Tenable Vulnerability Management Report

Tenable Vulnerability Management

Wed, 10 Sep 2025 22:59:25 UTC

Table Of Contents

Audits FAILED

WN10-00-000032 - Windows 10 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_10_V3R4_STIG.zip

References

800-171	3.13.16
800-171R3	03.13.08
800-53	SC-28
800-53	SC-28(1)
800-53R5	SC-28
800-53R5	SC-28(1)
CAT	I
CCI	CCI-001199
CCI	CCI-002475
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	MS_Windows_10_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.
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-220704r958552_rule
STIG-ID	WN10-00-000032
STIG-LEGACY	SV-104691
STIG-LEGACY	V-94861
TBA-FIISB	28.1
VULN-ID	V-220704

Assets

10.0.0.103

```
NULL
```

WN10-00-000090 - 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_10_V3R4_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	MS_Windows_10_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-220716r1051019_rule
STIG-ID	WN10-00-000090
STIG-LEGACY	SV-77861
STIG-LEGACY	V-63371
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-220716

Assets

10.0.0.103

```
'Name          SID
----          ---
admin         S-1-5-21-3886575422-42670501-2848359638-1001
administrator S-1-5-21-3886575422-42670501-2848359638-1000
Guest         S-1-5-21-3886575422-42670501-2848359638-501
user1lab      S-1-5-21-3886575422-42670501-2848359638-500'
```

WN10-00-000145 - Data Execution Prevention (DEP) must be configured to at least OptOut.

Info

Attackers are constantly looking for vulnerabilities in systems and applications. Data Execution Prevention (DEP) prevents harmful code from running in protected memory locations reserved for Windows and other programs.

Solution

Configure DEP to at least OptOut.
Note: Suspend BitLocker before making changes to the DEP configuration.
Open a command prompt (cmd.exe) or PowerShell with elevated privileges (Run as administrator).
Enter 'BCDEDIT /set {current} nx OptOut'. (If using PowerShell '{current}' must be enclosed in quotes.) 'AlwaysOn', a more restrictive selection, is also valid but does not allow applications that do not function properly to be opted out of DEP.
Opted out exceptions can be configured in the 'System Properties'.
Open 'System' in Control Panel.
Select 'Advanced system settings'.
Click 'Settings' in the 'Performance' section.
Select the 'Data Execution Prevention' tab.
Applications that are opted out are configured in the window below the selection 'Turn on DEP for all programs and services except those I select:'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_STIG.zip

References

800-53	SI-16
800-53R5	SI-16
CAT	I
CCI	CCI-002824
CSF2.0	PR.DS-10
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
RULE-ID	SV-220726r958928_rule
STIG-ID	WN10-00-000145
STIG-LEGACY	SV-83439
STIG-LEGACY	V-68845
VULN-ID	V-220726

Assets

10.0.0.103

```
'nx                    OptIn'
```

WN10-00-000155 - 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 should 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_10_V3R4_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	MS_Windows_10_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-220728r958478_rule
STIG-ID	WN10-00-000155
STIG-LEGACY	SV-85259
STIG-LEGACY	V-70637
SWIFT-CSCV1	2.3
VULN-ID	V-220728

Assets

10.0.0.103

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - PowerShellv2:
 Remote value: 'FeatureName : MicrosoftWindowsPowerShellV2
State       : Enabled'
 Policy value: 'State[\s]+:[\s]+Disabled'


-------------------------
FAILED - PowerShellv2Root:
 Remote value: 'FeatureName : MicrosoftWindowsPowerShellV2Root
State       : Enabled'
 Policy value: 'State[\s]+:[\s]+Disabled'
```

WN10-00-000175 - The Secondary Logon service must be disabled on Windows 10.

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_10_V3R4_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	MS_Windows_10_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-220732r958478_rule
STIG-ID	WN10-00-000175
STIG-LEGACY	SV-89393
STIG-LEGACY	V-74719
SWIFT-CSCV1	2.3

VULN-ID	V-220732

Assets

10.0.0.103

```
'manual'
```

WN10-AC-000005 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220739r958736_rule
STIG-ID	WN10-AC-000005
STIG-LEGACY	SV-77895
STIG-LEGACY	V-63405
TBA-FIISB	36.2.4

TBA-FIISB	45.1.2
VULN-ID	V-220739

Assets

10.0.0.103

10

WN10-AC-000010 - The number of allowed bad logon attempts must be configured to 3 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_10_V3R4_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	MS_Windows_10_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-220740r958388_rule
STIG-ID	WN10-AC-000010
STIG-LEGACY	SV-77899
STIG-LEGACY	V-63409
TBA-FIISB	45.1.2
TBA-FIISB	45.2.1

TBA-FIISB	45.2.2
VULN-ID	V-220740

Assets

10.0.0.103

10

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.8
800-171R3	03.01.08a.
800-171R3	03.01.08b.
800-53	AC-7a.
800-53	AC-7b.
800-53R5	AC-7a.
800-53R5	AC-7b.
CAT	II
CCI	CCI-000044
CCI	CCI-002238
CN-L3	7.1.2.7(f)
CN-L3	7.1.3.1(c)
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-7a.
ITSG-33	AC-7b.
NESA	T5.5.1
NIAV2	AM24
PCI-DSSV3.2.1	8.1.6

PCI-DSSV3.2.1	8.1.7
PCI-DSSV4.0	8.3.4
RULE-ID	SV-220741r958388_rule
STIG-ID	WN10-AC-000015
STIG-LEGACY	SV-77903
STIG-LEGACY	V-63413
TBA-FIISB	36.2.4
TBA-FIISB	45.1.2
TBA-FIISB	45.2.1
TBA-FIISB	45.2.2
VULN-ID	V-220741

Assets

10.0.0.103

```
10
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220742r1000079_rule

STIG-ID	WN10-AC-000020
STIG-LEGACY	SV-77905
STIG-LEGACY	V-63415
SWIFT-CSCV1	4.1
VULN-ID	V-220742

Assets

10.0.0.103

0

WN10-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_10_V3R4_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	MS_Windows_10_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-220744r1051021_rule
STIG-ID	WN10-AC-000030
STIG-LEGACY	SV-77911
STIG-LEGACY	V-63421
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-220744

Assets

10.0.0.103

```
0
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220745r1051022_rule
STIG-ID	WN10-AC-000035
STIG-LEGACY	SV-77913
STIG-LEGACY	V-63423
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.1
TBA-FIISB	26.2.4
VULN-ID	V-220745

Assets

10.0.0.103

0

WN10-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_10_V3R4_STIG.zip

References

800-171	3.5.7
800-171R3	03.05.07a.
800-53	IA-5(1)(a)
800-53R5	IA-5(1)(a)
CAT	II
CCI	CCI-000192
CCI	CCI-000193
CCI	CCI-000194
CCI	CCI-001619
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	MS_Windows_10_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-220746r1051023_rule
STIG-ID	WN10-AC-000040
STIG-LEGACY	SV-77917
STIG-LEGACY	V-63427
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.1
TBA-FIISB	26.2.4
VULN-ID	V-220746

Assets

10.0.0.103

```
'disabled'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220748r991578_rule
STIG-ID	WN10-AU-000005
STIG-LEGACY	SV-77921
STIG-LEGACY	V-63431
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220748

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220749r991578_rule
STIG-ID	WN10-AU-000010
STIG-LEGACY	SV-77925
STIG-LEGACY	V-63435
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220749

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220753r1051025_rule
STIG-ID	WN10-AU-000045
STIG-LEGACY	SV-77941
STIG-LEGACY	V-63451
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220753

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220754r1051026_rule
STIG-ID	WN10-AU-000050
STIG-LEGACY	SV-77943
STIG-LEGACY	V-63453
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220754

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220755r991578_rule
STIG-ID	WN10-AU-000054
STIG-LEGACY	SV-86383
STIG-LEGACY	V-71759
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220755

Assets

10.0.0.103

```
'success'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220756r991578_rule
STIG-ID	WN10-AU-000060
STIG-LEGACY	SV-77947
STIG-LEGACY	V-63457
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220756

Assets

10.0.0.103

```
'no auditing'
```

WN10-AU-000081 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220761r991583_rule
STIG-ID	WN10-AU-000081
STIG-LEGACY	SV-89701
STIG-LEGACY	V-75027
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220761

Assets

10.0.0.103

```
'no auditing'
```

WN10-AU-000082 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220762r991583_rule
STIG-ID	WN10-AU-000082
STIG-LEGACY	SV-89395
STIG-LEGACY	V-74721
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220762

Assets

10.0.0.103

```
'no auditing'
```

WN10-AU-000083 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220763r991583_rule
STIG-ID	WN10-AU-000083
STIG-LEGACY	SV-89085
STIG-LEGACY	V-74411
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220763

Assets

10.0.0.103

```
'no auditing'
```

WN10-AU-000084 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220764r991583_rule
STIG-ID	WN10-AU-000084
STIG-LEGACY	SV-89083
STIG-LEGACY	V-74409
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220764

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220765r991583_rule
STIG-ID	WN10-AU-000085
STIG-LEGACY	SV-77961
STIG-LEGACY	V-63471
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220765

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220766r991583_rule
STIG-ID	WN10-AU-000090
STIG-LEGACY	SV-77963
STIG-LEGACY	V-63473
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220766

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220769r991579_rule
STIG-ID	WN10-AU-000107
STIG-LEGACY	SV-86385
STIG-LEGACY	V-71761
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220769

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-220770r958732_rule
STIG-ID	WN10-AU-000110
STIG-LEGACY	SV-77973
STIG-LEGACY	V-63483
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-220770

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-220771r958732_rule
STIG-ID	WN10-AU-000115
STIG-LEGACY	SV-77977
STIG-LEGACY	V-63487
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-220771

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220772r991586_rule
STIG-ID	WN10-AU-000120
STIG-LEGACY	SV-77981
STIG-LEGACY	V-63491
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220772

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)

CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1

NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-220776r958732_rule
STIG-ID	WN10-AU-000150
STIG-LEGACY	SV-78003
STIG-LEGACY	V-63513
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-220776

Assets

10.0.0.103

```
'no auditing'
```

WN10-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, documented with the ISSO.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220780r958752_rule
STIG-ID	WN10-AU-000505
STIG-LEGACY	SV-78013
STIG-LEGACY	V-63523
VULN-ID	V-220780

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_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-220781r958752_rule
STIG-ID	WN10-AU-000510
STIG-LEGACY	SV-78017
STIG-LEGACY	V-63527
VULN-ID	V-220781

Assets

10.0.0.103

NULL

WN10-AU-000555 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220786r958412_rule
STIG-ID	WN10-AU-000555
STIG-LEGACY	SV-108657
STIG-LEGACY	V-99553
SWIFT-CSCV1	6.4
VULN-ID	V-220786

Assets

10.0.0.103

```
'no auditing'
```

WN10-AU-000560 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220787r958412_rule
STIG-ID	WN10-AU-000560
STIG-LEGACY	SV-108647
STIG-LEGACY	V-99543
SWIFT-CSCV1	6.4
VULN-ID	V-220787

Assets

10.0.0.103

```
'no auditing'
```

WN10-AU-000565 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220788r958412_rule
STIG-ID	WN10-AU-000565
STIG-LEGACY	SV-108645
STIG-LEGACY	V-99541
SWIFT-CSCV1	6.4
VULN-ID	V-220788

Assets

10.0.0.103

```
'no auditing'
```

WN10-AU-000570 - Windows 10 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 auditing of 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_10_V3R4_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	MS_Windows_10_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-220789r958412_rule
STIG-ID	WN10-AU-000570
STIG-LEGACY	SV-108649
STIG-LEGACY	V-99545
SWIFT-CSCV1	6.4
VULN-ID	V-220789

Assets

10.0.0.103

```
'no auditing'
```

WN10-AU-000575 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220790r958412_rule
STIG-ID	WN10-AU-000575
STIG-LEGACY	SV-108651
STIG-LEGACY	V-99547
SWIFT-CSCV1	6.4
VULN-ID	V-220790

Assets

10.0.0.103

```
'no auditing'
```

WN10-AU-000580 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220791r958412_rule
STIG-ID	WN10-AU-000580
STIG-LEGACY	SV-108653
STIG-LEGACY	V-99549
SWIFT-CSCV1	6.4
VULN-ID	V-220791

Assets

10.0.0.103

