CIS Microsoft Windows Server 2016 STIG Benchmark

v4.0.0 - 08-22-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Microsoft Windows Server 2016 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 10 Benchmark Date: 15 Jan 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Windows Server 2019 and are looking to comply with the STIG guidance.

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **DC SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for Microsoft Windows Server 2019.

- **DC SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for Microsoft Windows Server 2019.

- **DC SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for Microsoft Windows Server 2019.

- **MS SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

- **MS SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

- **MS SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Microsoft Windows Server 2016.

Recommendations

1 STIG RULES

Microsoft Windows Server 2016

Secure Technical Implementation Guide (STIG)

Version: 2 Release: 10 Date: 15 Jan 2025

CLASSIFICATION unclassified

1.1 WN16-00-000010 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Users with Administrative privileges must have separate accounts for administrative duties and normal operational tasks.

```
GROUP ID:V-224819
RULE ID:SV-224819r991589
```

Rationale:

Using a privileged account to perform routine functions makes the computer vulnerable to malicious software inadvertently introduced during a session that has been granted full privileges.

Audit:

Verify each user with administrative privileges has been assigned a unique administrative account separate from their standard user account.

If users with administrative privileges do not have separate accounts for administrative functions and standard user functions, this is a finding.

Remediation:

Ensure each user with administrative privileges has a separate account for user duties and one for privileged duties.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.2 WN16-00-000030 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Passwords for the built-in Administrator account must be changed at least every 60 days.

```
GROUP ID:V-224820
RULE ID:SV-224820r1038967
```

Rationale:

The longer a password is in use, the greater the opportunity for someone to gain unauthorized knowledge of the password. The built-in Administrator account is not generally used and its password not may be changed as frequently as necessary. Changing the password for the built-in Administrator account on a regular basis will limit its exposure.

It is highly recommended to use Microsoft's Local Administrator Password Solution (LAPS). Domain-joined systems can configure this to occur more frequently. LAPS will change the password every "30" days by default. The AO still has the overall authority to use another equivalent capability to accomplish the check.

Audit:

Review the password last set date for the built-in Administrator account.

Domain controllers:

Open "PowerShell".

Enter

```
"Get-ADUser -Filter * -Properties SID, PasswordLastSet | Where SID -Like "*-
500" | Ft Name, SID, PasswordLastSet"
```

If the "PasswordLastSet" date is greater than "60" days old, this is a finding.

Member servers and standalone or nondomain-joined systems:

Open "Command Prompt".

Enter

```
'Net User [account name] | Find /i "Password Last Set"
```

where [account name] is the name of the built-in administrator account.

(The name of the built-in Administrator account must be changed to something other than "Administrator" per STIG requirements.)

If the "PasswordLastSet" date is greater than "60" days old, this is a finding.

Remediation:

Change the built-in Administrator account password at least every "60" days.

It is highly recommended to use Microsoft's LAPS, which may be used on domain-joined member servers to accomplish this. The AO still has the overall authority to use another equivalent capability to accomplish the check.

Additional Information:

CCI-000199

The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53 :: IA-5 (1) (d)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (d)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.3 WN16-00-000040 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Administrative accounts must not be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email.

```
GROUP ID:V-224821
RULE ID:SV-224821r991589
```

Rationale:

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 require 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.

Whitelisting can be used to enforce the policy to ensure compliance.

Audit:

Determine whether organization policy, at a minimum, prohibits administrative accounts from using applications that access the Internet, such as web browsers, or with potential Internet sources, such as email, except as necessary for local service administration.

If it does not, this is a finding.

The organization may use technical means such as whitelisting to prevent the use of browsers and mail applications to enforce this requirement.

Remediation:

Establish a policy, at minimum, to prohibit administrative accounts from using applications that access the Internet, such as web browsers, or with potential Internet sources, such as email. Ensure the policy is enforced.

The organization may use technical means such as whitelisting to prevent the use of browsers and mail applications to enforce this requirement.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.4 WN16-00-000050 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Members of the Backup Operators group must have separate accounts for backup duties and normal operational tasks.

```
GROUP ID:V-224822
RULE ID:SV-224822r991589
```

Rationale:

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.

Audit:

If no accounts are members of the Backup Operators group, this is NA.

Verify users with accounts in the Backup Operators group have a separate user account for backup functions and for performing normal user tasks.

If users with accounts in the Backup Operators group do not have separate accounts for backup functions and standard user functions, this is a finding.

Remediation:

Ensure each member of the Backup Operators group has separate accounts for backup functions and standard user functions.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.5 WN16-00-000060 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Manually managed application account passwords must be at least 14 characters in length.

```
GROUP ID:V-224823
RULE ID:SV-224823r1016376
```

Rationale:

Application/service account passwords must be of sufficient length to prevent being easily cracked. Application/service accounts that are manually managed must have passwords at least 14 characters in length.

Audit:

Determine if manually managed application/service accounts exist. If none exist, this is NA.

Verify the organization has a policy to ensure passwords for manually managed application/service accounts are at least 14 characters in length.

If such a policy does not exist or has not been implemented, this is a finding.

Remediation:

Establish a policy that requires application/service account passwords that are manually managed to be at least 14 characters in length. Ensure the policy is enforced.

Additional Information:

CCI-000205

The information system enforces minimum password length.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (i)

1.6 WN16-00-000070 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Manually managed application account passwords must be changed at least annually or when a system administrator with knowledge of the password leaves the organization.

```
GROUP ID:V-224824
RULE ID:SV-224824r991589
```

Rationale:

Setting application account passwords to expire may cause applications to stop functioning. However, not changing them on a regular basis exposes them to attack. If managed service accounts are used, this alleviates the need to manually change application account passwords.

Audit:

Determine if manually managed application/service accounts exist. If none exist, this is NA.

If passwords for manually managed application/service accounts are not changed at least annually or when an administrator with knowledge of the password leaves the organization, this is a finding.

Identify manually managed application/service accounts.

To determine the date a password was last changed:

Domain controllers:

Open "PowerShell".

Enter

```
"Get-AdUser -Identity [application account name] -Properties PasswordLastSet
| FT Name, PasswordLastSet"
```

where [application account name] is the name of the manually managed application/service account.

If the "PasswordLastSet" date is more than one year old, this is a finding.

Member servers and standalone or nondomain-joined systems:

Open "Command Prompt".

Enter

```
'Net User [application account name] | Find /i "Password Last Set"'
```

where [application account name] is the name of the manually managed application/service account.

If the "Password Last Set" date is more than one year old, this is a finding.

Remediation:

Change passwords for manually managed application/service accounts at least annually or when an administrator with knowledge of the password leaves the organization.

It is recommended that system-managed service accounts be used whenever possible.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.7 WN16-00-000080 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Shared user accounts must not be permitted on the system.

```
GROUP ID:V-224825
RULE ID:SV-224825r958482
```

Rationale:

Shared accounts (accounts where two or more people log on with the same user identification) do not provide adequate identification and authentication. There is no way to provide for nonrepudiation or individual accountability for system access and resource usage.

Audit:

Determine whether any shared accounts exist. If no shared accounts exist, this is NA.

Shared accounts, such as required by an application, may be approved by the organization. This must be documented with the ISSO. Documentation must include the reason for the account, who has access to the account, and how the risk of using the shared account is mitigated to include monitoring account activity.

If unapproved shared accounts exist, this is a finding.

Remediation:

Remove unapproved shared accounts from the system.

Document required shared accounts with the ISSO. Documentation must include the reason for the account, who has access to the account, and how the risk of using the shared account is mitigated to include monitoring account activity.

Additional Information:

CCI-000764

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53 :: IA-2
- NIST SP 800-53 Revision 4 :: IA-2
- NIST SP 800-53 Revision 5 :: IA-2
- NIST SP 800-53A :: IA-2.1

1.8 WN16-00-000090 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

```
GROUP ID:V-224826
RULE ID:SV-224826r958808
```

Rationale:

Using an allowlist provides a configuration management method to allow 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.

Audit:

Verify the operating system employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

If an application allowlisting program is not in use on the system, this is a finding.

Configuration of allowlisting applications will vary by the program.

AppLocker is an allowlisting application built into Windows Server. A deny-by-default implementation is initiated by enabling any AppLocker rules within a category, only allowing what is specified by defined rules.

If AppLocker is used, perform the following to view the configuration of AppLocker:

Open "PowerShell".

If the AppLocker PowerShell module has not been imported previously, execute the following first:

```
Import-Module AppLocker
```

Execute the following command, substituting [c:\temp\file.xml] with a location and file name appropriate for the system:

```
Get-AppLockerPolicy -Effective -XML > c:\temp\file.xml
```

This will produce an xml file with the effective settings that can be viewed in a browser or opened in a program such as Excel for review.

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

Remediation:

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 Server.

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

Additional Information:

CCI-001774

Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.

- NIST SP 800-53 Revision 4 :: CM-7 (5) (b)
- NIST SP 800-53 Revision 5 :: CM-7 (5) (b)

1.9 WN16-00-000100 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 domain-joined systems must have a Trusted Platform Module (TPM) enabled and ready for use.

```
GROUP ID:V-224827
RULE ID:SV-224827r991589
```

Rationale:

Credential Guard uses virtualization-based security to protect data 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.

Audit:

For standalone or nondomain-joined systems, this is NA.

Verify the system has a TPM and it is ready for use.

Run "tpm.msc".

Review the sections in the center pane.

"Status" must indicate it has been configured with a message such as "The TPM is ready for use" or "The TPM is on and ownership has been taken".

TPM Manufacturer Information - Specific Version = 2.0 or 1.2

If a TPM is not found or is not ready for use, this is a finding.

Remediation:

Ensure domain-joined systems have a 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.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.10 WN16-00-000110 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Systems must be maintained at a supported servicing level.

```
GROUP ID:V-224828
RULE ID:SV-224828r1059570
```

Rationale:

Systems at unsupported servicing levels will not receive security updates for new vulnerabilities, which leaves them subject to exploitation. Systems must be maintained at a servicing level supported by the vendor with new security updates.

Audit:

This STIG is sunset and no longer maintained.

Open "Command Prompt".

Enter

```
"winver.exe"
```

If the "About Windows" dialog box displays "Microsoft Windows Server Version 1607 (Build 14393.xxx)" and there is not documented extended support for Microsoft Windows Server 2016, this is a finding.

Remediation:

Upgrade the operating system to a supported version.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.11 WN16-00-000120 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

The Windows Server 2016 system must use an anti-virus program.

```
GROUP ID:V-224829
RULE ID:SV-224829r991589
```

Rationale:

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.

Audit:

Verify an anti-virus solution is installed on the system. The anti-virus solution may be bundled with an approved host-based security solution.

If there is no anti-virus solution installed on the system, this is a finding.

Verify if Windows Defender is in use or enabled:

Open "PowerShell".

Enter

```
"get-service | where {$_.DisplayName -Like "*Defender*"} | Select
Status,DisplayName”
```

Verify if third-party anti-virus is in use or enabled:

Open "PowerShell".

Enter

```
"get-service | where {$_.DisplayName -Like "*mcafee*"} | Select
Status,DisplayName”
```

Enter

```
"get-service | where {$_.DisplayName -Like "*symantec*"} | Select
Status,DisplayName”
```

Remediation:

If no anti-virus software is in use, install Windows Defender or third-party anti-virus.

Open "PowerShell".

Enter

```
"Install-WindowsFeature -Name Windows-Defender”
```

For third-party anti-virus, install per anti-virus instructions and disable Windows Defender.

Open "PowerShell".

Enter

```
“Uninstall-WindowsFeature -Name Windows-Defender”
```

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.12 WN16-00-000140 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Servers must have a host-based intrusion detection or prevention system.

```
GROUP ID:V-224830
RULE ID:SV-224830r991589
```

Rationale:

A properly configured Host-based Intrusion Detection System (HIDS) or Host-based Intrusion Prevention System (HIPS) provides another level of defense against unauthorized access to critical servers. With proper configuration and logging enabled, such a system can stop and/or alert for many attempts to gain unauthorized access to resources.

Audit:

Determine whether there is a HIDS or HIPS on each server.

If the HIPS component of ESS is installed and active on the host and the alerts of blocked activity are being logged and monitored, this meets the requirement.

A HIDS device is not required on a system that has the role as the Network Intrusion Device (NID). However, this exception needs to be documented with the ISSO.

If a HIDS is not installed on the system, this is a finding.

Remediation:

Install a HIDS or HIPS on each server.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.13 WN16-00-000150 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Local volumes must use a format that supports NTFS attributes.

```
GROUP ID:V-224831
RULE ID:SV-224831r958472
```

Rationale:

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 a file system that supports NTFS attributes.

Audit:

Open "Computer Management".

Select "Disk Management" under "Storage".

For each local volume, if the file system does not indicate "NTFS", this is a finding.

"ReFS" (resilient file system) is also acceptable and would not be a finding.

This does not apply to system partitions such the Recovery and EFI System Partition.

Remediation:

Format volumes to use NTFS or ReFS.

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3
- NIST SP 800-53A :: AC-3.1

1.14 WN16-00-000160 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Permissions for the system drive root directory (usually C:) must conform to minimum requirements.

```
GROUP ID:V-224832
RULE ID:SV-224832r958702
```

Rationale:

Changing the system's file and directory permissions allows the possibility of unauthorized and anonymous modification to the operating system and installed applications.

The default permissions are adequate when the Security Option "Network access: Let everyone permissions apply to anonymous users" is set to "Disabled" (WN16-SO-000290).

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124

Audit:

The default permissions are adequate when the Security Option "Network access: Let everyone permissions apply to anonymous users" is set to "Disabled" (WN16-SO-000290).

Review the permissions for the system drive's root directory (usually C:). Non-privileged groups such as Users or Authenticated Users must not have greater than "Read & execute" permissions except where noted as defaults. (Individual accounts must not be used to assign permissions.)

If permissions are not as restrictive as the default permissions listed below, this is a finding.

Viewing in File Explorer:

View the Properties of the system drive's root directory.

Select the "Security" tab, and the "Advanced" button.

