NIAV2	SM6
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.5
PCI-DSSV3.2.1	10.5.2
PCI-DSSV4.0	10.3.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253501r958434_rule
STIG-ID	WN11-UR-000130
SWIFT-CSCV1	6.4
VULN-ID	V-253501

Assets

vm-win11-stig-s

WN11-UR-000140 - The 'Modify firmware environment values' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Modify firmware environment values' user right can change hardware configuration environment variables. This could result in hardware failures or a DoS.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Modify firmware environment values' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253502r958726_rule
STIG-ID	WN11-UR-000140
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253502

Assets

vm-win11-stig-s

WN11-UR-000145 - The 'Perform volume maintenance tasks' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Perform volume maintenance tasks' user right can manage volume and disk configurations. They could potentially delete volumes, resulting in data loss or a DoS.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Perform volume maintenance tasks' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253503r958726_rule
STIG-ID	WN11-UR-000145
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253503

Assets

vm-win11-stig-s

WN11-UR-000150 - The 'Profile single process' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Profile single process' user right can monitor non-system processes performance. An attacker could potentially use this to identify processes to attack.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Profile single process' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253504r958726_rule
STIG-ID	WN11-UR-000150
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253504

Assets

vm-win11-stig-s

WN11-UR-000160 - The 'Restore files and directories' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Restore files and directories' user right can circumvent file and directory permissions and could allow access to sensitive data. It could also be used to over-write more current data.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Restore files and directories' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253505r958726_rule
STIG-ID	WN11-UR-000160
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253505

Assets

vm-win11-stig-s

WN11-UR-000165 - The 'Take ownership of files or other objects' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Take ownership of files or other objects' user right can take ownership of objects and make changes.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Take ownership of files or other objects' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R5_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253506r958726_rule
STIG-ID	WN11-UR-000165
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253506

Assets

vm-win11-stig-s