```
'no auditing'
```

WN10-AU-000585 - Windows 10 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 >> Audit Process Creation is set to 'failure'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-257589r958412_rule
STIG-ID	WN10-AU-000585
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-257589

Assets

10.0.0.103

```
'no auditing'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220792r958478_rule
STIG-ID	WN10-CC-000005
STIG-LEGACY	SV-78035
STIG-LEGACY	V-63545

SWIFT-CSCV1	2.3
VULN-ID	V-220792

Assets

10.0.0.103

NULL

WN10-CC-000007 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220793r958478_rule
STIG-ID	WN10-CC-000007
STIG-LEGACY	SV-109197
STIG-LEGACY	V-100093
SWIFT-CSCV1	2.3
VULN-ID	V-220793

Assets

10.0.0.103

```
'Allow'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220795r991589_rule
STIG-ID	WN10-CC-000020
STIG-LEGACY	SV-78045
STIG-LEGACY	V-63555
SWIFT-CSCV1	2.3
VULN-ID	V-220795

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220796r991589_rule
STIG-ID	WN10-CC-000025
STIG-LEGACY	SV-78049
STIG-LEGACY	V-63559
SWIFT-CSCV1	2.3
VULN-ID	V-220796

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220797r991589_rule
STIG-ID	WN10-CC-000030
STIG-LEGACY	SV-78053
STIG-LEGACY	V-63563
SWIFT-CSCV1	2.3
VULN-ID	V-220797

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220798r958902_rule
STIG-ID	WN10-CC-000035
STIG-LEGACY	SV-78057
STIG-LEGACY	V-63567

VULN-ID	V-220798

Assets

10.0.0.103

NULL

WN10-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 10. 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 10.
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_10_V3R4_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	MS_Windows_10_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-220800r958478_rule
STIG-ID	WN10-CC-000038

STIG-LEGACY	SV-86387
STIG-LEGACY	V-71763
SWIFT-CSCV1	2.3
VULN-ID	V-220800

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_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-220801r958478_rule
STIG-ID	WN10-CC-000039

STIG-LEGACY	SV-86953
STIG-LEGACY	V-72329
SWIFT-CSCV1	2.3
VULN-ID	V-220801

Assets

10.0.0.103

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - batfile:
 Remote value: NULL
 Policy value: 4096


-------------------------
FAILED - cmdfile:
 Remote value: NULL
 Policy value: 4096


-------------------------
FAILED - exefile:
 Remote value: NULL
 Policy value: 4096


-------------------------
FAILED - mscfile:
 Remote value: NULL
 Policy value: 4096
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220802r991589_rule
STIG-ID	WN10-CC-000040
STIG-LEGACY	SV-78059
STIG-LEGACY	V-63569
SWIFT-CSCV1	2.3
VULN-ID	V-220802

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220803r958478_rule
STIG-ID	WN10-CC-000044
STIG-LEGACY	SV-86389
STIG-LEGACY	V-71765

SWIFT-CSCV1	2.3
VULN-ID	V-220803

Assets

10.0.0.103

NULL

WN10-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 to 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_10_V3R4_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	MS_Windows_10_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-250319r991589_rule
STIG-ID	WN10-CC-000050
STIG-LEGACY	SV-78067
STIG-LEGACY	V-63577
SWIFT-CSCV1	2.3
VULN-ID	V-250319

Assets

10.0.0.103

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - SYSVOL:
 Remote value: ''
 Policy value: 'RequireMutualAuthentication=1,[\s]*RequireIntegrity=1'


-------------------------
FAILED - NETLOGON:
 Remote value: ''
 Policy value: 'RequireMutualAuthentication=1,[\s]*RequireIntegrity=1'
```

WN10-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 should 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_10_V3R4_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	MS_Windows_10_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-220807r991589_rule
STIG-ID	WN10-CC-000060
STIG-LEGACY	SV-78075
STIG-LEGACY	V-63585
SWIFT-CSCV1	2.3
VULN-ID	V-220807

Assets

10.0.0.103

```
NULL
```

WN10-CC-000068 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220810r991589_rule
STIG-ID	WN10-CC-000068
STIG-LEGACY	SV-89373
STIG-LEGACY	V-74699
SWIFT-CSCV1	2.3
VULN-ID	V-220810

Assets

10.0.0.103

```
NULL
```

WN10-CC-000070 - Virtualization Based Security must be enabled on Windows 10 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

VBS, 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 requirements 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_10_V3R4_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	MS_Windows_10_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-220811r1016359_rule
STIG-ID	WN10-CC-000070
SWIFT-CSCV1	2.3
VULN-ID	V-220811

Assets

10.0.0.103

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - RequiredSecurityProperties:
 Remote value: '0'
 Policy value: '2'


-------------------------
FAILED - VirtualizationBasedSecurityStatus:
 Remote value: '0'
 Policy value: '2'
```

WN10-CC-000085 - Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers.

Info

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').
If this needs to be corrected 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_10_V3R4_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	MS_Windows_10_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-220813r991589_rule
STIG-ID	WN10-CC-000085
STIG-LEGACY	SV-78097
STIG-LEGACY	V-63607
SWIFT-CSCV1	2.3
VULN-ID	V-220813

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220814r991589_rule
STIG-ID	WN10-CC-000090
STIG-LEGACY	SV-78099
STIG-LEGACY	V-63609
SWIFT-CSCV1	2.3
VULN-ID	V-220814

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220815r958478_rule
STIG-ID	WN10-CC-000100
STIG-LEGACY	SV-78105

STIG-LEGACY	V-63615
SWIFT-CSCV1	2.3
VULN-ID	V-220815

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220816r958478_rule
STIG-ID	WN10-CC-000105

STIG-LEGACY	SV-78111
STIG-LEGACY	V-63621
SWIFT-CSCV1	2.3
VULN-ID	V-220816

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220819r958478_rule
STIG-ID	WN10-CC-000120
STIG-LEGACY	SV-78119
STIG-LEGACY	V-63629

SWIFT-CSCV1	2.3
VULN-ID	V-220819

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-220821r1051027_rule
STIG-ID	WN10-CC-000145
STIG-LEGACY	SV-78135
STIG-LEGACY	V-63645
VULN-ID	V-220821

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-220822r1051028_rule
STIG-ID	WN10-CC-000150
STIG-LEGACY	SV-78139
STIG-LEGACY	V-63649
VULN-ID	V-220822

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-220823r958524_rule
STIG-ID	WN10-CC-000155
STIG-LEGACY	SV-78141
STIG-LEGACY	V-63651
VULN-ID	V-220823

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_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-220824r971545_rule
STIG-ID	WN10-CC-000165
STIG-LEGACY	SV-78147
STIG-LEGACY	V-63657
TBA-FIISB	27.1
VULN-ID	V-220824

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220825r991589_rule
STIG-ID	WN10-CC-000170
STIG-LEGACY	SV-78149
STIG-LEGACY	V-63659
SWIFT-CSCV1	2.3
VULN-ID	V-220825

Assets

10.0.0.103

```
NULL
```

WN10-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 you insert media 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_10_V3R4_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	MS_Windows_10_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-220827r958804_rule
STIG-ID	WN10-CC-000180
STIG-LEGACY	SV-78157
STIG-LEGACY	V-63667
SWIFT-CSCV1	2.3
VULN-ID	V-220827

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_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-220828r958804_rule
STIG-ID	WN10-CC-000185
STIG-LEGACY	SV-78161
STIG-LEGACY	V-63671
SWIFT-CSCV1	2.3
VULN-ID	V-220828

Assets

10.0.0.103

NULL

WN10-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 you insert media 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 you enable this policy, you can also disable autoplay 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_10_V3R4_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	MS_Windows_10_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-220829r958804_rule
STIG-ID	WN10-CC-000190
STIG-LEGACY	SV-78163
STIG-LEGACY	V-63673
SWIFT-CSCV1	2.3
VULN-ID	V-220829

Assets

10.0.0.103

```
NULL
```

WN10-CC-000195 - Enhanced anti-spoofing for facial recognition must be enabled on Window 10.

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'.
v1607:
The policy name is 'Use enhanced anti-spoofing when available'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220830r991589_rule
STIG-ID	WN10-CC-000195
STIG-LEGACY	SV-78167
STIG-LEGACY	V-63677
SWIFT-CSCV1	2.3
VULN-ID	V-220830

Assets

10.0.0.103

NULL

WN10-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 whitelisting. 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_10_V3R4_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	MS_Windows_10_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-220831r958478_rule
STIG-ID	WN10-CC-000197
STIG-LEGACY	SV-86395

STIG-LEGACY	V-71771
SWIFT-CSCV1	2.3
VULN-ID	V-220831

Assets

10.0.0.103

```
NULL
```

WN10-CC-000204 - If Enhanced diagnostic data is enabled it 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 Enhanced diagnostic data to the minimum required by Windows Analytics' to 'Enabled' with 'Enable Windows Analytics collection' selected in 'Options:'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220833r991589_rule
STIG-ID	WN10-CC-000204
STIG-LEGACY	SV-96859
STIG-LEGACY	V-82145
SWIFT-CSCV1	2.3
VULN-ID	V-220833

Assets

10.0.0.103

```
NULL
```

WN10-CC-000210 - The Windows Defender SmartScreen for Explorer must be enabled.

Info

Windows Defender SmartScreen helps protect systems from programs downloaded from the internet that may be malicious. Enabling Windows 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 10 includes duplicate policies for this setting. It can also be configured under Computer Configuration >> Administrative Templates >> Windows Components >> Windows Defender SmartScreen >> Explorer.
v1607 LTSB:
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Configure Windows SmartScreen' to 'Enabled'. (Selection options are not available.)
v1507 LTSB:
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Configure Windows SmartScreen' to 'Enabled' with 'Require approval from an administrator before running downloaded unknown software' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220836r958478_rule
STIG-ID	WN10-CC-000210
STIG-LEGACY	SV-78175
STIG-LEGACY	V-63685
SWIFT-CSCV1	2.3
VULN-ID	V-220836

Assets

10.0.0.103

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - EnableSmartScreen:
 Remote value: NULL
 Policy value: 1


-------------------------
FAILED - ShellSmartScreenLevel:
 Remote value: ''
 Policy value: 'Block'
```

WN10-CC-000230 - Users must not be allowed to ignore Windows Defender SmartScreen filter warnings for malicious websites in Microsoft Edge.

Info

The Windows Defender SmartScreen filter in Microsoft Edge provides warning messages and blocks potentially malicious websites and file downloads. If users are allowed to ignore warnings from the Windows Defender SmartScreen filter they could still access malicious websites.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Microsoft Edge >> 'Prevent bypassing Windows Defender SmartScreen prompts for sites' to 'Enabled'.
Windows 10 includes duplicate policies for this setting. It can also be configured under Computer Configuration >> Administrative Templates >> Windows Components >> Windows Defender SmartScreen >> Microsoft Edge.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220840r991589_rule
STIG-ID	WN10-CC-000230
STIG-LEGACY	SV-78189
STIG-LEGACY	V-63699
SWIFT-CSCV1	2.3
VULN-ID	V-220840

Assets

10.0.0.103

```
NULL
```

WN10-CC-000235 - Users must not be allowed to ignore Windows Defender SmartScreen filter warnings for unverified files in Microsoft Edge.

Info

The Windows Defender SmartScreen filter in Microsoft Edge provides warning messages and blocks potentially malicious websites and file downloads. If users are allowed to ignore warnings from the Windows Defender SmartScreen filter they could still download potentially malicious files.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Microsoft Edge >> 'Prevent bypassing Windows Defender SmartScreen prompts for files' to 'Enabled'.
Windows 10 includes duplicate policies for this setting. It can also be configured under Computer Configuration >> Administrative Templates >> Windows Components >> Windows Defender SmartScreen >> Microsoft Edge.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220841r991589_rule
STIG-ID	WN10-CC-000235
STIG-LEGACY	SV-78191
STIG-LEGACY	V-63701
SWIFT-CSCV1	2.3
VULN-ID	V-220841

Assets

10.0.0.103

```
NULL
```

WN10-CC-000238 - Windows 10 must be configured to prevent certificate error overrides in Microsoft Edge.