Default permissions:

C:

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

- SYSTEM - Full control - This folder, subfolders, and files
- Administrators - Full control - This folder, subfolders, and files
- Users - Read & execute - This folder, subfolders, and files
- Users - Create folders/append data - This folder and subfolders
- Users - Create files/write data - Subfolders only
- CREATOR OWNER - Full Control - Subfolders and files only

Alternately, use icacls:
Open "Command Prompt (Admin)".
Enter

```
"icacls"
```

followed by the directory:

"icacls c:"

The following results should be displayed:

```
c:\
NT AUTHORITY\SYSTEM:(OI)(CI)(F)
BUILTIN\Administrators:(OI)(CI)(F)
BUILTIN\Users:(OI)(CI)(RX)
BUILTIN\Users:(CI)(AD)
BUILTIN\Users:(CI)(IO)(WD)
CREATOR OWNER:(OI)(CI)(IO)(F)
Successfully processed 1 files; Failed processing 0 files
```

Remediation:

Maintain the default permissions for the system drive's root directory and configure the Security Option "Network access: Let everyone permissions apply to anonymous users" to "Disabled" (WN16-SO-000290).

Default Permissions

C:

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

- SYSTEM - Full control - This folder, subfolders, and files
- Administrators - Full control - This folder, subfolders, and files
- Users - Read & execute - This folder, subfolders, and files
- Users - Create folders/append data - This folder and subfolders
- Users - Create files/write data - Subfolders only
- CREATOR OWNER - Full Control - Subfolders and files only

Additional Information:

CCI-002165

Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4 :: AC-3 (4)
- NIST SP 800-53 Revision 5 :: AC-3 (4)

1.15 WN16-00-000170 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Permissions for program file directories must conform to minimum requirements.

```
GROUP ID:V-224833
RULE ID:SV-224833r958702
```

Rationale:

Changing the system's file and directory permissions allows the possibility of unauthorized and anonymous modification to the operating system and installed applications.

The default permissions are adequate when the Security Option "Network access: Let everyone permissions apply to anonymous users" is set to "Disabled" (WN16-SO-000290).

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124

Audit:

The default permissions are adequate when the Security Option "Network access: Let everyone permissions apply to anonymous users" is set to "Disabled" (WN16-SO-000290).

Review the permissions for the program file directories (Program Files and Program Files [x86]). Non-privileged groups such as Users or Authenticated Users must not have greater than "Read & execute" permissions. (Individual accounts must not be used to assign permissions.)

If permissions are not as restrictive as the default permissions listed below, this is a finding.

Viewing in File Explorer:

For each folder, view the Properties.

Select the "Security" tab, and the "Advanced" button.

Default permissions:

\Program Files and \Program Files (x86)

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

- TrustedInstaller - Full control - This folder and subfolders
- SYSTEM - Modify - This folder only
- SYSTEM - Full control - Subfolders and files only
- Administrators - Modify - This folder only
- Administrators - Full control - Subfolders and files only
- Users - Read & execute - This folder, subfolders and files
- CREATOR OWNER - Full control - Subfolders and files only
- ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files
- ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

Alternately, use icacls:
Open a Command prompt (admin).
Enter

```
"icacls"
```

followed by the directory:

```
'icacls "c:\program files"'
'icacls "c:\program files (x86)"'
```

The following results should be displayed for each when entered:

```
c:\program files (c:\program files (x86))
NT SERVICE\TrustedInstaller:(F)
NT SERVICE\TrustedInstaller:(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(M)
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
BUILTIN\Administrators:(M)
BUILTIN\Administrators:(OI)(CI)(IO)(F)
BUILTIN\Users:(RX)
BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION
PACKAGES:(OI)(CI)(IO)(GR,GE)
Successfully processed 1 files; Failed processing 0 files
```

Remediation:

Maintain the default permissions for the program file directories and configure the Security Option "Network access: Let everyone permissions apply to anonymous users" to "Disabled" (WN16-SO-000290).

Default permissions:

\Program Files and \Program Files (x86)

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

- TrustedInstaller - Full control - This folder and subfolders
- SYSTEM - Modify - This folder only
- SYSTEM - Full control - Subfolders and files only
- Administrators - Modify - This folder only
- Administrators - Full control - Subfolders and files only
- Users - Read & execute - This folder, subfolders, and files
- CREATOR OWNER - Full control - Subfolders and files only
- ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files
- ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

Additional Information:

CCI-002165

Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4 :: AC-3 (4)
- NIST SP 800-53 Revision 5 :: AC-3 (4)

1.16 WN16-00-000180 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Permissions for the Windows installation directory must conform to minimum requirements.

```
GROUP ID:V-224834
RULE ID:SV-224834r958702
```

Rationale:

Changing the system's file and directory permissions allows the possibility of unauthorized and anonymous modification to the operating system and installed applications.

The default permissions are adequate when the Security Option "Network access: Let everyone permissions apply to anonymous users" is set to "Disabled" (WN16-SO-000290).

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124

Audit:

The default permissions are adequate when the Security Option "Network access: Let everyone permissions apply to anonymous users" is set to "Disabled" (WN16-SO-000290).

Review the permissions for the Windows installation directory (usually C:\Windows). Non-privileged groups such as Users or Authenticated Users must not have greater than "Read & execute" permissions. (Individual accounts must not be used to assign permissions.)

If permissions are not as restrictive as the default permissions listed below, this is a finding.

Viewing in File Explorer:

For each folder, view the Properties.

Select the "Security" tab and the "Advanced" button.

Default permissions:

\Windows

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

- TrustedInstaller - Full control - This folder and subfolders
- SYSTEM - Modify - This folder only
- SYSTEM - Full control - Subfolders and files only
- Administrators - Modify - This folder only
- Administrators - Full control - Subfolders and files only
- Users - Read & execute - This folder, subfolders, and files
- CREATOR OWNER - Full control - Subfolders and files only
- ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files
- ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

Alternately, use icacls:
Open a Command prompt (admin).
Enter

```
"icacls"
```

followed by the directory:

```
"icacls c:\windows"
```

The following results should be displayed for each when entered:

```
c:\windows
NT SERVICE\TrustedInstaller:(F)
NT SERVICE\TrustedInstaller:(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(M)
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
BUILTIN\Administrators:(M)
BUILTIN\Administrators:(OI)(CI)(IO)(F)
BUILTIN\Users:(RX)
BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION
PACKAGES:(OI)(CI)(IO)(GR,GE)
Successfully processed 1 files; Failed processing 0 files
```

Remediation:

Maintain the default file ACLs and configure the Security Option "Network access: Let everyone permissions apply to anonymous users" to "Disabled" (WN16-SO-000290).

Default permissions:

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

- TrustedInstaller - Full control - This folder and subfolders
- SYSTEM - Modify - This folder only
- SYSTEM - Full control - Subfolders and files only
- Administrators - Modify - This folder only
- Administrators - Full control - Subfolders and files only
- Users - Read & execute - This folder, subfolders, and files
- CREATOR OWNER - Full control - Subfolders and files only
- ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files
- ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

Additional Information:

CCI-002165

Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4 :: AC-3 (4)
- NIST SP 800-53 Revision 5 :: AC-3 (4)

1.17 WN16-00-000190 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained.

```
GROUP ID:V-224835
RULE ID:SV-224835r958726
```

Rationale:

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.

Audit:

Review the registry permissions for the keys of the HKEY_LOCAL_MACHINE hive noted below.

If any non-privileged groups such as Everyone, Users, or Authenticated Users have greater than Read permission, this is a finding.

If permissions are not as restrictive as the default permissions listed below, this is a finding.

Run "Regedit".

Right-click on the registry areas noted below.

Select "Permissions..." and the "Advanced" button.

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 - Subkeys only
- ALL APPLICATION PACKAGES - Read - This key and subkeys
- Server Operators – Read – This Key and subkeys (Domain controllers only)

Other examples under the noted keys may also be sampled. There may be some instances where non-privileged groups have greater than Read permission.
If the defaults have not been changed, these are not a finding.

Remediation:

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 - Subkeys only
- ALL APPLICATION PACKAGES - Read - This key and subkeys
- Server Operators – Read – This Key and subkeys (Domain controllers only)

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.18 WN16-00-000200 (Manual)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

Non-administrative accounts or groups must only have print permissions on printer shares.

```
GROUP ID:V-224836
RULE ID:SV-224836r958472
```

Rationale:

Windows shares are a means by which files, folders, printers, and other resources can be published for network users to access. Improper configuration can permit access to devices and data beyond a user's need.

Audit:

Open "Devices and Printers".

If there are no printers configured, this is NA. (Exclude Microsoft Print to PDF and Microsoft XPS Document Writer, which do not support sharing.)

For each printer:

Right-click on the printer.

Select "Printer Properties".

Select the "Sharing" tab.

If "Share this printer" is checked, select the "Security" tab.

If any standard user accounts or groups have permissions other than "Print", this is a finding.

The default is for the "Everyone" group to be given "Print" permission.

"All APPLICATION PACKAGES" and "CREATOR OWNER" are not standard user accounts.

Remediation:

Configure the permissions on shared printers to restrict standard users to only have Print permissions.

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3
- NIST SP 800-53A :: AC-3.1

1.19 WN16-00-000210 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Outdated or unused accounts must be removed from the system or disabled.

```
GROUP ID:V-224837
RULE ID:SV-224837r958482
```

Rationale:

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.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000118-GPOS-00060

Audit:

Open "Windows PowerShell".

Domain Controllers:

Enter "Search-ADAccount -AccountInactive -UsersOnly -TimeSpan 35.00:00:00"

This will return accounts that have not been logged on to for 35 days, along with various attributes such as the Enabled status and LastLogonDate.

Member servers and standalone or nondomain-joined systems:

Copy or enter the lines below to the PowerShell window and enter. (Entering twice may be required. Do not include the quotes at the beginning and end of the query.)

```
"([ADSI]('WinNT://{0}' -f $env:COMPUTERNAME)).Children | Where {
$_.SchemaClassName -eq 'user' } | ForEach {
 $user = ([ADSI]$_.Path)
 $lastLogin = $user.Properties.LastLogin.Value
 $enabled = ($user.Properties.UserFlags.Value -band 0x2) -ne 0x2
 if ($lastLogin -eq $null) {
 $lastLogin = 'Never'
 }
 Write-Host $user.Name $lastLogin $enabled
}"
```

This will return a list of local accounts with the account name, last logon, and if the account is enabled (True/False).

For example: User1 10/31/2015 5:49:56 AM True

Review the list of accounts returned by the above queries to determine the finding validity for each account reported.

Exclude the following accounts:

- Built-in administrator account (Renamed, SID ending in 500)
- Built-in guest account (Renamed, Disabled, SID ending in 501)
- Built-in default account (Renamed, Disabled, SID ending in 503)
- Application accounts

If any enabled accounts have not been logged on to within the past 35 days, this is a finding.
Inactive accounts that have been reviewed and deemed to be required must be documented with the ISSO.

Remediation:

Regularly review accounts to determine if they are still active. Remove or disable accounts that have not been used in the last 35 days.

Additional Information:

CCI-000764

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53 :: IA-2
- NIST SP 800-53 Revision 4 :: IA-2
- NIST SP 800-53 Revision 5 :: IA-2
- NIST SP 800-53A :: IA-2.1

CCI-000795

The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53 :: IA-4 e
- NIST SP 800-53 Revision 4 :: IA-4 e
- NIST SP 800-53A :: IA-4.1 (iii)

1.20 WN16-00-000220 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 accounts must require passwords.

```
GROUP ID:V-224838
RULE ID:SV-224838r958482
```

Rationale:

The lack of password protection enables anyone to gain access to the information system, which opens a backdoor opportunity for intruders to compromise the system as well as other resources. Accounts on a system must require passwords.

Audit:

Review the password required status for enabled user accounts.

Open "PowerShell".

Domain Controllers:

Enter

```
"Get-Aduser -Filter * -Properties Passwordnotrequired |FT Name,
Passwordnotrequired, Enabled"
```

Exclude disabled accounts (e.g., DefaultAccount, Guest) and Trusted Domain Objects (TDOs).

If "Passwordnotrequired" is "True" or blank for any enabled user account, this is a finding.

Member servers and standalone or nondomain-joined systems:

Enter

```
'Get-CimInstance -Class Win32_Useraccount -Filter "PasswordRequired=False and
LocalAccount=True" | FT Name, PasswordRequired, Disabled, LocalAccount'
```

Exclude disabled accounts (e.g., DefaultAccount, Guest).

If any enabled user accounts are returned with a "PasswordRequired" status of "False", this is a finding.

Remediation:

Configure all enabled user accounts to require passwords.

The password required flag can be set by entering the following on a command line: "Net user [username] /passwordreq:yes", substituting [username] with the name of the user account.

Additional Information:

CCI-000764

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53 :: IA-2
- NIST SP 800-53 Revision 4 :: IA-2
- NIST SP 800-53 Revision 5 :: IA-2
- NIST SP 800-53A :: IA-2.1

1.21 WN16-00-000230 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Passwords must be configured to expire.

```
GROUP ID:V-224839
RULE ID:SV-224839r1038967
```

Rationale:

Passwords that do not expire or are reused increase the exposure of a password with greater probability of being discovered or cracked.

Audit:

Review the password never expires status for enabled user accounts.

Open "PowerShell".

Domain Controllers:

Enter

```
"Search-ADAccount -PasswordNeverExpires -UsersOnly | FT Name,
PasswordNeverExpires, Enabled"
```

Exclude application accounts, disabled accounts (e.g., DefaultAccount, Guest), and the krbtgt account.

If any enabled user accounts are returned with a "PasswordNeverExpires" status of "True", this is a finding.

Member servers and standalone or nondomain-joined systems:

Enter

```
'Get-CimInstance -Class Win32_Useraccount -Filter "PasswordExpires=False and
LocalAccount=True" | FT Name, PasswordExpires, Disabled, LocalAccount'
```

Exclude application accounts and disabled accounts (e.g., DefaultAccount, Guest).

If any enabled user accounts are returned with a "PasswordExpires" status of "False", this is a finding.

Remediation:

Configure all enabled user account passwords to expire.

Uncheck "Password never expires" for all enabled user accounts in Active Directory Users and Computers for domain accounts and Users in Computer Management for member servers and standalone or nondomain-joined systems. Document any exceptions with the ISSO.

Additional Information:

CCI-000199

The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53 :: IA-5 (1) (d)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (d)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.22 WN16-00-000240 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

System files must be monitored for unauthorized changes.

```
GROUP ID:V-224840
RULE ID:SV-224840r958794
```

Rationale:

Monitoring system files for changes against a baseline on a regular basis may help detect the possible introduction of malicious code on a system.