Info

Web security certificates provide an indication whether a site is legitimate. This policy setting prevents the user from ignoring Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificate errors that interrupt browsing.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Microsoft Edge >> 'Prevent certificate error overrides' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220842r991589_rule
STIG-ID	WN10-CC-000238
STIG-LEGACY	SV-96853
STIG-LEGACY	V-82139
SWIFT-CSCV1	2.3
VULN-ID	V-220842

Assets

10.0.0.103

```
NULL
```

WN10-CC-000245 - The password manager function in the Edge browser must be disabled.

Info

Passwords save locally for re-use when browsing may be subject to compromise. Disabling the Edge password manager will prevent this for the browser.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Microsoft Edge >> 'Configure Password Manager' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220843r991589_rule
STIG-ID	WN10-CC-000245
STIG-LEGACY	SV-78199
STIG-LEGACY	V-63709
SWIFT-CSCV1	2.3
VULN-ID	V-220843

Assets

10.0.0.103

' '

WN10-CC-000250 - The Windows Defender SmartScreen filter for Microsoft Edge must be enabled.

Info

The Windows Defender SmartScreen filter in Microsoft Edge provides warning messages and blocks potentially malicious websites.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Microsoft Edge >> 'Configure Windows Defender SmartScreen' to 'Enabled'.
Windows 10 includes duplicate policies for this setting. It can also be configured under Computer Configuration >> Administrative Templates >> Windows Components >> Windows Defender SmartScreen >> Microsoft Edge.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220844r991589_rule
STIG-ID	WN10-CC-000250
STIG-LEGACY	SV-78203
STIG-LEGACY	V-63713
SWIFT-CSCV1	2.3
VULN-ID	V-220844

Assets

10.0.0.103

```
NULL
```

WN10-CC-000252 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220845r958478_rule
STIG-ID	WN10-CC-000252
STIG-LEGACY	SV-89091

STIG-LEGACY	V-74417
SWIFT-CSCV1	2.3
VULN-ID	V-220845

Assets

10.0.0.103

NULL

WN10-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'.
v1507 LTSB:
The policy path is Computer Configuration >> Administrative Templates >> Windows Components >> Microsoft Passport for Work.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220846r991589_rule
STIG-ID	WN10-CC-000255
STIG-LEGACY	SV-78207
STIG-LEGACY	V-63717
SWIFT-CSCV1	2.3
VULN-ID	V-220846

Assets

10.0.0.103

```
NULL
```

WN10-CC-000260 - Windows 10 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.
v1607 LTSB:
The policy path is Computer Configuration >> Administrative Templates >> Windows Components >> Windows Hello for Business >> Pin Complexity.
v1507 LTSB:
The policy path is Computer Configuration >> Administrative Templates >> Windows Components >> Microsoft Passport for Work >> Pin Complexity.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220847r991589_rule
STIG-ID	WN10-CC-000260
STIG-LEGACY	SV-78211
STIG-LEGACY	V-63721

SWIFT-CSCV1	2.3
VULN-ID	V-220847

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-220848r1051029_rule
STIG-ID	WN10-CC-000270
STIG-LEGACY	SV-78219
STIG-LEGACY	V-63729
VULN-ID	V-220848

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-220849r958524_rule
STIG-ID	WN10-CC-000275
STIG-LEGACY	SV-78221
STIG-LEGACY	V-63731
VULN-ID	V-220849

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-220850r1051030_rule
STIG-ID	WN10-CC-000280
STIG-LEGACY	SV-78223
STIG-LEGACY	V-63733
VULN-ID	V-220850

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220851r991554_rule
STIG-ID	WN10-CC-000285
STIG-LEGACY	SV-78227
STIG-LEGACY	V-63737
SWIFT-CSCV1	2.6
VULN-ID	V-220851

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.13
800-171	3.7.5
800-171R3	03.07.05
800-171R3	03.13.08
800-53	AC-17(2)
800-53	MA-4(6)
800-53R5	AC-17(2)
800-53R5	MA-4(6)
CAT	II
CCI	CCI-000068
CCI	CCI-002890
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.MA-2
CSF	PR.PT-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	MS_Windows_10_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)
ITSG-33	MA-4(6)
NESA	T2.3.4
NESA	T5.4.2
NESA	T5.4.4
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-220852r958408_rule
STIG-ID	WN10-CC-000290
STIG-LEGACY	SV-78231
STIG-LEGACY	V-63741
SWIFT-CSCV1	2.6
TBA-FIISB	45.2.3
VULN-ID	V-220852

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220853r991589_rule
STIG-ID	WN10-CC-000295
STIG-LEGACY	SV-78233
STIG-LEGACY	V-63743
SWIFT-CSCV1	2.3
VULN-ID	V-220853

Assets

10.0.0.103

NULL

WN10-CC-000315 - The Windows Installer 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_10_V3R4_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	MS_Windows_10_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-220857r1051032_rule
STIG-ID	WN10-CC-000315
STIG-LEGACY	SV-77815
STIG-LEGACY	V-63325
SWIFT-CSCV1	5.1
VULN-ID	V-220857

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220859r991591_rule
STIG-ID	WN10-CC-000325
STIG-LEGACY	SV-77823
STIG-LEGACY	V-63333
SWIFT-CSCV1	2.3
VULN-ID	V-220859

Assets

10.0.0.103

```
NULL
```

WN10-CC-000327 - PowerShell Transcription must be enabled on Windows 10.

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_10_V3R4_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-3c.
800-53R5	AU-3e.
CAT	II
CCI	CCI-000132
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	MS_Windows_10_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-252896r958420_rule
STIG-ID	WN10-CC-000327
SWIFT-CSCV1	6.4
VULN-ID	V-252896

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_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-220862r958510_rule
STIG-ID	WN10-CC-000330
STIG-LEGACY	SV-77825
STIG-LEGACY	V-63335
TBA-FIISB	45.2.3
VULN-ID	V-220862

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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
CCI	CCI-003123
CSF	PR.MA-2
DISA_BENCHMARK	MS_Windows_10_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-220863r958848_rule
STIG-ID	WN10-CC-000335
STIG-LEGACY	SV-77829
STIG-LEGACY	V-63339
SWIFT-CSCV1	2.6
TBA-FIISB	45.2.3
VULN-ID	V-220863

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220865r958510_rule
STIG-ID	WN10-CC-000345
STIG-LEGACY	SV-77837
STIG-LEGACY	V-63347
TBA-FIISB	45.2.3
VULN-ID	V-220865

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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
CCI	CCI-003123
CSF	PR.MA-2
DISA_BENCHMARK	MS_Windows_10_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-220866r958848_rule
STIG-ID	WN10-CC-000350
STIG-LEGACY	SV-77859
STIG-LEGACY	V-63369
SWIFT-CSCV1	2.6
TBA-FIISB	45.2.3
VULN-ID	V-220866

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-220867r1051033_rule
STIG-ID	WN10-CC-000355
STIG-LEGACY	SV-77865
STIG-LEGACY	V-63375
VULN-ID	V-220867

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220868r958510_rule
STIG-ID	WN10-CC-000360
STIG-LEGACY	SV-77831
STIG-LEGACY	V-63341
TBA-FIISB	45.2.3
VULN-ID	V-220868

Assets

10.0.0.103

```
NULL
```

WN10-CC-000365 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220869r958400_rule
STIG-ID	WN10-CC-000365
STIG-LEGACY	SV-104549
STIG-LEGACY	V-94719

VULN-ID	V-220869

Assets

10.0.0.103

NULL

WN10-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.
If this needs to be corrected, 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_10_V3R4_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	MS_Windows_10_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-220871r958478_rule
STIG-ID	WN10-CC-000385
STIG-LEGACY	SV-108665
STIG-LEGACY	V-99561

SWIFT-CSCV1	2.3
VULN-ID	V-220871

Assets

10.0.0.103

NULL

WN10-CC-000390 - Windows 10 should 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_10_V3R4_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	MS_Windows_10_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-220872r958478_rule
STIG-ID	WN10-CC-000390
STIG-LEGACY	SV-108667
STIG-LEGACY	V-99563

SWIFT-CSCV1	2.3
VULN-ID	V-220872

Assets

10.0.0.103

```
Non-compliant items:
  HKU\S-1-5-21-3886575422-42670501-2848359638-500\Software\Policies\Microsoft\Windows\CloudContent
 -
```

WN10-CC-000391 - Internet Explorer must be disabled for Windows 10.

Info

Internet Explorer 11 (IE11) is no longer supported on Windows 10 semi-annual channel.

Solution

For Windows 10 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_10_V3R4_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	MS_Windows_10_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-256894r958552_rule
STIG-ID	WN10-CC-000391
SWIFT-CSCV1	2.3
VULN-ID	V-256894

Assets

10.0.0.103

```
NULL
```

WN10-EP-000310 - Windows 10 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(TM) 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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-220902r958524_rule
STIG-ID	WN10-EP-000310
STIG-LEGACY	SV-108661
STIG-LEGACY	V-99557
VULN-ID	V-220902

Assets

10.0.0.103

NULL

WN10-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 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. 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_10_V3R4_STIG.zip

References

800-171	3.5.2
800-171	3.13.15
800-171R3	03.05.12
800-171R3	03.13.15
800-53	IA-5(2)(a)
800-53	SC-23(5)
800-53R5	IA-5(2)(b)(1)
800-53R5	SC-23(5)
CAT	II
CCI	CCI-000185
CCI	CCI-002470
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	MS_Windows_10_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)
ITSG-33	SC-23

ITSG-33	SC-23a.
NESA	T4.5.1
NESA	T5.2.3
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-220903r958448_rule
STIG-ID	WN10-PK-000005
STIG-LEGACY	SV-78069
STIG-LEGACY	V-63579
VULN-ID	V-220903

Assets

10.0.0.103

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Root CA 4:
 Remote value: 'No matching certificates found'
 Policy value: 'B8269F25DBD937ECAFD4C35A9838571723F2D026'


-------------------------
FAILED - Root CA 6:
 Remote value: 'No matching certificates found'
 Policy value: 'D37ECF61C0B4ED88681EF3630C4E2FC787B37AEF'


-------------------------
FAILED - Root CA 5:
 Remote value: 'No matching certificates found'
 Policy value: '4ECB5CC3095670454DA1CBD410FC921F46B8564B'


-------------------------
FAILED - Root CA 3:
 Remote value: 'No matching certificates found'
 Policy value: 'D73CA91102A2204A36459ED32213B467D7CE97FB'
```

WN10-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 certificate on unclassified systems.
ECA Root CA 4
The InstallRoot tool is 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_10_V3R4_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	MS_Windows_10_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-220904r958448_rule
STIG-ID	WN10-PK-000010

STIG-LEGACY	SV-78073
STIG-LEGACY	V-63583
VULN-ID	V-220904

Assets

10.0.0.103

```
'No matching certificates found'
```

WN10-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. 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_10_V3R4_STIG.zip

References

800-171	3.5.2
800-171	3.13.15
800-171R3	03.05.12
800-171R3	03.13.15
800-53	IA-5(2)(a)
800-53	SC-23(5)
800-53R5	IA-5(2)(b)(1)
800-53R5	SC-23(5)
CAT	II
CCI	CCI-000185
CCI	CCI-002470
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	MS_Windows_10_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)

ITSG-33	SC-23
ITSG-33	SC-23a.
NESA	T4.5.1
NESA	T5.2.3
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-220905r958448_rule
STIG-ID	WN10-PK-000015
STIG-LEGACY	SV-78077
STIG-LEGACY	V-63587
VULN-ID	V-220905

Assets

10.0.0.103

```
'No matching certificates found'
```

WN10-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 DOD Root CA 3 - US DOD CCEB Interoperability Root CA 2 9B74964506C7ED9138070D08D5F8B969866560C8 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. 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_10_V3R4_STIG.zip

References

800-171	3.5.2
800-171	3.13.15
800-171R3	03.05.12
800-171R3	03.13.15
800-53	IA-5(2)(a)
800-53	SC-23(5)
800-53R5	IA-5(2)(b)(1)
800-53R5	SC-23(5)
CAT	II
CCI	CCI-000185
CCI	CCI-002470
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	MS_Windows_10_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)
ITSG-33	SC-23
ITSG-33	SC-23a.
NESA	T4.5.1
NESA	T5.2.3
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-220906r1081051_rule
STIG-ID	WN10-PK-000020
STIG-LEGACY	SV-78079
STIG-LEGACY	V-63589
VULN-ID	V-220906

Assets

10.0.0.103

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Root CA 3:
 Remote value: 'No matching certificates found'
 Policy value: '[a-zA-Z\s-]*CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U\.S\. Government, C=US'


-------------------------
FAILED - Root CA 6:
 Remote value: 'No matching certificates found'
 Policy value: '[a-zA-Z\s-]*CN=DoD Root CA 6, OU=PKI, OU=DoD, O=U\.S\. Government, C=US'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220908r958482_rule
STIG-ID	WN10-SO-000005
STIG-LEGACY	SV-78091
STIG-LEGACY	V-63601
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-220908

Assets

10.0.0.103