Audit:

Determine if the system is monitored for unauthorized changes to system files (e.g., *.exe, *.bat, *.com, *.cmd, and *.dll) against a baseline on a weekly basis.

If system files are not being monitored for unauthorized changes, this is a finding.

An approved and properly configured solution will contain both a list of baselines that includes all system file locations and a file comparison task that is scheduled to run at least weekly.

Remediation:

Monitor the system for unauthorized changes to system files (e.g., *.exe, *.bat, *.com, *.cmd, and *.dll) against a baseline on a weekly basis. This can be done with the use of various monitoring tools.

Additional Information:

CCI-001744

Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

- NIST SP 800-53 Revision 4 :: CM-3 (5)
- NIST SP 800-53 Revision 5 :: CM-3 (5)

1.23 WN16-00-000250 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

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

```
GROUP ID:V-224841
RULE ID:SV-224841r958524
```

Rationale:

Shares on a system provide network access. To prevent exposing sensitive information, where shares are necessary, permissions must be reconfigured to give the minimum access to accounts that require it.

Audit:

If only system-created shares such as "ADMIN$", "C$", and "IPC$" exist on the system, this is NA. (System-created shares will display a message that it has been shared for administrative purposes when "Properties" is selected.)

Run "Computer Management".

Navigate to System Tools >> Shared Folders >> Shares.

Right-click any non-system-created shares.

Select "Properties".

Select the "Share Permissions" tab.

If the file shares have not been configured to restrict permissions to the specific groups or accounts that require access, this is a finding.

Select the "Security" tab.

If the permissions have not been configured to restrict permissions to the specific groups or accounts that require access, this is a finding.

Remediation:

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.

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4
- NIST SP 800-53A :: SC-4.1

1.24 WN16-00-000270 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Software certificate installation files must be removed from Windows Server 2016.

```
GROUP ID:V-224842
RULE ID:SV-224842r991589
```

Rationale:

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.

Audit:

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.

Remediation:

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 or Adobe PreFlight certificate files.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.25 WN16-00-000280 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Systems requiring data at rest protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

```
GROUP ID:V-224843
RULE ID:SV-224843r958552
```

Rationale:

This requirement addresses protection of user-generated data as well as operating system-specific configuration data. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate, in accordance with the security category and/or classification of the information.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Satisfies: SRG-OS-000185-GPOS-00079, SRG-OS-000404-GPOS-00183, SRG-OS-000405-GPOS-00184

Audit:

Verify systems that require additional protections due to factors such as inadequate physical protection or sensitivity of the data employ encryption to protect the confidentiality and integrity of all information at rest.

If they do not, this is a finding.

Remediation:

Configure systems that require additional protections due to factors such as inadequate physical protection or sensitivity of the data to employ encryption to protect the confidentiality and integrity of all information at rest.

Additional Information:

CCI-001199

Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53 :: SC-28
- NIST SP 800-53 Revision 4 :: SC-28
- NIST SP 800-53 Revision 5 :: SC-28
- NIST SP 800-53A :: SC-28.1

CCI-002475

Implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information when at rest on organization-defined system components.

- NIST SP 800-53 Revision 4 :: SC-28 (1)
- NIST SP 800-53 Revision 5 :: SC-28 (1)

CCI-002476

Implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4 :: SC-28 (1)
- NIST SP 800-53 Revision 5 :: SC-28 (1)

1.26 WN16-00-000290 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Protection methods such as TLS, encrypted VPNs, or IPsec must be implemented if the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process.

```
GROUP ID:V-224844
RULE ID:SV-224844r958912
```

Rationale:

Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Ensuring the confidentiality of transmitted information requires the operating system to take measures in preparing information for transmission. This can be accomplished via access control and encryption.

Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, operating systems need to support transmission protection mechanisms such as TLS, encrypted VPNs, or IPsec.

Satisfies: SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

If the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process, verify protection methods such as TLS, encrypted VPNs, or IPsec have been implemented.

If protection methods have not been implemented, this is a finding.

Remediation:

Configure protection methods such as TLS, encrypted VPNs, or IPsec when the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process.

Additional Information:

CCI-002420

Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

CCI-002422

Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

1.27 WN16-00-000300 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The roles and features required by the system must be documented.

```
GROUP ID:V-224845
RULE ID:SV-224845r958478
```

Rationale:

Unnecessary roles and features increase the attack surface of a system. Limiting roles and features of a system to only those necessary reduces this potential. The standard installation option (previously called Server Core) further reduces this when selected at installation.

Audit:

Required roles and features will vary based on the function of the individual system.

Roles and features specifically required to be disabled per the STIG are identified in separate requirements.

If the organization has not documented the roles and features required for the system(s), this is a finding.

The PowerShell command

```
"Get-WindowsFeature"
```

will list all roles and features with an "Install State".

Remediation:

Document the roles and features required for the system to operate. Uninstall any that are not required.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.28 WN16-00-000310 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

A host-based firewall must be installed and enabled on the system.

```
GROUP ID:V-224846
RULE ID:SV-224846r991589
```

Rationale:

A firewall provides a line of defense against attack, allowing or blocking inbound and outbound connections based on a set of rules.

Audit:

Determine if a host-based firewall is installed and enabled on the system.

If a host-based firewall is not installed and enabled on the system, this is a finding.

The configuration requirements will be determined by the applicable firewall STIG.

Remediation:

Install and enable a host-based firewall on the system.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CCI-002080

The organization employs either an allow-all, deny-by-exception or a deny-all, permit-by-exception policy for allowing organization-defined information systems to connect to external information systems.

- NIST SP 800-53 Revision 4 :: CA-3 (5)

1.29 WN16-00-000320 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where Endpoint Security Solution (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).

```
GROUP ID:V-224847
RULE ID:SV-224847r982191
```

Rationale:

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. The operating system may have an integrated solution incorporating continuous scanning using ESS and periodic scanning using other tools.

Audit:

Verify DoD-approved ESS software is installed and properly operating. Ask the site ISSM for documentation of the ESS software installation and configuration.

If the ISSM is not able to provide a documented configuration for an installed ESS or if the ESS software is not properly maintained or used, this is a finding.

Note: Example of documentation can be a copy of the site's CCB approved Software Baseline with version of software noted or a memo from the ISSM stating current ESS software and version.

Remediation:

Install a DoD-approved ESS software and ensure it is operating continuously.

Additional Information:

CCI-001233

The organization employs automated mechanisms on an organization-defined frequency to determine the state of information system components with regard to flaw remediation.

- NIST SP 800-53 :: SI-2 (2)
- NIST SP 800-53 Revision 4 :: SI-2 (2)
- NIST SP 800-53A :: SI-2 (2).1 (ii)

1.30 WN16-00-000330 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must automatically remove or disable temporary user accounts after 72 hours.

```
GROUP ID:V-224848
RULE ID:SV-224848r958364
```

Rationale:

If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be used to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

If temporary accounts are used, the operating system must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours.

To address access requirements, many operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Audit:

Review temporary user accounts for expiration dates.

Determine if temporary user accounts are used and identify any that exist. If none exist, this is NA.

Domain Controllers:

Open "PowerShell".

Enter

```
"Search-ADAccount -AccountExpiring | FT Name, AccountExpirationDate"
```

If "AccountExpirationDate" has not been defined within 72 hours for any temporary user account, this is a finding.

Member servers and standalone or nondomain-joined systems:

Open "Command Prompt".

Run

```
"Net user [username]"
```

where [username] is the name of the temporary user account.

If "Account expires" has not been defined within 72 hours for any temporary user account, this is a finding.

Remediation:

Configure temporary user accounts to automatically expire within 72 hours.

Domain accounts can be configured with an account expiration date under "Account" properties.

Local accounts can be configured to expire with the command

```
"Net user [username] /expires:[mm/dd/yyyy]"
```

where username is the name of the temporary user account.

Delete any temporary user accounts that are no longer necessary.

Additional Information:

CCI-000016

Automatically remove or disable temporary and emergency accounts after an organization-defined time-period for each type of account.

- NIST SP 800-53 :: AC-2 (2)
- NIST SP 800-53 Revision 4 :: AC-2 (2)
- NIST SP 800-53 Revision 5 :: AC-2 (2)
- NIST SP 800-53A :: AC-2 (2).1 (ii)

1.31 WN16-00-000340 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must automatically remove or disable emergency accounts after the crisis is resolved or within 72 hours.

```
GROUP ID:V-224849
RULE ID:SV-224849r958508
```

Rationale:

Emergency administrator accounts are privileged accounts established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency administrator accounts are different from infrequently used accounts (i.e., local logon accounts used by system administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Audit:

Determine if emergency administrator accounts are used and identify any that exist. If none exist, this is NA.

If emergency administrator accounts cannot be configured with an expiration date due to an ongoing crisis, the accounts must be disabled or removed when the crisis is resolved.

If emergency administrator accounts have not been configured with an expiration date or have not been disabled or removed following the resolution of a crisis, this is a finding.

Domain Controllers:

Open "PowerShell".

Enter

```
"Search-ADAccount –AccountExpiring | FT Name, AccountExpirationDate"
```

If "AccountExpirationDate" has been defined and is not within 72 hours for an emergency administrator account, this is a finding.

Member servers and standalone or nondomain-joined systems:

Open "Command Prompt".

Run

```
"Net user [username]"
```

where [username] is the name of the emergency account.

If "Account expires" has been defined and is not within 72 hours for an emergency administrator account, this is a finding.

Remediation:

Remove emergency administrator accounts after a crisis has been resolved or configure the accounts to automatically expire within 72 hours.

Domain accounts can be configured with an account expiration date under "Account" properties.

Local accounts can be configured to expire with the command

```
"Net user [username] /expires:[mm/dd/yyyy]"
```

where username is the name of the temporary user account.

Additional Information:

CCI-001682

Automatically removes or disables emergency accounts after an organization-defined time period for each type of account.

- NIST SP 800-53 :: AC-2 (2)
- NIST SP 800-53 Revision 4 :: AC-2 (2)
- NIST SP 800-53 Revision 5 :: AC-2 (2)
- NIST SP 800-53A :: AC-2 (2).1 (ii)

1.32 WN16-00-000350 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Fax Server role must not be installed.

```
GROUP ID:V-224850
RULE ID:SV-224850r958478
```

Rationale:

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Audit:

Open "PowerShell".

Enter

```
"Get-WindowsFeature | Where Name -eq Fax"
```

If "Installed State" is "Installed", this is a finding.

An Installed State of "Available" or "Removed" is not a finding.

Remediation:

Uninstall the "Fax Server" role.

Start "Server Manager".

Select the server with the role.

Scroll down to "ROLES AND FEATURES" in the right pane.

Select "Remove Roles and Features" from the drop-down "TASKS" list.

Select the appropriate server on the "Server Selection" page and click "Next".

Deselect "Fax Server" on the "Roles" page.

Click "Next" and "Remove" as prompted.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.33 WN16-00-000360 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Microsoft FTP service must not be installed unless required.

```
GROUP ID:V-224851
RULE ID:SV-224851r958480
```

Rationale:

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption.

Audit:

If the server has the role of an FTP server, this is NA.

Open "PowerShell".

Enter

```
"Get-WindowsFeature | Where Name -eq Web-Ftp-Service"
```

If "Installed State" is "Installed", this is a finding.

An Installed State of "Available" or "Removed" is not a finding.

If the system has the role of an FTP server, this must be documented with the ISSO.

Remediation:

Uninstall the "FTP Server" role.

Start "Server Manager".

Select the server with the role.

Scroll down to "ROLES AND FEATURES" in the right pane.

Select "Remove Roles and Features" from the drop-down "TASKS" list.

Select the appropriate server on the "Server Selection" page and click "Next".

Deselect "FTP Server" under "Web Server (IIS)" on the "Roles" page.

Click "Next" and "Remove" as prompted.

Additional Information:

CCI-000382

Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 b
- NIST SP 800-53 Revision 5 :: CM-7 b
- NIST SP 800-53A :: CM-7.1 (iii)

1.34 WN16-00-000370 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Peer Name Resolution Protocol must not be installed.

```
GROUP ID:V-224852
RULE ID:SV-224852r958478
```

Rationale:

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Audit:

Open "PowerShell".

Enter

```
"Get-WindowsFeature | Where Name -eq PNRP"
```

If "Installed State" is "Installed", this is a finding.

An Installed State of "Available" or "Removed" is not a finding.

Remediation:

Uninstall the "Peer Name Resolution Protocol" feature.

Start "Server Manager".

Select the server with the feature.

Scroll down to "ROLES AND FEATURES" in the right pane.

Select "Remove Roles and Features" from the drop-down "TASKS" list.

Select the appropriate server on the "Server Selection" page and click "Next".

Deselect "Peer Name Resolution Protocol" on the "Features" page.

Click "Next" and "Remove" as prompted.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.35 WN16-00-000380 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Simple TCP/IP Services must not be installed.

```
GROUP ID:V-224853
RULE ID:SV-224853r958478
```

Rationale:

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Audit:

Open "PowerShell".

Enter

```
"Get-WindowsFeature | Where Name -eq Simple-TCPIP"
```

If "Installed State" is "Installed", this is a finding.

An Installed State of "Available" or "Removed" is not a finding.

Remediation:

Uninstall the "Simple TCP/IP Services" feature.

Start "Server Manager".

Select the server with the feature.

Scroll down to "ROLES AND FEATURES" in the right pane.

Select "Remove Roles and Features" from the drop-down "TASKS" list.

Select the appropriate server on the "Server Selection" page and click "Next".

Deselect "Simple TCP/IP Services" on the "Features" page.

Click "Next" and "Remove" as prompted.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.36 WN16-00-000390 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Telnet Client must not be installed.

```
GROUP ID:V-224854
RULE ID:SV-224854r958480
```

Rationale:

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Audit:

Open "PowerShell".

Enter

```
"Get-WindowsFeature | Where Name -eq Telnet-Client"
```

If "Installed State" is "Installed", this is a finding.

An Installed State of "Available" or "Removed" is not a finding.

Remediation:

Uninstall the "Telnet Client" feature.

Start "Server Manager".

Select the server with the feature.

Scroll down to "ROLES AND FEATURES" in the right pane.

Select "Remove Roles and Features" from the drop-down "TASKS" list.

Select the appropriate server on the "Server Selection" page and click "Next".

Deselect "Telnet Client" on the "Features" page.

Click "Next" and "Remove" as prompted.