```
'enabled'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220909r958504_rule
STIG-ID	WN10-SO-000010
STIG-LEGACY	SV-78101

STIG-LEGACY	V-63611
SWIFT-CSCV1	2.8
VULN-ID	V-220909

Assets

10.0.0.103

```
'enabled'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220912r991589_rule
STIG-ID	WN10-SO-000025
STIG-LEGACY	SV-78115
STIG-LEGACY	V-63625
SWIFT-CSCV1	2.3
VULN-ID	V-220912

Assets

10.0.0.103

```
'Guest'
```

WN10-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 should be locked when unattended. The screen saver should 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.

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_10_V3R4_STIG.zip

References

800-171	3.1.10
800-171R3	03.01.10a.
800-53	AC-11a.
800-53R5	AC-11a.
CAT	II
CCI	CCI-000057
CN-L3	8.1.4.1(b)
DISA_BENCHMARK	MS_Windows_10_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-11a.
NESA	T2.3.8
NESA	T2.3.9
NIAV2	AM23a
NIAV2	AM23b
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8
RULE-ID	SV-220920r958402_rule
STIG-ID	WN10-SO-000070

STIG-LEGACY	SV-78159
STIG-LEGACY	V-63669
VULN-ID	V-220920

Assets

10.0.0.103

```
NULL
```

WN10-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.

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_10_V3R4_STIG.zip

References

800-171	3.1.9
800-171R3	03.01.09
800-53	AC-8a.
800-53	AC-8b.
800-53	AC-8c.1.
800-53	AC-8c.2.
800-53	AC-8c.3.
800-53R5	AC-8a.
800-53R5	AC-8b.
800-53R5	AC-8c.1.
800-53R5	AC-8c.2.
800-53R5	AC-8c.3.
CAT	II
CCI	CCI-000048
CCI	CCI-000050
CCI	CCI-001384
CCI	CCI-001385
CCI	CCI-001386

CCI	CCI-001387
CCI	CCI-001388
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-8a.
ITSG-33	AC-8b.
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
NIAV2	AM10f
RULE-ID	SV-220921r958390_rule
STIG-ID	WN10-SO-000075
STIG-LEGACY	SV-78165
STIG-LEGACY	V-63675
TBA-FIISB	45.2.4
VULN-ID	V-220921

Assets

10.0.0.103

```
'No content provided to compare with.'
```

WN10-SO-000080 - The Windows dialog box title for the legal banner 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 WN10-SO-000075.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220922r958390_rule
STIG-ID	WN10-SO-000080
STIG-LEGACY	SV-78171
STIG-LEGACY	V-63681
TBA-FIISB	45.2.4
VULN-ID	V-220922

Assets

10.0.0.103

```
'No content provided to compare with.'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220924r991589_rule
STIG-ID	WN10-SO-000095
STIG-LEGACY	SV-78187
STIG-LEGACY	V-63697
SWIFT-CSCV1	2.3
VULN-ID	V-220924

Assets

10.0.0.103

```
'0'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220925r958908_rule

STIG-ID	WN10-SO-000100
STIG-LEGACY	SV-78193
STIG-LEGACY	V-63703
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-220925

Assets

10.0.0.103

0

WN10-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_10_V3R4_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	MS_Windows_10_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-220927r958908_rule

STIG-ID	WN10-SO-000120
STIG-LEGACY	SV-78209
STIG-LEGACY	V-63719
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-220927

Assets

10.0.0.103

0

WN10-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_10_V3R4_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	MS_Windows_10_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-220933r1081053_rule
STIG-ID	WN10-SO-000167
STIG-LEGACY	SV-86393
STIG-LEGACY	V-71769
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220933

Assets

10.0.0.103

' '

WN10-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_10_V3R4_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	MS_Windows_10_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-220934r991589_rule
STIG-ID	WN10-SO-000180
STIG-LEGACY	SV-78255
STIG-LEGACY	V-63765
SWIFT-CSCV1	2.3
VULN-ID	V-220934

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_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-220935r991589_rule
STIG-ID	WN10-SO-000185
STIG-LEGACY	SV-78257
STIG-LEGACY	V-63767
SWIFT-CSCV1	2.3
VULN-ID	V-220935

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220936r971535_rule
STIG-ID	WN10-SO-000190
STIG-LEGACY	SV-78285
STIG-LEGACY	V-63795
VULN-ID	V-220936

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220938r991589_rule
STIG-ID	WN10-SO-000205
STIG-LEGACY	SV-78291
STIG-LEGACY	V-63801
SWIFT-CSCV1	2.3
VULN-ID	V-220938

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220940r991589_rule
STIG-ID	WN10-SO-000215
STIG-LEGACY	SV-78295
STIG-LEGACY	V-63805
SWIFT-CSCV1	2.3
VULN-ID	V-220940

Assets

10.0.0.103

```
536870912
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220941r991589_rule
STIG-ID	WN10-SO-000220
STIG-LEGACY	SV-78297
STIG-LEGACY	V-63807
SWIFT-CSCV1	2.3
VULN-ID	V-220941

Assets

10.0.0.103

```
536870912
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220942r959006_rule
STIG-ID	WN10-SO-000230
STIG-LEGACY	SV-78301
STIG-LEGACY	V-63811
VULN-ID	V-220942

Assets

10.0.0.103

0

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-220944r1051035_rule
STIG-ID	WN10-SO-000245
STIG-LEGACY	SV-78307
STIG-LEGACY	V-63817
VULN-ID	V-220944

Assets

10.0.0.103

```
NULL
```

WN10-SO-000250 - User Account Control must, at minimum, 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_10_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	MS_Windows_10_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-220945r958518_rule
STIG-ID	WN10-SO-000250
STIG-LEGACY	SV-78309
STIG-LEGACY	V-63819
VULN-ID	V-220945

Assets

10.0.0.103

5

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-220947r1051036_rule
STIG-ID	WN10-SO-000255
STIG-LEGACY	SV-78311
STIG-LEGACY	V-63821
VULN-ID	V-220947

Assets

10.0.0.103

3

WN10-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 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_10_V3R4_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	MS_Windows_10_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-220952r1051038_rule
STIG-ID	WN10-SO-000280
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-220952

Assets

10.0.0.103

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - Password last set date for Admin account.:
 Remote value: 'PASS: Password age within recommended limits'
 Policy value: 'PASS: Password age within recommended limits'


-------------------------
FAILED - LAPS password age configured.:
 Remote value: NULL
 Policy value: [0..60]


-------------------------
FAILED - LAPS password length configured.:
 Remote value: NULL
 Policy value: [14..4294967295]


-------------------------
FAILED - LAPS password complexity configured.:
 Remote value: NULL
 Policy value: 4


-------------------------
FAILED - LAPS name of administrator account enabled.:
 Remote value: 'HKLM\Software\Microsoft\Windows\CurrentVersion\Policies
\LAPS_registry_does_not_exist'
 Policy value: 'HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\LAPS'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220954r958478_rule
STIG-ID	WN10-UC-000015
STIG-LEGACY	SV-78329
STIG-LEGACY	V-63839

SWIFT-CSCV1	2.3
VULN-ID	V-220954

Assets

10.0.0.103

```
Non-compliant items:
  HKU\S-1-5-21-3886575422-42670501-2848359638-500\Software\Policies\Microsoft\Windows
\CurrentVersion\PushNotifications -
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220957r958472_rule
STIG-ID	WN10-UR-000010
STIG-LEGACY	SV-78335
STIG-LEGACY	V-63845
TBA-FIISB	31.1
VULN-ID	V-220957

Assets

10.0.0.103

```
'backup operators' && 'users' && 'administrators' && 'everyone'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220959r958472_rule
STIG-ID	WN10-UR-000025
STIG-LEGACY	SV-78341
STIG-LEGACY	V-63851
TBA-FIISB	31.1
VULN-ID	V-220959

Assets

10.0.0.103

```
'backup operators' && 'users' && 'administrators' && 'guest'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220960r958726_rule
STIG-ID	WN10-UR-000030
STIG-LEGACY	SV-78343
STIG-LEGACY	V-63853
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220960

Assets

10.0.0.103

```
'backup operators' && 'administrators'
```

WN10-UR-000035 - The Change the system time user right must only be assigned to Administrators and Local Service and NT SERVICE\autotimesvc.

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.
The NT SERVICE\autotimesvc is added in v1909 cumulative update.

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 NT SERVICE\autotimesvc is added in v1909 cumulative update.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220961r958726_rule
STIG-ID	WN10-UR-000035
STIG-LEGACY	SV-78345
STIG-LEGACY	V-63855
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220961

Assets

10.0.0.103

```
'administrators' && 'local service'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220968r958472_rule
STIG-ID	WN10-UR-000070
STIG-LEGACY	SV-78361
STIG-LEGACY	V-63871
TBA-FIISB	31.1
VULN-ID	V-220968

Assets

10.0.0.103

```
'guest'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220971r958472_rule
STIG-ID	WN10-UR-000085
STIG-LEGACY	SV-78367
STIG-LEGACY	V-63877
TBA-FIISB	31.1
VULN-ID	V-220971

Assets

10.0.0.103

```
'guest'
```

WN10-UR-000090 - The Deny log on through Remote Desktop Services user right on Windows 10 workstations must at a minimum 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_10_V3R4_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	MS_Windows_10_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-220972r958472_rule
STIG-ID	WN10-UR-000090
STIG-LEGACY	SV-78369
STIG-LEGACY	V-63879
SWIFT-CSCV1	2.6
TBA-FIISB	31.1
VULN-ID	V-220972

Assets

10.0.0.103

```
One of the following must pass to satisfy this requirement:

-------------------------
FAILED - Everyone:
 Remote value: NULL
 Policy value: 'Everyone'


-------------------------
FAILED - Guests:
 Remote value: NULL
 Policy value: 'Guests'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220982r958726_rule
STIG-ID	WN10-UR-000160
STIG-LEGACY	SV-78429
STIG-LEGACY	V-63939
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220982

Assets

10.0.0.103

```
'backup operators' && 'administrators'
```

Audits SKIPPED

Audits PASSED

DISA_Microsoft_Windows_10_STIG_v3r4.audit from DISA Microsoft Windows 10 STIG v3r4

Info

Solution

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_STIG.zip

Assets

10.0.0.103

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - Windows 10 build installed:
 Remote value: '19045'
 Policy value: '(1900[0-9]|190[1-9][0-9]|1[0-9][0-9][0-9]{2})'


-------------------------
PASSED - Windows 10 is installed:
 Remote value: 'Windows 10 Pro'
 Policy value: '^[Ww][Ii][Nn][Dd][Oo][Ww][Ss] 10.+$'
```

WN10-00-000005 - Domain-joined systems must use Windows 10 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. A number of system requirements must be met for Credential Guard to be configured and enabled properly. Virtualization-based security and Credential Guard are only available with Windows 10 Enterprise 64-bit version.

Solution

Use Windows 10 Enterprise 64-bit version for domain-joined systems.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220697r991589_rule
STIG-ID	WN10-00-000005
STIG-LEGACY	SV-77809
STIG-LEGACY	V-63319
SWIFT-CSCV1	2.3
VULN-ID	V-220697

Assets

10.0.0.103

PASSED

WN10-00-000015 - Windows 10 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 10, 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_10_V3R4_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	MS_Windows_10_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-220699r991589_rule
STIG-ID	WN10-00-000015
STIG-LEGACY	SV-91779
STIG-LEGACY	V-77083
SWIFT-CSCV1	2.3
VULN-ID	V-220699

Assets

10.0.0.103

```
'path                    \Windows\system32\winload.efi'
```

WN10-00-000020 - Secure Boot must be enabled on Windows 10 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 10, 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_10_V3R4_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	MS_Windows_10_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-220700r991589_rule
STIG-ID	WN10-00-000020
STIG-LEGACY	SV-91781
STIG-LEGACY	V-77085
SWIFT-CSCV1	2.3
VULN-ID	V-220700

Assets

10.0.0.103

```
'True'
```

WN10-00-000031 - Windows 10 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_10_V3R4_STIG.zip

References

800-171	3.13.16
800-171R3	03.13.08
800-53	SC-28
800-53	SC-28(1)
800-53R5	SC-28
800-53R5	SC-28(1)
CAT	I
CCI	CCI-001199
CCI	CCI-002475
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	MS_Windows_10_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.
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-220703r958552_rule
STIG-ID	WN10-00-000031
STIG-LEGACY	SV-104689
STIG-LEGACY	V-94859
TBA-FIISB	28.1
VULN-ID	V-220703

Assets

10.0.0.103

```
One of the following must pass to satisfy this requirement:

-------------------------
PASSED - UseTPMPin:
 Remote value: 1
 Policy value: 1 || 2


-------------------------
PASSED - UseTPMKeyPin:
 Remote value: 1
 Policy value: 1 || 2
```

WN10-00-000040 - Windows 10 systems must be maintained at a supported servicing level.

Info

Windows 10 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 semiannual 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 Version 22H2 (OS Build 19045.x)' or greater.
It is recommended systems be upgraded to the most recently released version.
Special-purpose systems using the LTSC\B may be at the following versions:
v1507 (Build 10240) v1607 (Build 14393) v1809 (Build 17763) v21H2 (Build 19044)

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220706r1050597_rule
STIG-ID	WN10-00-000040
STIG-LEGACY	SV-77839
STIG-LEGACY	V-63349
SWIFT-CSCV1	2.3

VULN-ID	V-220706

Assets

10.0.0.103

```
'19045'
```

WN10-00-000045 - The Windows 10 system must use an anti-virus 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

If no antivirus software is on the system and in use, install Windows Defender or a third-party antivirus solution.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220707r1016358_rule
STIG-ID	WN10-00-000045
STIG-LEGACY	SV-77841
STIG-LEGACY	V-63351
SWIFT-CSCV1	2.3
VULN-ID	V-220707

Assets

10.0.0.103

```
One of the following must pass to satisfy this requirement:

-------------------------
PASSED - Microsoft Defender Antivirus is installed:
```

```
 Remote value: 'Status DisplayName
 ------ -----------
Running Microsoft Defender Core Service
Running Windows Defender Firewall
Stopped Windows Defender Advanced Threat Protection Service
Running Microsoft Defender Antivirus Network Inspection Service
Running Microsoft Defender Antivirus Service
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$'


-------------------------
FAILED - check for trellix:
 Remote value: 'FAIL - Trellix Antivirus not found'
 Policy value: '^PASS$'
```

WN10-00-000050 - 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_10_V3R4_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	MS_Windows_10_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-220708r958472_rule
STIG-ID	WN10-00-000050
STIG-LEGACY	SV-77843
STIG-LEGACY	V-63353
TBA-FIISB	31.1
VULN-ID	V-220708

Assets

10.0.0.103

```
'None'
```

WN10-00-000075 - 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_10_V3R4_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	MS_Windows_10_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-220713r991589_rule
STIG-ID	WN10-00-000075
STIG-LEGACY	SV-77853
STIG-LEGACY	V-63363
SWIFT-CSCV1	2.3
VULN-ID	V-220713

Assets

10.0.0.103

```
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.'
```

WN10-00-000080 - Only authorized user accounts must be allowed to create or run virtual machines on Windows 10 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 10; 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_10_V3R4_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	MS_Windows_10_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-220714r958478_rule
STIG-ID	WN10-00-000080

STIG-LEGACY	SV-77855
STIG-LEGACY	V-63365
SWIFT-CSCV1	2.3
VULN-ID	V-220714

Assets

10.0.0.103

```
'No entries found'
```

WN10-00-000085 - 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_10_V3R4_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	MS_Windows_10_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-220715r991589_rule
STIG-ID	WN10-00-000085
STIG-LEGACY	SV-77857
STIG-LEGACY	V-63367
SWIFT-CSCV1	2.3
VULN-ID	V-220715

Assets

10.0.0.103

PASSED

WN10-00-000095 - 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' (WN10-SO-000160).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220717r1081048_rule
STIG-ID	WN10-00-000095
STIG-LEGACY	SV-77863
STIG-LEGACY	V-63373
TBA-FIISB	31.1
VULN-ID	V-220717

Assets

10.0.0.103

PASSED

WN10-00-000100 - Internet Information System (IIS) or its subcomponents must not be installed on a workstation.

Info

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_10_V3R4_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	MS_Windows_10_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-220718r958478_rule
STIG-ID	WN10-00-000100
STIG-LEGACY	SV-77867
STIG-LEGACY	V-63377

SWIFT-CSCV1	2.3
VULN-ID	V-220718

Assets

10.0.0.103

```
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$'
```

WN10-00-000105 - Simple Network Management Protocol (SNMP) must not be installed on the system.

Info

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_10_V3R4_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	MS_Windows_10_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-220719r958480_rule
STIG-ID	WN10-00-000105
STIG-LEGACY	SV-77871
STIG-LEGACY	V-63381
SWIFT-CSCV1	2.3
VULN-ID	V-220719

Assets

10.0.0.103

```
'%windir%\System32\snmp.exe_file_does_not_exist'
```

WN10-00-000107 - Copilot in Windows must be disabled for Windows 10.

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

Configure the policy value for User Configuration >> Administrative Templates >> Windows Components >> Windows Copilot >> 'Turn off Windows Copilot' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-268315r1016354_rule

STIG-ID	WN10-00-000107
SWIFT-CSCV1	2.3
VULN-ID	V-268315

Assets

10.0.0.103

```
Compliant items:
  HKU\S-1-5-21-3886575422-42670501-2848359638-500\Software\Policies\Microsoft\Windows
\WindowsCopilot - 1
```

WN10-00-000110 - Simple TCP/IP Services must not be installed on the system.

Info

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_10_V3R4_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	MS_Windows_10_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-220720r958478_rule
STIG-ID	WN10-00-000110
STIG-LEGACY	SV-77873
STIG-LEGACY	V-63383

SWIFT-CSCV1	2.3
VULN-ID	V-220720

Assets

10.0.0.103

```
'HKLM\System\CurrentControlSet\Services\Simptcp_registry_does_not_exist'
```

WN10-00-000115 - The Telnet Client must not be installed on the system.

Info

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_10_V3R4_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	MS_Windows_10_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-220721r958480_rule

STIG-ID	WN10-00-000115
STIG-LEGACY	SV-77875
STIG-LEGACY	V-63385
SWIFT-CSCV1	2.3
VULN-ID	V-220721

Assets

10.0.0.103

```
'%windir%\System32\telnet.exe_file_does_not_exist'
```

WN10-00-000120 - The TFTP Client must not be installed on the system.

Info

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_10_V3R4_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	MS_Windows_10_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-220722r958480_rule

STIG-ID	WN10-00-000120
STIG-LEGACY	SV-77879
STIG-LEGACY	V-63389
SWIFT-CSCV1	2.3
VULN-ID	V-220722

Assets

10.0.0.103

```
'%windir%\System32\TFTP.exe_file_does_not_exist'
```

WN10-00-000150 - 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_10_V3R4_STIG.zip

References

800-53	SI-16
800-53R5	SI-16
CAT	I
CCI	CCI-002824
CSF2.0	PR.DS-10
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
RULE-ID	SV-220727r958928_rule
STIG-ID	WN10-00-000150
STIG-LEGACY	SV-83445
STIG-LEGACY	V-68849
VULN-ID	V-220727

Assets

10.0.0.103

PASSED

WN10-00-000160 - 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_10_V3R4_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	MS_Windows_10_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-220729r958478_rule
STIG-ID	WN10-00-000160
STIG-LEGACY	SV-85261
STIG-LEGACY	V-70639
SWIFT-CSCV1	2.3
VULN-ID	V-220729

Assets

10.0.0.103

```
'State : Disabled'
```

WN10-00-000165 - 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_10_V3R4_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	MS_Windows_10_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-220730r958478_rule

STIG-ID	WN10-00-000165
STIG-LEGACY	SV-89397
STIG-LEGACY	V-74723
SWIFT-CSCV1	2.3
VULN-ID	V-220730

Assets

10.0.0.103

PASSED

WN10-00-000170 - 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_10_V3R4_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	MS_Windows_10_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-220731r958478_rule
STIG-ID	WN10-00-000170
STIG-LEGACY	SV-89399
STIG-LEGACY	V-74725
SWIFT-CSCV1	2.3
VULN-ID	V-220731

Assets

10.0.0.103

PASSED

WN10-00-000210 - 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_10_V3R4_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	MS_Windows_10_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-220734r958478_rule
STIG-ID	WN10-00-000210
STIG-LEGACY	SV-87403
STIG-LEGACY	V-72765
SWIFT-CSCV1	2.3

VULN-ID V-220734

Assets

10.0.0.103

```
'No entries found'
```

WN10-00-000220 - 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_10_V3R4_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	MS_Windows_10_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-220735r958478_rule
STIG-ID	WN10-00-000220
STIG-LEGACY	SV-87405
STIG-LEGACY	V-72767

SWIFT-CSCV1	2.3
VULN-ID	V-220735

Assets

10.0.0.103

```
'No entries found'
```

WN10-00-000395 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-257593r991589_rule
STIG-ID	WN10-00-000395
SWIFT-CSCV1	2.3
VULN-ID	V-257593

Assets

10.0.0.103

PASSED

WN10-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_10_V3R4_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	MS_Windows_10_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-220743r1051020_rule
STIG-ID	WN10-AC-000025
STIG-LEGACY	SV-77909
STIG-LEGACY	V-63419
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-220743

Assets

10.0.0.103

42

WN10-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_10_V3R4_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	MS_Windows_10_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-220747r1051024_rule
STIG-ID	WN10-AC-000045

STIG-LEGACY	SV-77919
STIG-LEGACY	V-63429
SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-220747

Assets

10.0.0.103

```
'disabled'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.1
800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.01
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-2(4)
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-2(4)
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000018
CCI	CCI-000172
CCI	CCI-001403
CCI	CCI-001404
CCI	CCI-001405
CCI	CCI-002130
CCI	CCI-002234

CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-1
CSF	PR.AC-4
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.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.16

ISO-27001-2022	A.5.18
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-2(4)
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM9a
NIAV2	AM9b
NIAV2	AM9c
NIAV2	AM9d
NIAV2	AM9e
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2

QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-220750r958368_rule
STIG-ID	WN10-AU-000030
STIG-LEGACY	SV-77935
STIG-LEGACY	V-63445
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	36.2.3
TBA-FIISB	45.1.1
VULN-ID	V-220750

Assets

10.0.0.103

```
'success'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.1
800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.01
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-2(4)
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-2(4)
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000018
CCI	CCI-000172
CCI	CCI-001403
CCI	CCI-001404
CCI	CCI-001405
CCI	CCI-002130
CCI	CCI-002234

CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-1
CSF	PR.AC-4
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.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.16

ISO-27001-2022	A.5.18
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-2(4)
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM9a
NIAV2	AM9b
NIAV2	AM9c
NIAV2	AM9d
NIAV2	AM9e
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2

QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-220751r958368_rule
STIG-ID	WN10-AU-000035
STIG-LEGACY	SV-77937
STIG-LEGACY	V-63447
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	36.2.3
TBA-FIISB	45.1.1
VULN-ID	V-220751

Assets

10.0.0.103

```
'success, failure'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.1
800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.01
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-2(4)
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-2(4)
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000018
CCI	CCI-000172
CCI	CCI-001403
CCI	CCI-001404
CCI	CCI-001405
CCI	CCI-002130
CCI	CCI-002234

CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-1
CSF	PR.AC-4
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.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.16

ISO-27001-2022	A.5.18
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-2(4)
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM9a
NIAV2	AM9b
NIAV2	AM9c
NIAV2	AM9d
NIAV2	AM9e
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2

QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-220752r958368_rule
STIG-ID	WN10-AU-000040
STIG-LEGACY	SV-77939
STIG-LEGACY	V-63449
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	36.2.3
TBA-FIISB	45.1.1
VULN-ID	V-220752

Assets

10.0.0.103