Additional Information:

CCI-000382

Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 b
- NIST SP 800-53 Revision 5 :: CM-7 b
- NIST SP 800-53A :: CM-7.1 (iii)

1.37 WN16-00-000400 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The TFTP Client must not be installed.

```
GROUP ID:V-224855
RULE ID:SV-224855r958478
```

Rationale:

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Audit:

Open "PowerShell".

Enter

```
"Get-WindowsFeature | Where Name -eq TFTP-Client"
```

If "Installed State" is "Installed", this is a finding.

An Installed State of "Available" or "Removed" is not a finding.

Remediation:

Uninstall the "TFTP Client" feature.

Start "Server Manager".

Select the server with the feature.

Scroll down to "ROLES AND FEATURES" in the right pane.

Select "Remove Roles and Features" from the drop-down "TASKS" list.

Select the appropriate server on the "Server Selection" page and click "Next".

Deselect "TFTP Client" on the "Features" page.

Click "Next" and "Remove" as prompted.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.38 WN16-00-000410 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Server Message Block (SMB) v1 protocol must be uninstalled.

```
GROUP ID:V-224856
RULE ID:SV-224856r958478
```

Rationale:

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 and is not FIPS compliant.

Audit:

Different methods are available to disable SMBv1 on Windows 2016. This is the preferred method, however if V-78123 and V-78125 are configured, this is NA.

Open "Windows PowerShell" with elevated privileges (run as administrator).

Enter

```
"Get-WindowsFeature -Name FS-SMB1"
```

If "Installed State" is "Installed", this is a finding.

An Installed State of "Available" or "Removed" is not a finding.

Remediation:

Uninstall the SMBv1 protocol.

Open "Windows PowerShell" with elevated privileges (run as administrator).

Enter

```
"Uninstall-WindowsFeature -Name FS-SMB1 -Restart"
```

(Omit the Restart parameter if an immediate restart of the system cannot be done.)

Alternately:

Start "Server Manager".

Select the server with the feature.

Scroll down to "ROLES AND FEATURES" in the right pane.

Select "Remove Roles and Features" from the drop-down "TASKS" list.

Select the appropriate server on the "Server Selection" page and click "Next".

Deselect "SMB 1.0/CIFS File Sharing Support" on the "Features" page.

Click "Next" and "Remove" as prompted.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.39 WN16-00-000411 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.

```
GROUP ID:V-224857
RULE ID:SV-224857r958478
```

Rationale:

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.

Audit:

Different methods are available to disable SMBv1 on Windows 2016, if V-73299 is configured, this is NA.

If the following registry value does not exist or is not configured as specified, this is a finding:

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\

Value Name: SMB1

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> MS Security Guide >>
"Configure SMBv1 Server" to "Disabled"
```

The system must be restarted for the change to take effect.

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.

References:

1. CIS Recommendation: Configure SMB v1 server
2. GRID: MS-00000243

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.40 WN16-00-000412 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.

```
GROUP ID:V-224858
RULE ID:SV-224858r958478
```

Rationale:

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.

Audit:

Different methods are available to disable SMBv1 on Windows 2016, if V-73299 is configured, this is NA.

If the following registry value is not configured as specified, this is a finding:

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\mrxsmb10\

Value Name: Start

Type: REG_DWORD
Value: 0x00000004 (4)
```

Remediation:

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"
```

The system must be restarted for the changes to take effect.

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.

References:

1. CIS Recommendation: Configure SMB v1 client driver
2. GRID: MS-00000242

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.41 WN16-00-000420 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows PowerShell 2.0 must not be installed.

```
GROUP ID:V-224859
RULE ID:SV-224859r958478
```

Rationale:

Windows PowerShell 5.0 added advanced logging features that 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.

Audit:

Open "PowerShell".

Enter

```
"Get-WindowsFeature | Where Name -eq PowerShell-v2"
```

If "Installed State" is "Installed", this is a finding.

An Installed State of "Available" or "Removed" is not a finding.

Remediation:

Uninstall the "Windows PowerShell 2.0 Engine".

Start "Server Manager".

Select the server with the feature.

Scroll down to "ROLES AND FEATURES" in the right pane.

Select "Remove Roles and Features" from the drop-down "TASKS" list.

Select the appropriate server on the "Server Selection" page and click "Next".

Deselect "Windows PowerShell 2.0 Engine" under "Windows PowerShell" on the "Features" page.

Click "Next" and "Remove" as prompted.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.42 WN16-00-000430 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

FTP servers must be configured to prevent anonymous logons.

```
GROUP ID:V-224860
RULE ID:SV-224860r991589
```

Rationale:

The FTP service allows remote users to access shared files and directories. Allowing anonymous FTP connections makes user auditing difficult.

Using accounts that have administrator privileges to log on to FTP risks that the userid and password will be captured on the network and give administrator access to an unauthorized user.

Audit:

If FTP is not installed on the system, this is NA.

Open "Internet Information Services (IIS) Manager".

Select the server.

Double-click "FTP Authentication".

If the "Anonymous Authentication" status is "Enabled", this is a finding.

Remediation:

Configure the FTP service to prevent anonymous logons.

Open "Internet Information Services (IIS) Manager".

Select the server.

Double-click "FTP Authentication".

Select "Anonymous Authentication".

Select "Disabled" under "Actions".

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.43 WN16-00-000440 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

FTP servers must be configured to prevent access to the system drive.

```
GROUP ID:V-224861
RULE ID:SV-224861r991589
```

Rationale:

The FTP service allows remote users to access shared files and directories that could provide access to system resources and compromise the system, especially if the user can gain access to the root directory of the boot drive.

Audit:

If FTP is not installed on the system, this is NA.

Open "Internet Information Services (IIS) Manager".

Select "Sites" under the server name.

For any sites with a Binding that lists FTP, right-click the site and select "Explore".

If the site is not defined to a specific folder for shared FTP resources, this is a finding.

If the site includes any system areas such as root of the drive, Program Files, or Windows directories, this is a finding.

Remediation:

Configure the FTP sites to allow access only to specific FTP shared resources. Do not allow access to other areas of the system.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.44 WN16-00-000450 (Manual)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

The time service must synchronize with an appropriate DoD time source.

```
GROUP ID:V-224862
RULE ID:SV-224862r1038944
```

Rationale:

The Windows Time Service controls time synchronization settings. Time synchronization is essential for authentication and auditing purposes. If the Windows Time Service is used, it must synchronize with a secure, authorized time source. Domain-joined systems are automatically configured to synchronize with domain controllers. If an NTP server is configured, it must synchronize with a secure, authorized time source.

Audit:

Review the Windows time service configuration.

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"W32tm /query /configuration"
```

Domain-joined systems (excluding the domain controller with the PDC emulator role):

If the value for "Type" under "NTP Client" is not "NT5DS", this is a finding.

Other systems:

If systems are configured with a "Type" of "NTP", including standalone or nondomain-joined systems and the domain controller with the PDC Emulator role, and do not have a DoD time server defined for "NTPServer", this is a finding.

To determine the domain controller with the PDC Emulator role:

Open "PowerShell".

Enter

```
"Get-ADDomain | FT PDCEmulator"
```

Remediation:

Configure the system to synchronize time with an appropriate DoD time source.

Domain-joined systems use NT5DS to synchronize time from other systems in the domain by default.

If the system needs to be configured to an NTP server, configure the system to point to an authorized time server by setting the policy value for Computer Configuration >> Administrative Templates >> System >> Windows Time Service >> Time Providers >> "Configure Windows NTP Client" to "Enabled", and configure the "NtpServer" field to point to an appropriate DoD time server.

The US Naval Observatory operates stratum 1 time servers, which are identified at:

https://www.cnmoc.usff.navy.mil/Our-Commands/United-States-Naval-Observatory/Precise-Time-Department/Network-Time-Protocol-NTP/

Time synchronization will occur through a hierarchy of time servers down to the local level. Clients and lower-level servers will synchronize with an authorized time server in the hierarchy.

Additional Information:

CCI-001891

The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4 :: AU-8 (1) (a)

1.45 WN16-00-000460 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Orphaned security identifiers (SIDs) must be removed from user rights on Windows 2016.

```
GROUP ID:V-224863
RULE ID:SV-224863r991589
```

Rationale:

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.

Audit:

Review the effective User Rights setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

Review each User Right listed for any unresolved SIDs to determine whether they are valid, such as due to being temporarily disconnected from the domain. (Unresolved SIDs have the format of "*S-1-…".)

If any unresolved SIDs exist and are not for currently valid accounts or groups, this is a finding.

For server core installations, run the following command:

```
Secedit /export /areas USER_RIGHTS /cfg c:\path\UserRights.txt
```

The results in the file identify user right assignments by SID instead of group name. Review the SIDs for unidentified ones. A list of typical SIDs \ Groups is below, search Microsoft for articles on well-known SIDs for others.

If any unresolved SIDs exist and are not for currently valid accounts or groups, this is a finding.

SID - Group

- S-1-5-11 - Authenticated Users
- S-1-5-113 - Local account
- S-1-5-114 - Local account and member of Administrators group
- S-1-5-19 - Local Service
- S-1-5-20 - Network Service
- S-1-5-32-544 - Administrators
- S-1-5-32-546 - Guests
- S-1-5-6 - Service
- S-1-5-9 - Enterprise Domain Controllers
- S-1-5-domain-512 - Domain Admins
- S-1-5-root domain-519 - Enterprise Admins
- S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420 - NT Service\WdiServiceHost

Remediation:

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.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.46 WN16-00-000470 (Manual)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

Secure Boot must be enabled on Windows Server 2016 systems.

```
GROUP ID:V-224864
RULE ID:SV-224864r991589
```

Rationale:

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 Server 2016, including Virtualization Based Security and Credential Guard. If Secure Boot is turned off, these security features will not function.

Audit:

Some older systems may not have UEFI firmware. This is currently a CAT III; it will be raised in severity at a future date when broad support of Windows hardware and firmware requirements are expected to be met. Devices that have UEFI firmware must have Secure Boot enabled.

Run "System Information".

Under "System Summary", if "Secure Boot State" does not display "On", this is a finding.

Remediation:

Enable Secure Boot in the system firmware.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.47 WN16-00-000480 (Manual)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

Windows 2016 systems must have Unified Extensible Firmware Interface (UEFI) firmware and be configured to run in UEFI mode, not Legacy BIOS.

```
GROUP ID:V-224865
RULE ID:SV-224865r991589
```

Rationale:

UEFI provides additional security features in comparison to legacy BIOS firmware, including Secure Boot. UEFI is required to support additional security features in Windows Server 2016, including Virtualization Based Security and Credential Guard. Systems with UEFI that are operating in "Legacy BIOS" mode will not support these security features.

Audit:

Some older systems may not have UEFI firmware. This is currently a CAT III; it will be raised in severity at a future date when broad support of Windows hardware and firmware requirements are expected to be met. Devices that have UEFI firmware must run in "UEFI" mode.

Verify the system firmware is configured to run in "UEFI" mode, not "Legacy BIOS".

Run "System Information".

Under "System Summary", if "BIOS Mode" does not display "UEFI", this is a finding.

Remediation:

Configure UEFI firmware to run in "UEFI" mode, not "Legacy BIOS" mode.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.48 WN16-AC-000010 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows 2016 account lockout duration must be configured to 15 minutes or greater.

```
GROUP ID:V-224866
RULE ID:SV-224866r958736
```

Rationale:

The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number of failed logon attempts.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Account Policies >> Account Lockout Policy
```

If the "Account lockout duration" is less than "15" minutes (excluding "0"), this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "LockoutDuration" is less than "15" (excluding "0") in the file, this is a finding.

Configuring this to "0", requiring an administrator to unlock the account, is more restrictive and is not a finding.

Remediation:

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.

References:

1. CIS Recommendation: Account lockout duration
2. GRID: MS-00000008

Additional Information:

CCI-002238

Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4 :: AC-7 b
- NIST SP 800-53 Revision 5 :: AC-7 b

1.49 WN16-AC-000020 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.

```
GROUP ID:V-224867
RULE ID:SV-224867r958388
```

Rationale:

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 normal user logon.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Account Policies >> Account Lockout Policy
```

If the "Account lockout threshold" is "0" or more than "3" attempts, this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "LockoutBadCount" equals "0" or is greater than "3" in the file, this is a finding.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Account
Policies >> Account Lockout Policy >> "Account lockout threshold" to "3" or
fewer invalid logon attempts (excluding "0", which is unacceptable)
```

References:

1. CIS Recommendation: Account lockout threshold
2. GRID: MS-00000009

Additional Information:

CCI-000044

Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

1.50 WN16-AC-000030 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.

```
GROUP ID: V-224868
RULE ID: SV-224868r958388
```

Rationale:

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.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Account Policies >> Account Lockout Policy
```

If the "Reset account lockout counter after" value is less than "15" minutes, this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "ResetLockoutCount" is less than "15" in the file, this is a finding.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Account
Policies >> Account Lockout Policy >> "Reset account lockout counter after"
to at least "15" minutes
```

References:

1. CIS Recommendation: Reset account lockout counter after
2. GRID: MS-00000011

Additional Information:

CCI-000044

Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a

CCI-002238

Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4 :: AC-7 b
- NIST SP 800-53 Revision 5 :: AC-7 b

1.51 WN16-AC-000040 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 password history must be configured to 24 passwords remembered.

```
GROUP ID: V-224869
RULE ID: SV-224869r982201
```

Rationale:

A system is more vulnerable to unauthorized access when system users recycle the same password several times without being required to change 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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Account Policies >> Password Policy
```

If the value for "Enforce password history" is less than "24" passwords remembered, this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "PasswordHistorySize" is less than "24" in the file, this is a finding.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> "Enforce password history" to "24" passwords remembered
```

References:

1. CIS Recommendation: Enforce password history
2. GRID: MS-00000001

Additional Information:

CCI-000200

The information system prohibits password reuse for the organization-defined number of generations.

- NIST SP 800-53 :: IA-5 (1) (e)
- NIST SP 800-53A :: IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (e)

1.52 WN16-AC-000050 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 maximum password age must be configured to 60 days or less.