```
'success, failure'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.12
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.12
800-171R3	03.03.03a.
800-53	AC-17(1)
800-53	AU-12c.
800-53R5	AC-17(1)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000067
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)
CN-L3	8.1.4.4(c)
CN-L3	8.1.10.6(i)
CSF	DE.CM-1
CSF	DE.CM-3

CSF	DE.CM-7
CSF	PR.AC-3
CSF	PR.PT-1
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.16
ISO/IEC-27001	A.6.2.2
ISO/IEC-27001	A.12.4.1
ITSG-33	AC-17(1)
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.4.4
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1

QCSC-V1	13.2
RULE-ID	SV-220757r958406_rule
STIG-ID	WN10-AU-000065
STIG-LEGACY	SV-77951
STIG-LEGACY	V-63459
SWIFT-CSCV1	2.6
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220757

Assets

10.0.0.103

```
'success'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.12
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.12
800-171R3	03.03.03a.
800-53	AC-17(1)
800-53	AU-12c.
800-53R5	AC-17(1)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000067
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)
CN-L3	8.1.4.4(c)
CN-L3	8.1.10.6(i)
CSF	DE.CM-1
CSF	DE.CM-3

CSF	DE.CM-7
CSF	PR.AC-3
CSF	PR.PT-1
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.16
ISO/IEC-27001	A.6.2.2
ISO/IEC-27001	A.12.4.1
ITSG-33	AC-17(1)
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.4.4
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1

QCSC-V1	13.2
RULE-ID	SV-220758r958406_rule
STIG-ID	WN10-AU-000070
STIG-LEGACY	SV-77953
STIG-LEGACY	V-63463
SWIFT-CSCV1	2.6
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220758

Assets

10.0.0.103

```
'success, failure'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.12
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.12
800-171R3	03.03.03a.
800-53	AC-17(1)
800-53	AU-12c.
800-53R5	AC-17(1)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000067
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)
CN-L3	8.1.4.4(c)
CN-L3	8.1.10.6(i)
CSF	DE.CM-1
CSF	DE.CM-3

CSF	DE.CM-7
CSF	PR.AC-3
CSF	PR.PT-1
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.16
ISO/IEC-27001	A.6.2.2
ISO/IEC-27001	A.12.4.1
ITSG-33	AC-17(1)
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.4.4
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1

QCSC-V1	13.2
RULE-ID	SV-220759r958406_rule
STIG-ID	WN10-AU-000075
STIG-LEGACY	SV-77957
STIG-LEGACY	V-63467
SWIFT-CSCV1	2.6
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220759

Assets

10.0.0.103

```
'success, failure'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220760r991578_rule
STIG-ID	WN10-AU-000080
STIG-LEGACY	SV-77959
STIG-LEGACY	V-63469
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220760

Assets

10.0.0.103

```
'success'
```

WN10-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 Audit Policy Change' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220767r991579_rule
STIG-ID	WN10-AU-000100
STIG-LEGACY	SV-77969
STIG-LEGACY	V-63479
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220767

Assets

10.0.0.103

```
'success'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-220768r958732_rule
STIG-ID	WN10-AU-000105
STIG-LEGACY	SV-77971
STIG-LEGACY	V-63481
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-220768

Assets

10.0.0.103

```
'success'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220773r991579_rule
STIG-ID	WN10-AU-000130
STIG-LEGACY	SV-77989
STIG-LEGACY	V-63499
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220773

Assets

10.0.0.103

```
'success, failure'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220774r991579_rule
STIG-ID	WN10-AU-000135
STIG-LEGACY	SV-77993
STIG-LEGACY	V-63503
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-220774

Assets

10.0.0.103

```
'success, failure'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)

CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1

NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-220775r958732_rule
STIG-ID	WN10-AU-000140
STIG-LEGACY	SV-77997
STIG-LEGACY	V-63507
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-220775

Assets

10.0.0.103

```
'success'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1

CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f

NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-220777r958732_rule
STIG-ID	WN10-AU-000155
STIG-LEGACY	SV-78005
STIG-LEGACY	V-63515
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-220777

Assets

10.0.0.103

```
'success, failure'
```

WN10-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_10_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1

CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f

NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-220778r958732_rule
STIG-ID	WN10-AU-000160
STIG-LEGACY	SV-78007
STIG-LEGACY	V-63517
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-220778

Assets

10.0.0.103

```
'success, failure'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220779r958752_rule
STIG-ID	WN10-AU-000500
STIG-LEGACY	SV-78009
STIG-LEGACY	V-63519
VULN-ID	V-220779

Assets

10.0.0.103

32768

WN10-AU-000515 - Windows 10 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_10_V3R4_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
CCI	CCI-000163
CCI	CCI-000164
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	MS_Windows_10_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-220782r958434_rule
STIG-ID	WN10-AU-000515
STIG-LEGACY	SV-78023
STIG-LEGACY	V-63533
VULN-ID	V-220782

Assets

10.0.0.103

```
'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'
```

WN10-AU-000520 - Windows 10 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_10_V3R4_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
CCI	CCI-000163
CCI	CCI-000164
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	MS_Windows_10_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-220783r958434_rule
STIG-ID	WN10-AU-000520
STIG-LEGACY	SV-78027
STIG-LEGACY	V-63537
VULN-ID	V-220783

Assets

10.0.0.103

```
'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'
```

WN10-AU-000525 - Windows 10 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_10_V3R4_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
CCI	CCI-000163
CCI	CCI-000164
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	MS_Windows_10_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-220784r958434_rule
STIG-ID	WN10-AU-000525
STIG-LEGACY	SV-78031
STIG-LEGACY	V-63541
VULN-ID	V-220784

Assets

10.0.0.103

```
'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'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220794r958478_rule
STIG-ID	WN10-CC-000010
STIG-LEGACY	SV-78039
STIG-LEGACY	V-63549

SWIFT-CSCV1	2.3
VULN-ID	V-220794

Assets

10.0.0.103

1

WN10-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_10_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	MS_Windows_10_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-220799r958518_rule
STIG-ID	WN10-CC-000037
STIG-LEGACY	SV-78087
STIG-LEGACY	V-63597
VULN-ID	V-220799

Assets

10.0.0.103

PASSED

WN10-CC-000052 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220805r971535_rule
STIG-ID	WN10-CC-000052
STIG-LEGACY	SV-89087
STIG-LEGACY	V-74413
VULN-ID	V-220805

Assets

10.0.0.103

```
'NistP384' && 'NistP256'
```

WN10-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 must 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_10_V3R4_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	MS_Windows_10_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-220806r991589_rule
STIG-ID	WN10-CC-000055
STIG-LEGACY	SV-78071
STIG-LEGACY	V-63581
SWIFT-CSCV1	2.3

VULN-ID	V-220806

Assets

10.0.0.103

NULL

WN10-CC-000063 - Windows 10 systems must use either Group Policy or an approved Mobile Device Management (MDM) product to enforce STIG compliance.

Info

Without Windows 10 systems being managed, devices could be rogue and become targets of an attacker.

Solution

Configure the Windows 10 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_10_V3R4_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	MS_Windows_10_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-268319r1081055_rule
STIG-ID	WN10-CC-000063
SWIFT-CSCV1	2.3
VULN-ID	V-268319

Assets

10.0.0.103

PASSED

WN10-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'.
v1507 LTSB does not include this group policy setting. It may be configured through other means such as using group policy from a later version of Windows 10 or a registry update.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220808r991589_rule
STIG-ID	WN10-CC-000065
STIG-LEGACY	SV-78081
STIG-LEGACY	V-63591
SWIFT-CSCV1	2.3
VULN-ID	V-220808

Assets

10.0.0.103

PASSED

WN10-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_10_V3R4_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	MS_Windows_10_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-220809r958422_rule
STIG-ID	WN10-CC-000066
STIG-LEGACY	SV-83409
STIG-LEGACY	V-68817
SWIFT-CSCV1	6.4
VULN-ID	V-220809

Assets

10.0.0.103

1

WN10-CC-000075 - Credential Guard must be running on Windows 10 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 VDIs 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 Not Applicable.
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:'.
v1507 LTSB does not include selection options; select 'Enable Credential Guard'.
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_10_V3R4_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	MS_Windows_10_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-220812r991589_rule
STIG-ID	WN10-CC-000075

STIG-LEGACY	SV-78089
STIG-LEGACY	V-63599
SWIFT-CSCV1	2.3
VULN-ID	V-220812

Assets

10.0.0.103

PASSED

WN10-CC-000080 - Virtualization-based protection of code integrity must be enabled.

Info

Virtualization-based protection of code integrity enforces kernel mode memory protections and protects 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 VDIs 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_10_V3R4_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	MS_Windows_10_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-252903r991589_rule
STIG-ID	WN10-CC-000080
SWIFT-CSCV1	2.3
VULN-ID	V-252903

Assets

10.0.0.103

PASSED

WN10-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_10_V3R4_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	MS_Windows_10_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-220817r958478_rule
STIG-ID	WN10-CC-000110
STIG-LEGACY	SV-78113

STIG-LEGACY	V-63623
SWIFT-CSCV1	2.3
VULN-ID	V-220817

Assets

10.0.0.103

1

WN10-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 or nondomain-joined systems, this is NA.
The default behavior for 'Support device authentication using certificate' is 'Automatic'.
If this needs to be corrected, configure 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_10_V3R4_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	MS_Windows_10_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-220818r991589_rule
STIG-ID	WN10-CC-000115
STIG-LEGACY	SV-78117
STIG-LEGACY	V-63627
SWIFT-CSCV1	2.3
VULN-ID	V-220818

Assets

10.0.0.103

PASSED

WN10-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 or nondomain-joined 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_10_V3R4_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	MS_Windows_10_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-220820r958478_rule
STIG-ID	WN10-CC-000130
STIG-LEGACY	SV-78123
STIG-LEGACY	V-63633

SWIFT-CSCV1	2.3
VULN-ID	V-220820

Assets

10.0.0.103

PASSED

WN10-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_10_V3R4_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	MS_Windows_10_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-220826r958478_rule
STIG-ID	WN10-CC-000175
STIG-LEGACY	SV-78153

STIG-LEGACY	V-63663
SWIFT-CSCV1	2.3
VULN-ID	V-220826

Assets

10.0.0.103

1

WN10-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_10_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	MS_Windows_10_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-220832r958518_rule
STIG-ID	WN10-CC-000200
STIG-LEGACY	SV-78169
STIG-LEGACY	V-63679
VULN-ID	V-220832

Assets

10.0.0.103

0

WN10-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. This requires the configuration of an additional setting available with v1709 and later of Windows 10.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Data Collection and Preview Builds >> 'Allow Telemetry' to 'Enabled' with '0 - Security [Enterprise Only]' or '1 - Basic' selected in 'Options:'.
If an organization is using v1709 or later of Windows 10, this may be configured to '2 - Enhanced' to support Windows Analytics. V-220833 must also be configured to limit the Enhanced diagnostic data to the minimum required by Windows Analytics.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220834r991589_rule
STIG-ID	WN10-CC-000205
STIG-LEGACY	SV-78173
STIG-LEGACY	V-63683

SWIFT-CSCV1	2.3
VULN-ID	V-220834

Assets

10.0.0.103

0

WN10-CC-000206 - Windows Update must not obtain updates from other PCs on the internet.

Info

Windows 10 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)
v1507 (LTSB) does not include this group policy setting locally. For domain-joined systems, configure through domain group policy as 'HTTP only (0)' or 'Lan (1)'.
For standalone or nondomain-joined systems, configure using Settings >> Update & Security >> Windows Update >> Advanced Options >> 'Choose how updates are delivered' with either 'Off' or 'PCs on my local network' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220835r991589_rule
STIG-ID	WN10-CC-000206
STIG-LEGACY	SV-80171
STIG-LEGACY	V-65681
SWIFT-CSCV1	2.3

VULN-ID V-220835

Assets

10.0.0.103

```
Compliant items:
  HKU\S-1-5-20\SOFTWARE\Microsoft\Windows\CurrentVersion\DeliveryOptimization\Config - 1
```

WN10-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.
If this needs to be corrected, 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_10_V3R4_STIG.zip

References

800-53	SI-16
800-53R5	SI-16
CAT	II
CCI	CCI-002824
CSF2.0	PR.DS-10
DISA_BENCHMARK	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
RULE-ID	SV-220837r958928_rule
STIG-ID	WN10-CC-000215
STIG-LEGACY	SV-78179
STIG-LEGACY	V-63689
VULN-ID	V-220837

Assets

10.0.0.103

NULL

WN10-CC-000220 - Turning off 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.
If this needs to be corrected, 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_10_V3R4_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	MS_Windows_10_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-220838r958902_rule
STIG-ID	WN10-CC-000220
STIG-LEGACY	SV-78181
STIG-LEGACY	V-63691
VULN-ID	V-220838

Assets

10.0.0.103

NULL

WN10-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.
If this needs to be corrected, 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_10_V3R4_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	MS_Windows_10_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-220839r991589_rule
STIG-ID	WN10-CC-000225
STIG-LEGACY	SV-78185
STIG-LEGACY	V-63695
SWIFT-CSCV1	2.3
VULN-ID	V-220839

Assets

10.0.0.103

NULL

WN10-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.
If this needs to be corrected, 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_10_V3R4_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	MS_Windows_10_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-220854r958478_rule
STIG-ID	WN10-CC-000300
STIG-LEGACY	SV-78237
STIG-LEGACY	V-63747

SWIFT-CSCV1	2.3
VULN-ID	V-220854

Assets

10.0.0.103

NULL

WN10-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_10_V3R4_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	MS_Windows_10_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-220855r958478_rule
STIG-ID	WN10-CC-000305
STIG-LEGACY	SV-78241
STIG-LEGACY	V-63751
SWIFT-CSCV1	2.3

VULN-ID	V-220855

Assets

10.0.0.103

0

WN10-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_10_V3R4_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	MS_Windows_10_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-220856r1051031_rule
STIG-ID	WN10-CC-000310
STIG-LEGACY	SV-77811
STIG-LEGACY	V-63321
SWIFT-CSCV1	5.1
VULN-ID	V-220856

Assets

10.0.0.103

0

WN10-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.
If this needs to be corrected, 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_10_V3R4_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	MS_Windows_10_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-220858r991589_rule
STIG-ID	WN10-CC-000320
STIG-LEGACY	SV-77819
STIG-LEGACY	V-63329
SWIFT-CSCV1	2.3
VULN-ID	V-220858

Assets

10.0.0.103

```
NULL
```

WN10-CC-000326 - PowerShell script block logging must be enabled on Windows 10.

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_10_V3R4_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	MS_Windows_10_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-220860r958422_rule
STIG-ID	WN10-CC-000326
STIG-LEGACY	SV-83411
STIG-LEGACY	V-68819
SWIFT-CSCV1	6.4
VULN-ID	V-220860

Assets

10.0.0.103

1

WN10-CC-000370 - The convenience PIN for Windows 10 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.
If this needs to be corrected 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_10_V3R4_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	MS_Windows_10_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-220870r958478_rule
STIG-ID	WN10-CC-000370
STIG-LEGACY	SV-108663
STIG-LEGACY	V-99559

SWIFT-CSCV1	2.3
VULN-ID	V-220870

Assets

10.0.0.103

0

WN10-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 10 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_10_V3R4_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	MS_Windows_10_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-220907r958726_rule
STIG-ID	WN10-RG-000005
STIG-LEGACY	SV-78083
STIG-LEGACY	V-63593
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220907

Assets

10.0.0.103

```
 All of the following must pass to satisfy this requirement:

-------------------------
PASSED - HKEY_LOCAL_MACHINE\SECURITY:
 Remote value:

  administrators:
  + Apply To: 'this key and subkeys'
```

```
   |- Inheritance: 'not inherited'
   |- Allow: 'read control' | 'write dac'

  system:
  + Apply To: 'this key and subkeys'
   |- Inheritance: 'not inherited'
   |- Allow: 'create link' | 'create subkey' | 'delete' | 'enumerate subkeys' | 'full control' |
 'notify' | 'query value' | 'read control' | 'set value' | 'write dac' | 'write owner'


 Policy value:

 administrators:
  + Apply To: 'this key and subkeys'
  |- Inheritance: 'not inherited'
  |- Allow: 'read control' | 'write dac'

 system:
  + Apply To: 'this key and subkeys'
  |- Inheritance: 'not inherited'
  |- Allow: 'create link' | 'create subkey' | 'delete' | 'enumerate subkeys' | 'full control' |
 'notify' | 'query value' | 'read control' | 'set value' | 'write dac' | 'write owner'




-------------------------
PASSED - HKEY_LOCAL_MACHINE\SOFTWARE:
 Remote value:


 1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681:
  + Apply To: 'this key and subkeys'
   |- Inheritance: 'not inherited'
   |- Allow: 'enumerate subkeys' | 'notify' | 'query value' | 'read control'

  administrators:
  + Apply To: 'this key and subkeys'
   |- Inheritance: 'not inherited'
   |- Allow: 'create link' | 'create subkey' | 'delete' | 'enumerate subkeys' | 'full control' |
 'notify' | 'query value' | 'read control' | 'set value' | 'write [...]
```

WN10-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 should 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_10_V3R4_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	MS_Windows_10_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-220910r991589_rule
STIG-ID	WN10-SO-000015
STIG-LEGACY	SV-78107
STIG-LEGACY	V-63617
SWIFT-CSCV1	2.3
VULN-ID	V-220910

Assets

10.0.0.103

```
1
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220911r991589_rule
STIG-ID	WN10-SO-000020
STIG-LEGACY	SV-78109
STIG-LEGACY	V-63619
SWIFT-CSCV1	2.3
VULN-ID	V-220911

Assets

10.0.0.103

```
'user1lab'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220913r958442_rule
STIG-ID	WN10-SO-000030
STIG-LEGACY	SV-78125
STIG-LEGACY	V-63635
SWIFT-CSCV1	6.4
VULN-ID	V-220913

Assets

10.0.0.103

1

WN10-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_10_V3R4_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	MS_Windows_10_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-220914r958908_rule
STIG-ID	WN10-SO-000035

STIG-LEGACY	SV-78129
STIG-LEGACY	V-63639
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-220914

Assets

10.0.0.103

1

WN10-SO-000040 - Outgoing secure channel traffic must be encrypted when possible.

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_10_V3R4_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	MS_Windows_10_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-220915r958908_rule
STIG-ID	WN10-SO-000040

STIG-LEGACY	SV-78133
STIG-LEGACY	V-63643
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-220915

Assets

10.0.0.103

1

WN10-SO-000045 - Outgoing secure channel traffic must be signed when possible.

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_10_V3R4_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	MS_Windows_10_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-220916r958908_rule
STIG-ID	WN10-SO-000045

STIG-LEGACY	SV-78137
STIG-LEGACY	V-63647
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-220916

Assets

10.0.0.103

1

WN10-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 your 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_10_V3R4_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	MS_Windows_10_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-220917r991589_rule
STIG-ID	WN10-SO-000050
STIG-LEGACY	SV-78143
STIG-LEGACY	V-63653
SWIFT-CSCV1	2.3
VULN-ID	V-220917

Assets

10.0.0.103

```
0
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220918r991589_rule
STIG-ID	WN10-SO-000055
STIG-LEGACY	SV-78151
STIG-LEGACY	V-63661
SWIFT-CSCV1	2.3
VULN-ID	V-220918

Assets

10.0.0.103

```
30
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220919r958908_rule
STIG-ID	WN10-SO-000060

STIG-LEGACY	SV-78155
STIG-LEGACY	V-63665
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-220919

Assets

10.0.0.103

1

WN10-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_10_V3R4_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	MS_Windows_10_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-220923r991589_rule
STIG-ID	WN10-SO-000085
STIG-LEGACY	SV-78177
STIG-LEGACY	V-63687
SWIFT-CSCV1	2.3

VULN-ID	V-220923

Assets

10.0.0.103

PASSED

WN10-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_10_V3R4_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	MS_Windows_10_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-220926r987796_rule
STIG-ID	WN10-SO-000110

STIG-LEGACY	SV-78201
STIG-LEGACY	V-63711
SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-220926

Assets

10.0.0.103

```
0
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220928r991589_rule
STIG-ID	WN10-SO-000140
STIG-LEGACY	SV-78229
STIG-LEGACY	V-63739
SWIFT-CSCV1	2.3
VULN-ID	V-220928

Assets

10.0.0.103

```
'disabled'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220929r991589_rule
STIG-ID	WN10-SO-000145
STIG-LEGACY	SV-78235
STIG-LEGACY	V-63745
SWIFT-CSCV1	2.3
VULN-ID	V-220929

Assets

10.0.0.103

1

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-220930r958524_rule
STIG-ID	WN10-SO-000150
STIG-LEGACY	SV-78239
STIG-LEGACY	V-63749
VULN-ID	V-220930

Assets

10.0.0.103

1

WN10-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_10_V3R4_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	MS_Windows_10_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-220931r991589_rule
STIG-ID	WN10-SO-000160
STIG-LEGACY	SV-78245
STIG-LEGACY	V-63755
SWIFT-CSCV1	2.3
VULN-ID	V-220931

Assets

10.0.0.103

```
0
```

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-220932r958524_rule
STIG-ID	WN10-SO-000165
STIG-LEGACY	SV-78249
STIG-LEGACY	V-63759
VULN-ID	V-220932

Assets

10.0.0.103

1

WN10-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_10_V3R4_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	MS_Windows_10_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-220937r1051034_rule

STIG-ID	WN10-SO-000195
STIG-LEGACY	SV-78287
STIG-LEGACY	V-63797
SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-220937

Assets

10.0.0.103

1

WN10-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_10_V3R4_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	MS_Windows_10_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-220939r991589_rule
STIG-ID	WN10-SO-000210
STIG-LEGACY	SV-78293
STIG-LEGACY	V-63803
SWIFT-CSCV1	2.3
VULN-ID	V-220939

Assets

10.0.0.103

1

WN10-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_10_V3R4_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	MS_Windows_10_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-220943r991589_rule
STIG-ID	WN10-SO-000240
STIG-LEGACY	SV-78305
STIG-LEGACY	V-63815
SWIFT-CSCV1	2.3
VULN-ID	V-220943

Assets

10.0.0.103

```
1
```

WN10-SO-000251 - Windows 10 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 is suggested based on the organization's needs and capabilities.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220946r958484_rule
STIG-ID	WN10-SO-000251
STIG-LEGACY	SV-111577
STIG-LEGACY	V-102627
SWIFT-CSCV1	1.2
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-220946

Assets

10.0.0.103

PASSED

WN10-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_10_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	MS_Windows_10_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-220948r958518_rule
STIG-ID	WN10-SO-000260
STIG-LEGACY	SV-78315
STIG-LEGACY	V-63825
VULN-ID	V-220948

Assets

10.0.0.103

1

WN10-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_10_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	MS_Windows_10_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-220949r958518_rule
STIG-ID	WN10-SO-000265
STIG-LEGACY	SV-78317
STIG-LEGACY	V-63827
VULN-ID	V-220949

Assets

10.0.0.103

1

WN10-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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-220950r1051037_rule
STIG-ID	WN10-SO-000270
STIG-LEGACY	SV-78319
STIG-LEGACY	V-63829
VULN-ID	V-220950

Assets

10.0.0.103

1

WN10-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_10_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	MS_Windows_10_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-220951r958518_rule
STIG-ID	WN10-SO-000275
STIG-LEGACY	SV-78321
STIG-LEGACY	V-63831
VULN-ID	V-220951

Assets

10.0.0.103

1

WN10-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.
If this needs to be corrected, 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_10_V3R4_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	MS_Windows_10_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-220955r991589_rule
STIG-ID	WN10-UC-000020
STIG-LEGACY	SV-78331
STIG-LEGACY	V-63841
SWIFT-CSCV1	2.3
VULN-ID	V-220955

Assets

10.0.0.103

```
Compliant items:
```

```
  HKU\S-1-5-21-3886575422-42670501-2848359638-500\Software\Microsoft\Windows\Currentversion
\Policies\Attachments -
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220956r958726_rule
STIG-ID	WN10-UR-000005
STIG-LEGACY	SV-78333
STIG-LEGACY	V-63843
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220956

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220958r958726_rule
STIG-ID	WN10-UR-000015
STIG-LEGACY	SV-78337
STIG-LEGACY	V-63847
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220958

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220962r958726_rule
STIG-ID	WN10-UR-000040
STIG-LEGACY	SV-78347
STIG-LEGACY	V-63857
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220962

Assets

10.0.0.103

```
'administrators'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220963r958726_rule
STIG-ID	WN10-UR-000045
STIG-LEGACY	SV-78349
STIG-LEGACY	V-63859
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220963

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220964r958726_rule
STIG-ID	WN10-UR-000050
STIG-LEGACY	SV-78351
STIG-LEGACY	V-63861
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220964

Assets

10.0.0.103

```
'service' && 'administrators' && 'network service' && 'local service'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220965r958726_rule
STIG-ID	WN10-UR-000055
STIG-LEGACY	SV-78353
STIG-LEGACY	V-63863
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220965

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220966r958726_rule
STIG-ID	WN10-UR-000060
STIG-LEGACY	SV-78355
STIG-LEGACY	V-63865
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220966

Assets

10.0.0.103

```
'administrators'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220967r958726_rule
STIG-ID	WN10-UR-000065
STIG-LEGACY	SV-78359
STIG-LEGACY	V-63869
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220967

Assets

10.0.0.103

```
'administrators'
```

WN10-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 that could lead to the compromise of an entire domain.