```
GROUP ID: V-224870
RULE ID: SV-224870r1038967
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Account Policies >> Password Policy
```

If the value for the "Maximum password age" is greater than "60" days, this is a finding.

If the value is set to "0" (never expires), this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "MaximumPasswordAge" is greater than "60" or equal to "0" in the file, this is a finding.

Remediation:

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)
```

References:

1. CIS Recommendation: Maximum password age
2. GRID: MS-00000002

Additional Information:

CCI-000199

The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53 :: IA-5 (1) (d)
- NIST SP 800-53A :: IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (d)

1.53 WN16-AC-000060 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 minimum password age must be configured to at least one day.

```
GROUP ID:V-224871
RULE ID:SV-224871r982188
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Account Policies >> Password Policy
```

If the value for the "Minimum password age" is set to "0" days ("Password can be changed immediately"), this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "MinimumPasswordAge" equals "0" in the file, this is a finding.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Account
Policies >> Password Policy >> "Minimum password age" to at least "1" day
```

References:

1. CIS Recommendation: Minimum password age
2. GRID: MS-00000003

Additional Information:

CCI-000198

The information system enforces minimum password lifetime restrictions.

- NIST SP 800-53 :: IA-5 (1) (d)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (d)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.54 WN16-AC-000070 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 minimum password length must be configured to 14 characters.

```
GROUP ID:V-224872
RULE ID:SV-224872r982202
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Account Policies >> Password Policy
```

If the value for the "Minimum password length," is less than "14" characters, this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "MinimumPasswordLength" is less than "14" in the file, this is a finding.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Account
Policies >> Password Policy >> "Minimum password length" to "14" characters
```

References:

1. CIS Recommendation: Minimum password length
2. GRID: MS-00000004

Additional Information:

CCI-000205

The information system enforces minimum password length.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (i)

1.55 WN16-AC-000080 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must have the built-in Windows password complexity policy enabled.

```
GROUP ID:V-224873
RULE ID:SV-224873r982195
```

Rationale:

The use of complex passwords increases their strength against attack. The built-in Windows password complexity policy requires passwords to contain at least three of the four types of characters (numbers, upper- and lower-case letters, and special characters) and prevents the inclusion of user names or parts of user names.

Satisfies: SRG-OS-000069-GPOS-00037, SRG-OS-000070-GPOS-00038, SRG-OS-000071-GPOS-00039, SRG-OS-000266-GPOS-00101

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Account Policies >> Password Policy
```

If the value for "Password must meet complexity requirements" is not set to "Enabled", this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "PasswordComplexity" equals "0" in the file, this is a finding.

Note: If an external password filter is in use that enforces all four character types and requires this setting to be set to "Disabled", this would not be considered a finding. If this setting does not affect the use of an external password filter, it must be enabled for fallback purposes.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Account
Policies >> Password Policy >> "Password must meet complexity requirements"
to "Enabled"
```

References:

1. CIS Recommendation: Password must meet complexity requirements
2. GRID: MS-00000005

Additional Information:

CCI-000192

The information system enforces password complexity by the minimum number of upper case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CCI-000193

The information system enforces password complexity by the minimum number of lower case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CCI-000194

The information system enforces password complexity by the minimum number of numeric characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CCI-001619

The information system enforces password complexity by the minimum number of special characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.56 WN16-AC-000090 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Windows Server 2016 reversible password encryption must be disabled.

```
GROUP ID:V-224874
RULE ID:SV-224874r982199
```

Rationale:

Storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords, which are easily compromised. For this reason, this policy must never be enabled.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Account Policies >> Password Policy
```

If the value for "Store passwords using reversible encryption" is not set to "Disabled", this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "ClearTextPassword" equals "1" in the file, this is a finding.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Account
Policies >> Password Policy >> "Store passwords using reversible encryption"
to "Disabled"
```

References:

1. CIS Recommendation: Store passwords using reversible encryption
2. GRID: MS-00000007

Additional Information:

CCI-000196

The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.57 WN16-AU-000010 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Audit records must be backed up to a different system or media than the system being audited.

```
GROUP ID:V-224875
RULE ID:SV-224875r958754
```

Rationale:

Protection of log data includes assuring the log data is not accidentally lost or deleted. Audit information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Audit:

Determine if a process to back up log data to a different system or media than the system being audited has been implemented.

If it has not, this is a finding.

Remediation:

Establish and implement a process for backing up log data to another system or media other than the system being audited.

Additional Information:

CCI-001851

Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.58 WN16-AU-000020 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must, at a minimum, offload audit records of interconnected systems in real time and offload standalone or nondomain-joined systems weekly.

```
GROUP ID:V-224876
RULE ID:SV-224876r959008
```

Rationale:

Protection of log data includes ensuring the log data is not accidentally lost or deleted. Audit information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Audit:

Verify the audit records, at a minimum, are offloaded for interconnected systems in real time and offloaded for standalone or nondomain-joined systems weekly.

If they are not, this is a finding.

Remediation:

Configure the system to, at a minimum, offload audit records of interconnected systems in real time and offload standalone or nondomain-joined systems weekly.

Additional Information:

CCI-001851

Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.59 WN16-AU-000030 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Permissions for the Application event log must prevent access by non-privileged accounts.

```
GROUP ID:V-224877
RULE ID:SV-224877r958434
```

Rationale:

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.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Navigate to the Application event log file.

The default location is the "%SystemRoot%\System32\winevt\Logs" folder. However, the logs may have been moved to another folder.

If the permissions for the "Application.evtx" file are not as restrictive as the default permissions listed below, this is a finding.

- Eventlog - Full Control
- SYSTEM - Full Control
- Administrators - Full Control

Remediation:

Configure the permissions on the Application event log file (Application.evtx) to prevent access by non-privileged accounts. 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" folder.
If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as "NT Service\Eventlog".

Additional Information:

CCI-000162

Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000163

Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000164

Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

1.60 WN16-AU-000040 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Permissions for the Security event log must prevent access by non-privileged accounts.

```
GROUP ID:V-224878
RULE ID:SV-224878r958434
```

Rationale:

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.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Navigate to the Security event log file.

The default location is the "%SystemRoot%\System32\winevt\Logs" folder. However, the logs may have been moved to another folder.

If the permissions for the "Security.evtx" file are not as restrictive as the default permissions listed below, this is a finding.

- Eventlog - Full Control
- SYSTEM - Full Control
- Administrators - Full Control

Remediation:

Configure the permissions on the Security event log file (Security.evtx) to prevent access by non-privileged accounts. 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" folder.
If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as "NT Service\Eventlog".

Additional Information:

CCI-000162

Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000163

Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000164

Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

1.61 WN16-AU-000050 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Permissions for the System event log must prevent access by non-privileged accounts.

```
GROUP ID:V-224879
RULE ID:SV-224879r958434
```

Rationale:

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.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Navigate to the System event log file.

The default location is the "%SystemRoot%\System32\winevt\Logs" folder. However, the logs may have been moved to another folder.

If the permissions for the "System.evtx" file are not as restrictive as the default permissions listed below, this is a finding.

- Eventlog - Full Control
- SYSTEM - Full Control
- Administrators - Full Control

Remediation:

Configure the permissions on the System event log file (System.evtx) to prevent access by non-privileged accounts. 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" folder.
If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as "NT Service\Eventlog".

Additional Information:

CCI-000162

Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000163

Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000164

Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

1.62 WN16-AU-000060 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Event Viewer must be protected from unauthorized modification and deletion.

```
GROUP ID:V-224880
RULE ID:SV-224880r991558
```

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys in order to make access decisions regarding the modification or deletion of audit tools.

Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

Audit:

Navigate to "%SystemRoot%\System32".

View the permissions on "Eventvwr.exe".

If any groups or accounts other than TrustedInstaller have "Full control" or "Modify" permissions, this is a finding.

The default permissions below satisfy this requirement:

- TrustedInstaller - Full Control
- Administrators, SYSTEM, Users, ALL APPLICATION PACKAGES, ALL RESTRICTED APPLICATION PACKAGES - Read & Execute

Remediation:

Configure the permissions on the "Eventvwr.exe" file to prevent modification by any groups or accounts other than TrustedInstaller. The default permissions listed below satisfy this requirement:

- TrustedInstaller - Full Control
- Administrators, SYSTEM, Users, ALL APPLICATION PACKAGES, ALL RESTRICTED APPLICATION PACKAGES - Read & Execute

The default location is the "%SystemRoot%\ System32" folder.

Additional Information:

CCI-001494

Protect audit tools from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9
- NIST SP 800-53A :: AU-9.1

CCI-001495

Protect audit tools from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9
- NIST SP 800-53A :: AU-9.1

1.63 WN16-AU-000070 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.

```
GROUP ID:V-224881
RULE ID:SV-224881r991578
```

Rationale:

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.

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Account Logon >> Credential Validation - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Credential Validation
2. GRID: MS-00000196

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.64 WN16-AU-000080 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.

```
GROUP ID:V-224882
RULE ID:SV-224882r991578
```

Rationale:

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.

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Account Logon >> Credential Validation - Failure
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Credential Validation
2. GRID: MS-00000196

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.65 WN16-AU-000100 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.

```
GROUP ID:V-224883
RULE ID:SV-224883r958732
```

Rationale:

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.

Other Account Management Events records events such as the access of a password hash or the Password Policy Checking API being called.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Account Management >> Other Account Management Events - Success
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Advanced
Audit Policy Configuration >> System Audit Policies >> Account Management >>
"Audit Other Account Management Events" with "Success" selected
```

References:

1. CIS Recommendation: Audit Other Account Management Events
2. GRID: MS-00000202

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

1. NIST SP 800-53 :: AU-12 c
2. NIST SP 800-53 Revision 4 :: AU-12 c
3. NIST SP 800-53 Revision 5 :: AU-12 c
4. NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.66 WN16-AU-000120 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.

```
GROUP ID:V-224884
RULE ID:SV-224884r958368
```

Rationale:

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 security groups, including changes in group members.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Account Management >> Security Group Management - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Security Group Management
2. GRID: MS-00000203

Additional Information:

CCI-000018

Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403

Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404

Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405

Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130

Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

1.67 WN16-AU-000140 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Account Management - User Account Management successes.

```
GROUP ID:V-224885
RULE ID:SV-224885r958368
```

Rationale:

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.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Account Management >> User Account Management - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit User Account Management
2. GRID: MS-00000204

Additional Information:

CCI-000018

Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403

Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404

Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405

Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130

Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

1.68 WN16-AU-000150 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Account Management - User Account Management failures.

```
GROUP ID:V-224886
RULE ID:SV-224886r958368
```

Rationale:

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.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Account Management >> User Account Management - Failure
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit User Account Management
2. GRID: MS-00000204

Additional Information:

CCI-000018

Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403

Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404

Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405

Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130

Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

1.69 WN16-AU-000160 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Detailed Tracking - Plug and Play Events successes.

```
GROUP ID:V-224887
RULE ID:SV-224887r991583
```

Rationale:

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.

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Detailed Tracking >> Plug and Play Events - Success
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Advanced Audit Policy
Configuration >> System Audit Policies >> Detailed Tracking >> "Audit PNP
Activity" with "Success" selected
```

References:

1. CIS Recommendation: Audit PNP Activity
2. GRID: MS-00000205

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.70 WN16-AU-000170 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.

```
GROUP ID:V-224888
RULE ID:SV-224888r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000471-GPOS-00215

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Detailed Tracking >> Process Creation - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Process Creation
2. GRID: MS-00000206

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.71 WN16-AU-000230 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.

```
GROUP ID:V-224890
RULE ID:SV-224890r991552
```

Rationale:

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.

Satisfies: SRG-OS-000240-GPOS-00090, SRG-OS-000470-GPOS-00214

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following. If the system does not audit the following, this is a finding.

```
Logon/Logoff >> Account Lockout - Failure
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Account Lockout
2. GRID: MS-00000209

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001404

Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

1.72 WN16-AU-000240 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Logon/Logoff - Group Membership successes.

```
GROUP ID:V-224891
RULE ID:SV-224891r991578
```

Rationale:

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.

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Logon/Logoff >> Group Membership - Success
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Advanced Audit Policy
Configuration >> System Audit Policies >> Logon/Logoff >> "Audit Group
Membership" with "Success" selected
```

References:

1. CIS Recommendation: Audit Group Membership
2. GRID: MS-00000210

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.73 WN16-AU-000250 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.

```
GROUP ID:V-224892
RULE ID:SV-224892r958406
```

Rationale:

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.

Satisfies: SRG-OS-000032-GPOS-00013, SRG-OS-000470-GPOS-00214, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218, SRG-OS-000475-GPOS-00220

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Logon/Logoff >> Logoff - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Logoff
2. GRID: MS-00000211

Additional Information:

CCI-000067

Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53 :: AC-17 (1)
- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)
- NIST SP 800-53A :: AC-17 (1).1

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.74 WN16-AU-000260 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.

```
GROUP ID:V-224893
RULE ID:SV-224893r958406
```

Rationale:

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.

Satisfies: SRG-OS-000032-GPOS-00013, SRG-OS-000470-GPOS-00214, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218, SRG-OS-000475-GPOS-00220

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Logon/Logoff >> Logon - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Logon
2. GRID: MS-00000212

Additional Information:

CCI-000067

Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53 :: AC-17 (1)
- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)
- NIST SP 800-53A :: AC-17 (1).1

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.75 WN16-AU-000270 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.

```
GROUP ID:V-224894
RULE ID:SV-224894r958406
```

Rationale:

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.

Satisfies: SRG-OS-000032-GPOS-00013, SRG-OS-000470-GPOS-00214, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218, SRG-OS-000475-GPOS-00220

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Logon/Logoff >> Logon - Failure
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Logon
2. GRID: MS-00000212

Additional Information:

CCI-000067

Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53 :: AC-17 (1)
- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)
- NIST SP 800-53A :: AC-17 (1).1

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.76 WN16-AU-000280 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.

```
GROUP ID:V-224895
RULE ID:SV-224895r991578
```

Rationale:

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 that have administrative privileges and can be used to elevate processes.

Satisfies: SRG-OS-000470-GPOS-00214, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218, SRG-OS-000475-GPOS-00220

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Logon/Logoff >> Special Logon - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Special Logon
2. GRID: MS-00000214

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.77 WN16-AU-000285 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.

```
GROUP ID:V-224896
RULE ID:SV-224896r991578
```

Rationale:

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.

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the "AuditPol" tool to review the current Audit Policy configuration:

Open "PowerShell" or a "Command Prompt" with elevated privileges ("Run as Administrator").

Enter

```
"AuditPol /get /category:*"
```

Compare the "AuditPol" settings with the following:

If the system does not audit the following, this is a finding.

```
Object Access >> Other Object Access Events - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Other Object Access Events
2. GRID: MS-00000213

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.78 WN16-AU-000286 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.

```
GROUP ID:V-224897
RULE ID:SV-224897r991578
```

Rationale:

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.

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the "AuditPol" tool to review the current Audit Policy configuration:

Open "PowerShell" or a "Command Prompt" with elevated privileges ("Run as Administrator").

Enter

```
"AuditPol /get /category:*"
```

Compare the "AuditPol" settings with the following:

If the system does not audit the following, this is a finding.

```
Object Access >> Other Object Access Events - Failure
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Other Object Access Events
2. GRID: MS-00000213

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.79 WN16-AU-000290 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Object Access - Removable Storage successes.

```
GROUP ID:V-224898
RULE ID:SV-224898r991583
```

Rationale:

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.

Removable Storage auditing under Object Access records events related to access attempts on file system objects on removable storage devices.

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Object Access >> Removable Storage - Success
```

Virtual machines or systems that use network attached storage may generate excessive audit events for secondary virtual drives or the network attached storage when this setting is enabled. This may be set to Not Configured in such cases and would not be a finding.

Remediation:

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
```

References:

1. CIS Recommendation: Audit Removable Storage
2. GRID: MS-00000218

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.80 WN16-AU-000300 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Object Access - Removable Storage failures.

```
GROUP ID:V-224899
RULE ID:SV-224899r991583
```

Rationale:

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.

Removable Storage auditing under Object Access records events related to access attempts on file system objects on removable storage devices.

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Object Access >> Removable Storage - Failure
```

Virtual machines or systems that use network attached storage may generate excessive audit events for secondary virtual drives or the network attached storage when this setting is enabled. This may be set to Not Configured in such cases and would not be a finding.

Remediation:

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
```

References:

1. CIS Recommendation: Audit Removable Storage
2. GRID: MS-00000218

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.81 WN16-AU-000310 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.

```
GROUP ID:V-224900
RULE ID:SV-224900r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Policy Change >> Audit Policy Change - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Audit Policy Change
2. GRID: MS-00000219

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.82 WN16-AU-000320 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.

```
GROUP ID:V-224901
RULE ID:SV-224901r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Policy Change >> Audit Policy Change - Failure
```

Remediation:

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 "Failure" selected
```

References:

1. CIS Recommendation: Audit Audit Policy Change
2. GRID: MS-00000219

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.83 WN16-AU-000330 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.

```
GROUP ID:V-224902
RULE ID:SV-224902r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Policy Change >> Authentication Policy Change - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Authentication Policy Change
2. GRID: MS-00000220

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.84 WN16-AU-000340 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.

```
GROUP ID:V-224903
RULE ID:SV-224903r958732
```

Rationale:

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".

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Policy Change >> Authorization Policy Change - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Authorization Policy Change
2. GRID: MS-00000221

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.85 WN16-AU-000350 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.

```
GROUP ID:V-224904
RULE ID:SV-224904r958732
```

Rationale:

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".

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Privilege Use >> Sensitive Privilege Use - Success
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Sensitive Privilege Use
2. GRID: MS-00000224

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.86 WN16-AU-000360 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.

```
GROUP ID:V-224905
RULE ID:SV-224905r958732
```

Rationale:

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".

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

```
Privilege Use >> Sensitive Privilege Use - Failure
```

Remediation:

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
```

References:

1. CIS Recommendation: Audit Sensitive Privilege Use
2. GRID: MS-00000224

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.87 WN16-AU-000370 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit System - IPsec Driver successes.

```
GROUP ID:V-224906
RULE ID:SV-224906r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

System >> IPsec Driver - Success

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> "Audit IPsec Driver"
```

with "Success" selected.

References:

1. CIS Recommendation: Audit IPsec Driver
2. GRID: MS-00000225

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.88 WN16-AU-000380 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit System - IPsec Driver failures.

```
GROUP ID:V-224907
RULE ID:SV-224907r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

System >> IPsec Driver - Failure

Remediation:

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.

References:

1. CIS Recommendation: Audit IPsec Driver
2. GRID: MS-00000225

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.89 WN16-AU-000390 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit System - Other System Events successes.

```
GROUP ID:V-224908
RULE ID:SV-224908r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

System >> Other System Events - Success

Remediation:

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.

References:

1. CIS Recommendation: Audit Other System Events
2. GRID: MS-00000226

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.90 WN16-AU-000400 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit System - Other System Events failures.

```
GROUP ID:V-224909
RULE ID:SV-224909r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

System >> Other System Events - Failure

Remediation:

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.

References:

1. CIS Recommendation: Audit Other System Events
2. GRID: MS-00000226

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.91 WN16-AU-000410 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit System - Security State Change successes.

```
GROUP ID:V-224910
RULE ID:SV-224910r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

System >> Security State Change - Success

Remediation:

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.

References:

1. CIS Recommendation: Audit Security State Change
2. GRID: MS-00000227

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.92 WN16-AU-000420 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit System - Security System Extension successes.

```
GROUP ID:V-224911
RULE ID:SV-224911r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

System >> Security System Extension - Success

Remediation:

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.

References:

1. CIS Recommendation: Audit Security System Extension
2. GRID: MS-00000228

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.93 WN16-AU-000440 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit System - System Integrity successes.

```
GROUP ID:V-224912
RULE ID:SV-224912r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

System >> System Integrity - Success

Remediation:

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.

References:

1. CIS Recommendation: Audit System Integrity
2. GRID: MS-00000229

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.94 WN16-AU-000450 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit System - System Integrity failures.

```
GROUP ID:V-224913
RULE ID:SV-224913r958732
```

Rationale:

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.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

System >> System Integrity - Failure

Remediation:

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.

References:

1. CIS Recommendation: Audit System Integrity
2. GRID: MS-00000229

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.95 WN16-CC-000010 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The display of slide shows on the lock screen must be disabled.

```
GROUP ID:V-224914
RULE ID:SV-224914r958478
```

Rationale:

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.

Audit:

Verify the registry value below.

If it does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Personalization\

Value Name: NoLockScreenSlideshow

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Control Panel >>
Personalization >> "Prevent enabling lock screen slide show"
```

to "Enabled".

References:

1. CIS Recommendation: Prevent enabling lock screen slide show
2. GRID: MS-00000232

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.96 WN16-CC-000030 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

WDigest Authentication must be disabled on Windows Server 2016.

```
GROUP ID:V-224915
RULE ID:SV-224915r958478
```

Rationale:

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 Server 2016. This setting ensures this is enforced.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive:  HKEY_LOCAL_MACHINE
Registry Path:  \SYSTEM\CurrentControlSet\Control\SecurityProviders\Wdigest\

Value Name:  UseLogonCredential

Type:  REG_DWORD
Value:  0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> MS Security Guide >>
"WDigest Authentication (disabling may require KB2871997)"
```

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.

References:

1. CIS Recommendation: WDigest Authentication
2. GRID: MS-00000248

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.97 WN16-CC-000040 (Automated)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.

```
GROUP ID:V-224916
RULE ID:SV-224916r991589
```

Rationale:

Configuring the system to disable IPv6 source routing protects against spoofing.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\

Value Name: DisableIPSourceRouting

Type: REG_DWORD
Value: 0x00000002 (2)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> MSS (Legacy) >> "MSS:
(DisableIPSourceRouting IPv6) IP source routing protection level (protects
against packet spoofing)"
```

to "Enabled" with "Highest protection, source routing is completely disabled" selected.

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.

References:

1. CIS Recommendation: MSS: (DisableIPSourceRouting IPv6) IP source routing protection level
2. GRID: MS-00000250

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.98 WN16-CC-000050 (Automated)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.

```
GROUP ID:V-224917
RULE ID:SV-224917r991589
```

Rationale:

Configuring the system to disable IP source routing protects against spoofing.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\

Value Name: DisableIPSourceRouting

Value Type: REG_DWORD
Value: 0x00000002 (2)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> MSS (Legacy) >> "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)"
```

to "Enabled" with "Highest protection, source routing is completely disabled" selected.

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.

References:

1. CIS Recommendation: MSS: (DisableIPSourceRouting) IP source routing protection level
2. GRID: MS-00000251

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.99 WN16-CC-000060 (Automated)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.

```
GROUP ID:V-224918
RULE ID:SV-224918r991589
```

Rationale:

Allowing ICMP redirect of routes can lead to traffic not being routed properly. When disabled, this forces ICMP to be routed via the shortest path first.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\

Value Name: EnableICMPRedirect

Value Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

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.

References:

1. CIS Recommendation: MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes
2. GRID: MS-00000253

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.100 WN16-CC-000070 (Automated)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.

```
GROUP ID:V-224919
RULE ID:SV-224919r958902
```

Rationale:

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 server's WINS resolution capability.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive:  HKEY_LOCAL_MACHINE
Registry Path:  \SYSTEM\CurrentControlSet\Services\Netbt\Parameters\

Value Name:  NoNameReleaseOnDemand

Value Type:  REG_DWORD
Value:  0x00000001 (1)
```

Remediation:

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.

References:

1. CIS Recommendation: MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers
2. GRID: MS-00000255

Additional Information:

CCI-002385

Protect against or limit the effects of organization-defined types of denial of service events.

- NIST SP 800-53 Revision 4 :: SC-5
- NIST SP 800-53 Revision 5 :: SC-5 a

1.101 WN16-CC-000080 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Insecure logons to an SMB server must be disabled.

```
GROUP ID:V-224920
RULE ID:SV-224920r991589
```

Rationale:

Insecure guest logons allow unauthenticated access to shared folders. Shared resources on a system must require authentication to establish proper access.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation\

Value Name: AllowInsecureGuestAuth

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Network >> Lanman
Workstation >> "Enable insecure guest logons"
```

to "Disabled".

References:

1. CIS Recommendation: Enable insecure guest logons
2. GRID: MS-00000266

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.102 WN16-CC-000090 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *SYSVOL and* \\NETLOGON shares.

```
GROUP ID:V-224921
RULE ID:SV-224921r991589
```

Rationale:

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.

Audit:

This requirement is applicable to domain-joined systems. For standalone or nondomain-joined systems, this is NA.

If the following registry values do not exist or are not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths\

Value Name: \\*\NETLOGON
Value Type: REG_SZ
Value: RequireMutualAuthentication=1, RequireIntegrity=1

Value Name: \\*\SYSVOL
Value Type: REG_SZ
Value: RequireMutualAuthentication=1, RequireIntegrity=1
```

Additional entries would not be a finding.

Remediation:

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
```

References:

1. CIS Recommendation: Hardened UNC Paths
2. GRID: MS-00000273

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.103 WN16-CC-000100 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Command line data must be included in process creation events.

```
GROUP ID:V-224922
RULE ID:SV-224922r958422
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit\

Value Name: ProcessCreationIncludeCmdLine_Enabled

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> System >> Audit Process
Creation >> "Include command line in process creation events"
```

to "Enabled".

References:

1. CIS Recommendation: Include command line in process creation events
2. GRID: MS-00000294

Additional Information:

CCI-000135

Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

1.104 WN16-CC-000110 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 virtualization-based security must be enabled with the platform security level configured to Secure Boot or Secure Boot with DMA Protection.

```
GROUP ID:V-224923
RULE ID:SV-224923r991589
```

Rationale:

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).

Audit:

For standalone or nondomain-joined systems, this is NA.

Open "PowerShell" with elevated privileges (run as administrator).

Enter the following:

```
"Get-CimInstance -ClassName Win32_DeviceGuard -Namespace
root\Microsoft\Windows\DeviceGuard"
```

If "RequiredSecurityProperties" does not include a value of "2" indicating "Secure Boot" (e.g., "{1, 2}"), this is a finding.

If "Secure Boot and DMA Protection" is configured, "3" will also be displayed in the results (e.g., "{1, 2, 3}").

If "VirtualizationBasedSecurityStatus" is not a value of "2" indicating "Running", this is a finding.

Alternately:

Run "System Information".

Under "System Summary", verify the following:

If "Device Guard Virtualization based security" does not display "Running", this is a finding.

If "Device Guard Required Security Properties" does not display "Base Virtualization Support, Secure Boot", this is a finding.

If "Secure Boot and DMA Protection" is configured, "DMA Protection" will also be displayed (e.g., "Base Virtualization Support, Secure Boot, DMA Protection").

The policy settings referenced in the Fix section will configure the following registry values. However, due to hardware requirements, the registry values alone do not ensure proper function.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\DeviceGuard\

Value Name: EnableVirtualizationBasedSecurity
Value Type: REG_DWORD
Value: 0x00000001 (1)

Value Name: RequirePlatformSecurityFeatures
Value Type: REG_DWORD
Value: 0x00000001 (1) (Secure Boot only) or 0x00000003 (3) (Secure Boot and
DMA Protection)
```

A Microsoft TechNet article on Credential Guard, including system requirement details, can be found at the following link:

https://technet.microsoft.com/itpro/windows/keep-secure/credential-guard

Remediation:

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.

A Microsoft TechNet article on Credential Guard, including system requirement details, can be found at the following link:

https://technet.microsoft.com/itpro/windows/keep-secure/credential-guard

References:

1. CIS Recommendation: Turn On Virtualization Based Security
2. GRID: MS-00000297
3. Turn On Virtualization Based Security: Select Platform Security Level
4. GRID: MS-00000302

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.105 WN16-CC-000140 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.

```
GROUP ID:V-224924
RULE ID:SV-224924r991589
```

Rationale:

Compromised boot drivers can introduce malware prior to protection mechanisms that load after initialization. The Early Launch Antimalware driver can limit allowed drivers based on classifications determined by the malware protection application. At a minimum, drivers determined to be bad must not be allowed.

Audit:

The default behavior is for Early Launch Antimalware - Boot-Start Driver Initialization policy to enforce "Good, unknown and bad but critical" (preventing "bad").

If the registry value name below does not exist, this is not a finding.

If it exists and is configured with a value of "0x00000007 (7)", this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Policies\EarlyLaunch\

Value Name: DriverLoadPolicy

Value Type: REG_DWORD
Value: 0x00000001 (1), 0x00000003 (3), or 0x00000008 (8) (or if the Value
Name does not exist)
```

Possible values for this setting are:

- 8 - Good only
- 1 - Good and unknown
- 3 - Good, unknown and bad but critical
- 7 - All (which includes "bad" and would be a finding)

Remediation:

The default behavior is for Early Launch Antimalware - Boot-Start Driver Initialization policy to enforce "Good, unknown and bad but critical" (preventing "bad").

If this needs to be corrected or a more secure setting is desired, configure the policy value for

```
Computer Configuration >> Administrative Templates >> System >> Early Launch Antimalware >> "Boot-Start Driver Initialization Policy"
```

to "Not Configured" or "Enabled" with any option other than "All" selected.

References:

1. CIS Recommendation: Boot-Start Driver Initialization Policy
2. GRID: MS-00000311

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.106 WN16-CC-000150 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Group Policy objects must be reprocessed even if they have not changed.