Solution

This requirement is applicable to domain-joined systems. For standalone or nondomain-joined 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_10_V3R4_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	MS_Windows_10_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-220969r958472_rule
STIG-ID	WN10-UR-000075
STIG-LEGACY	SV-78363
STIG-LEGACY	V-63873
TBA-FIISB	31.1
VULN-ID	V-220969

Assets

10.0.0.103

PASSED

WN10-UR-000080 - The Deny log on as a service user right on Windows 10 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 or nondomain-joined 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_10_V3R4_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	MS_Windows_10_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-220970r958472_rule
STIG-ID	WN10-UR-000080
STIG-LEGACY	SV-78365
STIG-LEGACY	V-63875
TBA-FIISB	31.1
VULN-ID	V-220970

Assets

10.0.0.103

PASSED

WN10-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_10_V3R4_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	MS_Windows_10_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-220973r958726_rule
STIG-ID	WN10-UR-000095
STIG-LEGACY	SV-78371
STIG-LEGACY	V-63881
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220973

Assets

10.0.0.103

```
NULL
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220974r958726_rule
STIG-ID	WN10-UR-000100
STIG-LEGACY	SV-78373
STIG-LEGACY	V-63883
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220974

Assets

10.0.0.103

```
'administrators'
```

WN10-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 SERVICE

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_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	MS_Windows_10_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-220975r958726_rule
STIG-ID	WN10-UR-000110
STIG-LEGACY	SV-78379
STIG-LEGACY	V-63889
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220975

Assets

10.0.0.103

```
'service' && 'administrators' && 'network service' && 'local service'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220976r958726_rule
STIG-ID	WN10-UR-000120
STIG-LEGACY	SV-78407
STIG-LEGACY	V-63917
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220976

Assets

10.0.0.103

```
'administrators'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220977r958726_rule
STIG-ID	WN10-UR-000125
STIG-LEGACY	SV-78415
STIG-LEGACY	V-63925
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220977

Assets

10.0.0.103

```
NULL
```

WN10-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.

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_10_V3R4_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.
800-53	AU-12(3)
800-53R5	AU-9a.
800-53R5	AU-12b.
800-53R5	AU-12(3)
CAT	II
CCI	CCI-000162
CCI	CCI-000163
CCI	CCI-000164
CCI	CCI-000171
CCI	CCI-001914
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	MS_Windows_10_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-12
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-220978r958434_rule
STIG-ID	WN10-UR-000130
STIG-LEGACY	SV-78417
STIG-LEGACY	V-63927
SWIFT-CSCV1	6.4
VULN-ID	V-220978

Assets

10.0.0.103

```
'administrators'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220979r958726_rule
STIG-ID	WN10-UR-000140
STIG-LEGACY	SV-78421
STIG-LEGACY	V-63931
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220979

Assets

10.0.0.103

```
'administrators'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220980r958726_rule
STIG-ID	WN10-UR-000145
STIG-LEGACY	SV-78423
STIG-LEGACY	V-63933
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220980

Assets

10.0.0.103

```
'administrators'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220981r958726_rule
STIG-ID	WN10-UR-000150
STIG-LEGACY	SV-78425
STIG-LEGACY	V-63935
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220981

Assets

10.0.0.103

```
'administrators'
```

WN10-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_10_V3R4_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	MS_Windows_10_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-220983r958726_rule
STIG-ID	WN10-UR-000165
STIG-LEGACY	SV-78431
STIG-LEGACY	V-63941
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220983

Assets

10.0.0.103

```
'administrators'
```

Audits INFO,WARNING,ERROR

WN10-00-000010 - Windows 10 domain-joined systems must have a Trusted Platform Module (TPM) enabled and ready for use.

Info

Credential Guard uses virtualization-based security to protect information that could be used in credential theft attacks if compromised. A number of system requirements must be met 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.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

For standalone or nondomain-joined systems, this is NA.
Virtualization-based security, including Credential Guard, currently cannot be implemented in 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 have a Trusted Platform Module (TPM) that is configured for use. (Versions 2.0 or 1.2 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_10_V3R4_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	MS_Windows_10_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-220698r991589_rule
STIG-ID	WN10-00-000010
STIG-LEGACY	SV-77813

STIG-LEGACY	V-63323
SWIFT-CSCV1	2.3
VULN-ID	V-220698

Assets

10.0.0.103

WN10-00-000025 - Windows 10 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_10_V3R4_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	MS_Windows_10_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-220701r1000076_rule
STIG-ID	WN10-00-000025
STIG-LEGACY	SV-77833
STIG-LEGACY	V-63343
SWIFT-CSCV1	2.3

VULN-ID	V-220701

Assets

10.0.0.103

WN10-00-000030 - Windows 10 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 (WN10-00-000031 and WN10-00-000032).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V3R4_STIG.zip

References

800-171	3.13.16
800-171R3	03.13.08
800-53	SC-28
800-53	SC-28(1)
800-53R5	SC-28
800-53R5	SC-28(1)
CAT	I
CCI	CCI-001199
CCI	CCI-002475
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	MS_Windows_10_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.
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-220702r958552_rule
STIG-ID	WN10-00-000030
STIG-LEGACY	SV-77827
STIG-LEGACY	V-63337
TBA-FIISB	28.1
VULN-ID	V-220702

Assets

10.0.0.103

```
'VolumeType       : OperatingSystem
MountPoint       : C:
ProtectionStatus : Off

VolumeType       : Data
MountPoint       : D:
ProtectionStatus : Off


Some disks not encrypted.'
```

WN10-00-000035 - 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 not performed this check. Please review 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 10 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 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_10_V3R4_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	MS_Windows_10_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-220705r958808_rule
STIG-ID	WN10-00-000035
STIG-LEGACY	SV-77835
STIG-LEGACY	V-63345
SWIFT-CSCV1	2.3
TBA-FIISB	44.2.2
TBA-FIISB	49.2.3
VULN-ID	V-220705

Assets

10.0.0.103

WN10-00-000055 - 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 10 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_10_V3R4_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	MS_Windows_10_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-220709r991589_rule
STIG-ID	WN10-00-000055
STIG-LEGACY	SV-77845
STIG-LEGACY	V-63355
SWIFT-CSCV1	2.3
VULN-ID	V-220709

Assets

10.0.0.103

WN10-00-000060 - Non system-created file shares on a system must limit access to groups that require it.

Info

Shares which provide network access, should not typically 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_10_V3R4_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	MS_Windows_10_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-220710r958524_rule
STIG-ID	WN10-00-000060
STIG-LEGACY	SV-77847
STIG-LEGACY	V-63357
VULN-ID	V-220710

Assets

10.0.0.103

WN10-00-000065 - 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, disabled until needed.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Regularly 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_10_V3R4_STIG.zip

References

800-171	3.5.5
800-171	3.5.6
800-171R3	03.05.05
800-53	IA-4e.
800-53R5	AC-2(3)(a)
CAT	III
CCI	CCI-000795
CCI	CCI-003627
CN-L3	7.1.2.7(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
DISA_BENCHMARK	MS_Windows_10_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-4e.
PCI-DSSV3.2.1	8.1.4
PCI-DSSV4.0	8.2.6
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-220711r1051018_rule

STIG-ID	WN10-00-000065
STIG-LEGACY	SV-77849
STIG-LEGACY	V-63359
SWIFT-CSCV1	5
VULN-ID	V-220711

Assets

10.0.0.103

WN10-00-000070 - 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_10_V3R4_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	MS_Windows_10_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-220712r958726_rule
STIG-ID	WN10-00-000070
STIG-LEGACY	SV-77851
STIG-LEGACY	V-63361
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-220712

Assets

10.0.0.103

```
'Finding: levy-windows10\admin is a standard user account in the local Administrators group.
Finding: levy-windows10\Guest is a standard user account in the local Administrators group.
Finding: levy-windows10\user1lab is a standard user account in the local Administrators group.'
```

WN10-00-000130 - Software certificate installation files must be removed from Windows 10.

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_10_V3R4_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	MS_Windows_10_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-220723r991589_rule
STIG-ID	WN10-00-000130
STIG-LEGACY	SV-77883
STIG-LEGACY	V-63393
SWIFT-CSCV1	2.3
VULN-ID	V-220723

Assets

10.0.0.103

WN10-00-000135 - 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.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

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_10_V3R4_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	MS_Windows_10_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-220724r991589_rule
STIG-ID	WN10-00-000135
STIG-LEGACY	SV-77889
STIG-LEGACY	V-63399
SWIFT-CSCV1	2.3
VULN-ID	V-220724

Assets

10.0.0.103

WN10-00-000140 - Inbound exceptions to the firewall on Windows 10 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_10_V3R4_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	MS_Windows_10_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-220725r991589_rule
STIG-ID	WN10-00-000140
STIG-LEGACY	SV-77893
STIG-LEGACY	V-63403

SWIFT-CSCV1	2.3
VULN-ID	V-220725

Assets

10.0.0.103

```
 'DisplayName : WFD Driver-only (TCP-In)
Enabled     : True
Direction   : Inbound

DisplayName : WFD Driver-only (UDP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Delivery Optimization (TCP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Delivery Optimization (UDP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Connected Devices Platform (UDP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Connected Devices Platform (TCP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Connected Devices Platform - Wi-Fi Direct Transport (TCP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Destination Unreachable (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Packet Too Big (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Time Exceeded (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Parameter Problem (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Router Advertisement (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Router Solicitation (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Multicast Listener Query (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Multicast Listener Report (ICMPv6-In)
Enabled     : True
Direction   : Inbound
```

```
DisplayName : Core Networking - Multicast Listener Report v2 (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Multicast Listener Done (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core [...]
```

WN10-00-000190 - Orphaned security identifiers (SIDs) must be removed from user rights on Windows 10.

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_10_V3R4_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	MS_Windows_10_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-220733r991589_rule
STIG-ID	WN10-00-000190
STIG-LEGACY	SV-91201
STIG-LEGACY	V-76505
SWIFT-CSCV1	2.3
VULN-ID	V-220733

Assets

10.0.0.103

WN10-00-000230 - 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_10_V3R4_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	MS_Windows_10_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-220736r991589_rule
STIG-ID	WN10-00-000230
STIG-LEGACY	SV-87407
STIG-LEGACY	V-72769
SWIFT-CSCV1	2.3
VULN-ID	V-220736

Assets

10.0.0.103

```
Non-compliant items:
```

```
 HKU\S-1-5-21-3886575422-42670501-2848359638-500\Software\Microsoft\BluetoothAuthenticationAgent
- 2
```

WN10-00-000240 - 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 should 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 whitelisting 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 whitelisting 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_10_V3R4_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	MS_Windows_10_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-220737r991589_rule
STIG-ID	WN10-00-000240

STIG-LEGACY	SV-92835
STIG-LEGACY	V-78129
SWIFT-CSCV1	2.3
VULN-ID	V-220737

Assets

10.0.0.103

WN10-00-000250 - Windows 10 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 should 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_10_V3R4_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	MS_Windows_10_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-220738r958552_rule
STIG-ID	WN10-00-000250
STIG-LEGACY	SV-111557
STIG-LEGACY	V-102611
VULN-ID	V-220738

Assets

10.0.0.103