```
GROUP ID:V-224925
RULE ID:SV-224925r991589
```

Rationale:

Registry entries for group policy settings can potentially be changed from the required configuration. This could occur as part of troubleshooting or by a malicious process on a compromised system. Enabling this setting and then selecting the "Process even if the Group Policy objects have not changed" option ensures 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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Group Policy\{35378EAC-
683F-11D2-A89A-00C04FBBCFA2}\

Value Name: NoGPOListChanges

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> System >> Group Policy
>> "Configure registry policy processing"
```

to "Enabled" with the option "Process even if the Group Policy objects have not changed" selected.

References:

1. CIS Recommendation: Configure registry policy processing: Process even if the Group Policy objects have not changed
2. GRID: MS-00000313

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.107 WN16-CC-000160 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Downloading print driver packages over HTTP must be prevented.

```
GROUP ID:V-224926
RULE ID:SV-224926r958478
```

Rationale:

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 will prevent uncontrolled updates to the system.

This setting prevents the computer from downloading print driver packages over HTTP.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows NT\Printers\

Value Name: DisableWebPnPDownload

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Turn off downloading of print drivers over HTTP
2. GRID: MS-00000319

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.108 WN16-CC-000170 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Printing over HTTP must be prevented.

```
GROUP ID:V-224927
RULE ID:SV-224927r958478
```

Rationale:

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 will prevent 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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows NT\Printers\

Value Name: DisableHTTPPrinting

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> System >> Internet
Communication Management >> Internet Communication settings >> "Turn off
printing over HTTP"
```

to "Enabled".

References:

1. CIS Recommendation: Turn off printing over HTTP
2. GRID: MS-00000324

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.109 WN16-CC-000180 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The network selection user interface (UI) must not be displayed on the logon screen.

```
GROUP ID:V-224928
RULE ID:SV-224928r958478
```

Rationale:

Enabling interaction with the network selection UI allows users to change connections to available networks without signing in to Windows.

Audit:

Verify the registry value below. If it does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\System\

Value Name: DontDisplayNetworkSelectionUI

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for```

Computer Configuration >> Administrative Templates >> System >> Logon >> "Do not display network selection UI"

```
 to "Enabled".
```

References:

1. CIS Recommendation: Do not display network selection UI
2. GRID: MS-00000346

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.110 WN16-CC-000210 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Users must be prompted to authenticate when the system wakes from sleep (on battery).

```
GROUP ID:V-224929
RULE ID:SV-224929r991589
```

Rationale:

A system that does not require authentication when resuming from sleep may provide access to unauthorized users. Authentication must always be required when accessing a system. This setting ensures users are prompted for a password when the system wakes from sleep (on battery).

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb-
100d-47d6-a2d5-f7d2daa51f51\

Value Name: DCSettingIndex

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Require a password when a computer wakes (on battery)
2. GRID: MS-00000357

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.111 WN16-CC-000220 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Users must be prompted to authenticate when the system wakes from sleep (plugged in).

```
GROUP ID:V-224930
RULE ID:SV-224930r991589
```

Rationale:

A system that does not require authentication when resuming from sleep may provide access to unauthorized users. Authentication must always be required when accessing a system. This setting ensures users are prompted for a password when the system wakes from sleep (plugged in).

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb-
100d-47d6-a2d5-f7d2daa51f51\

Value Name: ACSettingIndex

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Require a password when a computer wakes (plugged in)
2. GRID: MS-00000358

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.112 WN16-CC-000240 (Automated)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.

```
GROUP ID: V-224931
RULE ID: SV-224931r958478
```

Rationale:

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 will prevent uncontrolled updates to the system.

This setting will prevent the Program Inventory from collecting data about a system and sending the information to Microsoft.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\AppCompat\

Value Name: DisableInventory

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Application Compatibility >> "Turn off Inventory Collector"
```

to "Enabled".

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53A :: CM-7.1 (ii)
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a

1.113 WN16-CC-000250 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

AutoPlay must be turned off for non-volume devices.

```
GROUP ID: V-224932
RULE ID: SV-224932r958804
```

Rationale:

Allowing AutoPlay to execute may introduce malicious code to a system. AutoPlay begins reading from a drive as soon as media is inserted into 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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Explorer\

Value Name: NoAutoplayfornonVolume

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
AutoPlay Policies >> "Disallow Autoplay for non-volume devices"
```

to "Enabled".

References:

1. CIS Recommendation: Disallow Autoplay for non-volume devices
2. GRID: MS-00000374

Additional Information:

CCI-001764

Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.114 WN16-CC-000260 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

The default AutoRun behavior must be configured to prevent AutoRun commands.

```
GROUP ID: V-224933
RULE ID: SV-224933r958804
```

Rationale:

Allowing AutoRun commands to execute may introduce malicious code to a system. Configuring this setting prevents AutoRun commands from executing.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\

Value Name: NoAutorun

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
AutoPlay Policies >> "Set the default behavior for AutoRun"
```

to "Enabled" with "Do not execute any autorun commands" selected.

References:

1. CIS Recommendation: Set the default behavior for AutoRun
2. GRID: MS-00000375

Additional Information:

CCI-001764

Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.115 WN16-CC-000270 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

AutoPlay must be disabled for all drives.

```
GROUP ID: V-224934
RULE ID: SV-224934r958804
```

Rationale:

Allowing AutoPlay to execute may introduce malicious code to a system. AutoPlay begins reading from a drive as soon media is inserted into 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. Enabling this policy disables AutoPlay on all drives.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\

Value Name: NoDriveTypeAutoRun

Type: REG_DWORD
Value: 0x000000ff (255)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
AutoPlay Policies >> "Turn off AutoPlay"
```

to "Enabled" with "All Drives" selected.

References:

1. CIS Recommendation: Turn off AutoPlay
2. GRID: MS-00000376

Additional Information:

CCI-001764

Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.116 WN16-CC-000280 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Administrator accounts must not be enumerated during elevation.

```
GROUP ID: V-224935
RULE ID: SV-224935r958518
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\

Value Name: EnumerateAdministrators

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Credential User Interface >> "Enumerate administrator accounts on elevation"
```

to "Disabled".

References:

1. CIS Recommendation: Enumerate administrator accounts on elevation
2. GRID: MS-00000430

Additional Information:

CCI-001084

Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3

1.117 WN16-CC-000290 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Telemetry must be configured to Security or Basic.

```
GROUP ID: V-224936
RULE ID: SV-224936r991589
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\DataCollection\

Value Name: AllowTelemetry

Type: REG_DWORD
Value: 0x00000000 (0) (Security), 0x00000001 (1) (Basic)
```

Remediation:

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".

References:

1. CIS Recommendation: Allow Diagnostic Data
2. GRID: MS-00000432

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.118 WN16-CC-000300 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Application event log size must be configured to 32768 KB or greater.

```
GROUP ID: V-224937
RULE ID: SV-224937r958752
```

Rationale:

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.

Audit:

If the system is configured to write events directly to an audit server, this is NA.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\EventLog\Application\

Value Name: MaxSize

Type: REG_DWORD
Value: 0x00008000 (32768) (or greater)
```

Remediation:

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.

References:

1. CIS Recommendation: Application: Specify the maximum log file size (KB)
2. GRID: MS-00000446

Additional Information:

CCI-001849

Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4 :: AU-4
- NIST SP 800-53 Revision 5 :: AU-4

1.119 WN16-CC-000310 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Security event log size must be configured to 196608 KB or greater.

```
GROUP ID: V-224938
RULE ID: SV-224938r958752
```

Rationale:

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.

Audit:

If the system is configured to write events directly to an audit server, this is NA.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\EventLog\Security\

Value Name: MaxSize

Type: REG_DWORD
Value: 0x00030000 (196608) (or greater)
```

Remediation:

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 "196608" or greater.

References:

1. CIS Recommendation: Security: Specify the maximum log file size (KB)
2. GRID: MS-00000448

Additional Information:

CCI-001849

Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4 :: AU-4
- NIST SP 800-53 Revision 5 :: AU-4

1.120 WN16-CC-000320 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The System event log size must be configured to 32768 KB or greater.

```
GROUP ID: V-224939
RULE ID: SV-224939r958752
```

Rationale:

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.

Audit:

If the system is configured to write events directly to an audit server, this is NA.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\EventLog\System\

Value Name: MaxSize

Type: REG_DWORD
Value: 0x00008000 (32768) (or greater)
```

Remediation:

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
```

References:

1. CIS Recommendation: System: Specify the maximum log file size (KB)
2. GRID: MS-00000453

Additional Information:

CCI-001849

Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4 :: AU-4
- NIST SP 800-53 Revision 5 :: AU-4

1.121 WN16-CC-000330 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 Windows SmartScreen must be enabled.

```
GROUP ID: V-224940
RULE ID: SV-224940r958478
```

Rationale:

Windows SmartScreen helps protect systems from programs downloaded from the internet that may be malicious. Enabling SmartScreen will warn users of potentially malicious programs.

Audit:

This is applicable to unclassified systems; for other systems, this is NA.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\System\

Value Name: EnableSmartScreen

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
File Explorer >> "Configure Windows SmartScreen" to "Enabled"
```

References:

1. CIS Recommendation: Configure Windows Defender SmartScreen
2. GRID: MS-00000526

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53A :: CM-7.1 (ii)
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a

1.122 WN16-CC-000340 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Explorer Data Execution Prevention must be enabled.

```
GROUP ID: V-224941
RULE ID: SV-224941r958928
```

Rationale:

Data Execution Prevention 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.

Audit:

The default behavior is for Data Execution Prevention to be turned on for File Explorer.

If the registry value name below does not exist, this is not a finding.

If it exists and is configured with a value of "0", this is not a finding.

If it exists and is configured with a value of "1", this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Explorer\

Value Name: NoDataExecutionPrevention

Value Type: REG_DWORD
Value: 0x00000000 (0) (or if the Value Name does not exist)
```

Remediation:

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"
```

Additional Information:

CCI-002824

Implement organization-defined controls to protect the system memory from unauthorized code execution.

- NIST SP 800-53 Revision 4 :: SI-16
- NIST SP 800-53 Revision 5 :: SI-16

1.123 WN16-CC-000350 (Automated)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

Turning off File Explorer heap termination on corruption must be disabled.

```
GROUP ID: V-224942
RULE ID: SV-224942r991589
```

Rationale:

Legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Disabling this feature will prevent this.

Audit:

The default behavior is for File Explorer heap termination on corruption to be enabled.

If the registry Value Name below does not exist, this is not a finding.

If it exists and is configured with a value of "0", this is not a finding.

If it exists and is configured with a value of "1", this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Explorer\

Value Name: NoHeapTerminationOnCorruption

Value Type: REG_DWORD
Value: 0x00000000 (0) (or if the Value Name does not exist)
```

Remediation:

The default behavior is for File Explorer heap termination on corruption to be disabled.

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"
```

References:

1. CIS Recommendation: Turn off heap termination on corruption
2. GRID: MS-00000456

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.124 WN16-CC-000360 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

File Explorer shell protocol must run in protected mode.

```
GROUP ID: V-224943
RULE ID: SV-224943r991589
```

Rationale:

The shell protocol will limit the set of folders that 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.

Audit:

The default behavior is for shell protected mode to be turned on for File Explorer.

If the registry value name below does not exist, this is not a finding.

If it exists and is configured with a value of "0", this is not a finding.

If it exists and is configured with a value of "1", this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\

Value Name: PreXPSP2ShellProtocolBehavior

Value Type: REG_DWORD
Value: 0x00000000 (0) (or if the Value Name does not exist)
```

Remediation:

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"
```

References:

1. CIS Recommendation: Turn off shell protocol protected mode
2. GRID: MS-00000457

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.125 WN16-CC-000370 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Passwords must not be saved in the Remote Desktop Client.

```
GROUP ID: V-224944
RULE ID: SV-224944r1050790
```

Rationale:

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.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: DisablePasswordSaving

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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"
```

References:

1. CIS Recommendation: Do not allow passwords to be saved
2. GRID: MS-00000488

Additional Information:

CCI-002038

The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11
- NIST SP 800-53 Revision 5 :: IA-11

1.126 WN16-CC-000380 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Local drives must be prevented from sharing with Remote Desktop Session Hosts.

```
GROUP ID: V-224945
RULE ID: SV-224945r958524
```

Rationale:

Preventing users from sharing the local drives on their client computers with Remote Session Hosts that they access helps reduce possible exposure of sensitive data.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: fDisableCdm

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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"
```

References:

1. CIS Recommendation: Do not allow drive redirection
2. GRID: MS-00000493

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53A :: SC-4.1
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4

1.127 WN16-CC-000390 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Remote Desktop Services must always prompt a client for passwords upon connection.

```
GROUP ID: V-224946
RULE ID: SV-224946r1050790
```

Rationale:

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.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: fPromptForPassword

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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"
```

References:

1. CIS Recommendation: Always prompt for password upon connection
2. GRID: MS-00000498

Additional Information:

CCI-002038

The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11
- NIST SP 800-53 Revision 5 :: IA-11

1.128 WN16-CC-000400 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.

```
GROUP ID: V-224947
RULE ID: SV-224947r991554
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: fEncryptRPCTraffic

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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"
```

References:

1. CIS Recommendation: Require secure RPC communication
2. GRID: MS-00000499

Additional Information:

CCI-001453

Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)

1.129 WN16-CC-000410 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Remote Desktop Services must be configured with the client connection encryption set to High Level.

```
GROUP ID: V-224948
RULE ID: SV-224948r991554
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\

Value Name: MinEncryptionLevel

Type: REG_DWORD
Value: 0x00000003 (3)
```

Remediation:

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" with "High Level" selected
```

References:

1. CIS Recommendation: Set client connection encryption level
2. GRID: MS-00000502

Additional Information:

CCI-001453

Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)

1.130 WN16-CC-000420 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Attachments must be prevented from being downloaded from RSS feeds.

```
GROUP ID: V-224949
RULE ID: SV-224949r991589
```

Rationale:

Attachments from RSS feeds may not be secure. This setting will prevent attachments from being downloaded from RSS feeds.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Internet Explorer\Feeds\

Value Name: DisableEnclosureDownload

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
RSS Feeds >> "Prevent downloading of enclosures" to "Enabled"
```

References:

1. CIS Recommendation: Prevent downloading of enclosures
2. GRID: MS-00000507

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.131 WN16-CC-000421 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Windows Explorer Preview pane must be disabled for Windows Server 2016.

```
GROUP ID: V-236000
RULE ID: SV-236000r958478
```

Rationale:

A known vulnerability in Windows could allow the execution of malicious code by either opening a compromised document or viewing it in the Windows Preview pane.

Organizations must disable the Windows Preview pane and Windows Detail pane.

Audit:

If the following registry values do not exist or are not configured as specified, this is a finding:

```
Registry Hive: HKEY_CURRENT_USER
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

Value Name: NoPreviewPane

Value Type: REG_DWORD

Value: 1
```

Remediation:

Ensure the following settings are configured for Windows Server 2016 locally or applied through group policy.

Configure the policy value for

```
User Configuration >> Administrative Templates >> Windows Components >> File
Explorer >> Explorer Frame Pane "Turn off Preview Pane
```

to "Enabled".

Configure the policy value for

```
User Configuration >> Administrative Templates >> Windows Components >> File
Explorer >> Explorer Frame Pane "Turn on or off details pane"
```

to "Enabled" and "Configure details pane" to "Always hide".

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.132 WN16-CC-000430 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Basic authentication for RSS feeds over HTTP must not be used.

```
GROUP ID: V-224951
RULE ID: SV-224951r958478
```

Rationale:

Basic authentication uses plain-text passwords that could be used to compromise a system. Disabling Basic authentication will reduce this potential.

Audit:

The default behavior is for the Windows RSS platform to not use Basic authentication over HTTP connections.

If the registry value name below does not exist, this is not a finding.

If it exists and is configured with a value of "0", this is not a finding.

If it exists and is configured with a value of "1", this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Internet Explorer\Feeds\

Value Name: AllowBasicAuthInClear

Value Type: REG_DWORD
Value: 0x00000000 (0) (or if the Value Name does not exist)
```

Remediation:

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"
```

References:

1. CIS Recommendation: Turn on Basic feed authentication over HTTP
2. GRID: MS-00000593

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53A :: CM-7.1 (ii)
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a

1.133 WN16-CC-000440 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Indexing of encrypted files must be turned off.

```
GROUP ID: V-224952
RULE ID: SV-224952r958478
```

Rationale:

Indexing of encrypted files may expose sensitive data. This setting prevents encrypted files from being indexed.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Search\

Value Name: AllowIndexingEncryptedStoresOrItems

Value Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Search >> "Allow indexing of encrypted files" to "Disabled"
```

References:

1. CIS Recommendation: Allow indexing of encrypted files
2. GRID: MS-00000511

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53A :: CM-7.1 (ii)
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a

1.134 WN16-CC-000450 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Users must be prevented from changing installation options.

```
GROUP ID: V-224953
RULE ID: SV-224953r982210
```

Rationale:

Installation options for applications are typically controlled by administrators. This setting prevents users from changing installation options that may bypass security features.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Installer\

Value Name: EnableUserControl

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Windows Installer >> "Allow user control over installs" to "Disabled"
```

References:

1. CIS Recommendation: Allow user control over installs
2. GRID: MS-00000531

Additional Information:

CCI-001812

The information system prohibits user installation of software without explicit privileged status.

- NIST SP 800-53 Revision 4 :: CM-11 (2)

1.135 WN16-CC-000460 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

The Windows Installer Always install with elevated privileges option must be disabled.

```
GROUP ID: V-224954
RULE ID: SV-224954r982210
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Installer\

Value Name: AlwaysInstallElevated

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Windows Installer >> "Always install with elevated privileges" to "Disabled"
```

References:

1. CIS Recommendation: Always install with elevated privileges
2. GRID: MS-00000532

Additional Information:

CCI-001812

The information system prohibits user installation of software without explicit privileged status.

- NIST SP 800-53 Revision 4 :: CM-11 (2)

1.136 WN16-CC-000470 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Users must be notified if a web-based program attempts to install software.

```
GROUP ID: V-224955
RULE ID: SV-224955r991589
```

Rationale:

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.

Audit:

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 the registry value name below does not exist, this is not a finding.

If it exists and is configured with a value of "0", this is not a finding.

If it exists and is configured with a value of "1", this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Installer\

Value Name: SafeForScripting

Value Type: REG_DWORD
Value: 0x00000000 (0) (or if the Value Name does not exist)
```

Remediation:

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"
```

References:

1. CIS Recommendation: Prevent Internet Explorer security prompt for Windows Installer scripts
2. GRID: MS-00000533

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.137 WN16-CC-000480 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Automatically signing in the last interactive user after a system-initiated restart must be disabled.

```
GROUP ID: V-224956
RULE ID: SV-224956r991591
```

Rationale:

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.

Audit:

Verify the registry value below. If it does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: DisableAutomaticRestartSignOn

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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"
```

References:

1. CIS Recommendation: Sign-in last interactive user automatically after a system-initiated restart
2. GRID: MS-00000535

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.138 WN16-CC-000490 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

PowerShell script block logging must be enabled.

```
GROUP ID: V-224957
RULE ID: SV-224957r958422
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\
Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\

Value Name: EnableScriptBlockLogging

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Windows PowerShell >> "Turn on PowerShell Script Block Logging" to "Enabled"
```

References:

1. CIS Recommendation: Turn on PowerShell Script Block Logging
2. GRID: MS-00000536

Additional Information:

CCI-000135

Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)

1.139 WN16-CC-000500 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

The Windows Remote Management (WinRM) client must not use Basic authentication.

```
GROUP ID: V-224958
RULE ID: SV-224958r958510
```

Rationale:

Basic authentication uses plain-text passwords that could be used to compromise a system. Disabling Basic authentication will reduce this potential.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\WinRM\Client\

Value Name: AllowBasic

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Windows Remote Management (WinRM) >> WinRM Client >> "Allow Basic
authentication" to "Disabled"
```

References:

1. CIS Recommendation: Allow Basic authentication
2. GRID: MS-00000538

Additional Information:

CCI-000877

Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 :: MA-4 c
- NIST SP 800-53A :: MA-4.1 (iv)
- NIST SP 800-53 Revision 4 :: MA-4 c
- NIST SP 800-53 Revision 5 :: MA-4 c

1.140 WN16-CC-000510 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Windows Remote Management (WinRM) client must not allow unencrypted traffic.

```
GROUP ID: V-224959
RULE ID: SV-224959r958848
```

Rationale:

Unencrypted remote access to a system can allow sensitive information to be compromised. Windows remote management connections must be encrypted to prevent this.

Satisfies: SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\WinRM\Client\

Value Name: AllowUnencryptedTraffic

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Windows Remote Management (WinRM) >> WinRM Client >> "Allow unencrypted
traffic" to "Disabled"
```

References:

1. CIS Recommendation: Allow unencrypted traffic
2. GRID: MS-00000539

Additional Information:

CCI-002890

Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

CCI-003123

Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

1.141 WN16-CC-000520 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Windows Remote Management (WinRM) client must not use Digest authentication.

```
GROUP ID: V-224960
RULE ID: SV-224960r958510
```

Rationale:

Digest authentication is not as strong as other options and may be subject to man-in-the-middle attacks. Disallowing Digest authentication will reduce this potential.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\WinRM\Client\

Value Name: AllowDigest

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Windows Remote Management (WinRM) >> WinRM Client >> "Disallow Digest
authentication" to "Enabled"
```

References:

1. CIS Recommendation: Disallow Digest authentication
2. GRID: MS-00000540

Additional Information:

CCI-000877

Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 :: MA-4 c
- NIST SP 800-53A :: MA-4.1 (iv)
- NIST SP 800-53 Revision 4 :: MA-4 c
- NIST SP 800-53 Revision 5 :: MA-4 c

1.142 WN16-CC-000530 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

The Windows Remote Management (WinRM) service must not use Basic authentication.

```
GROUP ID: V-224961
RULE ID: SV-224961r958510
```

Rationale:

Basic authentication uses plain-text passwords that could be used to compromise a system. Disabling Basic authentication will reduce this potential.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\

Value Name: AllowBasic

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Windows Remote Management (WinRM) >> WinRM Service >> "Allow Basic
authentication" to "Disabled".
```

References:

1. CIS Recommendation: Allow Basic authentication
2. GRID: MS-00000541

Additional Information:

CCI-000877

Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 :: MA-4 c
- NIST SP 800-53A :: MA-4.1 (iv)
- NIST SP 800-53 Revision 4 :: MA-4 c
- NIST SP 800-53 Revision 5 :: MA-4 c

1.143 WN16-CC-000540 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Windows Remote Management (WinRM) service must not allow unencrypted traffic.

```
GROUP ID: V-224962
RULE ID: SV-224962r958848
```

Rationale:

Unencrypted remote access to a system can allow sensitive information to be compromised. Windows remote management connections must be encrypted to prevent this.

Satisfies: SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\

Value Name: AllowUnencryptedTraffic

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> Windows Components >>
Windows Remote Management (WinRM) >> WinRM Service >> "Allow unencrypted
traffic" to "Disabled".
```

References:

1. CIS Recommendation: Allow unencrypted traffic
2. GRID: MS-00000543

Additional Information:

CCI-002890

Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

CCI-003123

Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

1.144 WN16-CC-000550 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Windows Remote Management (WinRM) service must not store RunAs credentials.

```
GROUP ID: V-224963
RULE ID: SV-224963r1050790
```

Rationale:

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.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\

Value Name: DisableRunAs

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".
```

References:

1. CIS Recommendation: Disallow WinRM from storing RunAs credentials
2. GRID: MS-00000544

Additional Information:

CCI-002038

The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11
- NIST SP 800-53 Revision 5 :: IA-11

1.145 WN16-CC-000555 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must have PowerShell Transcription enabled.

```
GROUP ID: V-257502
RULE ID: SV-257502r958420
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding:

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription\

Value Name: EnableTranscripting

Value Type: REG_DWORD
Value: 1
```

Remediation:

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.

References:

1. CIS Recommendation: Turn on PowerShell Transcription
2. GRID: MS-00000537

Additional Information:

CCI-000134

Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53A :: AU-3.1
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 e

1.146 WN16-DC-000010 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I

Description:

Only administrators responsible for the domain controller must have Administrator rights on the system.

```
GROUP ID: V-224964
RULE ID: SV-224964r958726
```

Rationale:

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 using only accounts with the minimum level of authority necessary.

Standard user accounts must not be members of the built-in Administrators group.

Audit:

This applies to domain controllers. A separate version applies to other systems.

Review the Administrators group. Only the appropriate administrator groups or accounts responsible for administration of the system may be members of the group.

Standard user accounts must not be members of the local administrator group.

If prohibited accounts are members of the local administrators group, this is a finding.

If the built-in Administrator account or other required administrative accounts are found on the system, this is not a finding.

Remediation:

Configure the Administrators group to include only administrator groups or accounts that are responsible for the system.

Remove any standard user accounts.

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.147 WN16-DC-000020 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Kerberos user logon restrictions must be enforced.

```
GROUP ID: V-224965
RULE ID: SV-224965r958494
```

Rationale:

This policy setting determines whether the Kerberos Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the target computer. The policy is enabled by default, which is the most secure setting for validating that access to target resources is not circumvented.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Audit:

This applies to domain controllers. It is NA for other systems.

Verify the following is configured in the Default Domain Policy.

Open "Group Policy Management".

Navigate to "Group Policy Objects" in the Domain being reviewed (Forest >> Domains >> Domain).

Right-click on the "Default Domain Policy".

Select "Edit".

Navigate to Computer Configuration >> Policies >> Windows Settings >> Security Settings >> Account Policies >> Kerberos Policy.

If the "Enforce user logon restrictions" is not set to "Enabled", this is a finding.

Remediation:

Configure the policy value in the Default Domain Policy for

```
Computer Configuration >> Policies >> Windows Settings >> Security Settings
>> Account Policies >> Kerberos Policy >> "Enforce user logon restrictions"
```

to "Enabled".

Additional Information:

CCI-001941

Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (8)
- NIST SP 800-53 Revision 5 :: IA-2 (8)

CCI-001942

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (9)

1.148 WN16-DC-000030 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.

```
GROUP ID: V-224966
RULE ID: SV-224966r958494
```

Rationale:

This setting determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service. Session tickets are used only to authenticate new connections with servers. Ongoing operations are not interrupted if the session ticket used to authenticate the connection expires during the connection.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Audit:

This applies to domain controllers. It is NA for other systems.

Verify the following is configured in the Default Domain Policy.

Open "Group Policy Management".

Navigate to "Group Policy Objects" in the Domain being reviewed (Forest >> Domains >> Domain).

Right-click on the "Default Domain Policy".

Select "Edit".

Navigate to Computer Configuration >> Policies >> Windows Settings >> Security Settings >> Account Policies >> Kerberos Policy.

If the value for "Maximum lifetime for service ticket" is "0" or greater than "600" minutes, this is a finding.

Remediation:

Configure the policy value in the Default Domain Policy for

```
Computer Configuration >> Policies >> Windows Settings >> Security Settings
>> Account Policies >> Kerberos Policy >> "Maximum lifetime for service
ticket"
```

to a maximum of "600" minutes, but not "0", which equates to "Ticket doesn't expire".

Additional Information:

CCI-001941

Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (8)
- NIST SP 800-53 Revision 5 :: IA-2 (8)

CCI-001942

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (9)

1.149 WN16-DC-000040 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Kerberos user ticket lifetime must be limited to 10 hours or less.

```
GROUP ID: V-224967
RULE ID: SV-224967r958494
```

Rationale:

In Kerberos, there are two types of tickets: Ticket Granting Tickets (TGTs) and Service Tickets. Kerberos tickets have a limited lifetime so the time an attacker has to implement an attack is limited. This policy controls how long TGTs can be renewed. With Kerberos, the user's initial authentication to the domain controller results in a TGT, which is then used to request Service Tickets to resources. Upon startup, each computer gets a TGT before requesting a service ticket to the domain controller and any other computers it needs to access. For services that start up under a specified user account, users must always get a TGT first and then get Service Tickets to all computers and services accessed.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Audit:

This applies to domain controllers. It is NA for other systems.

Verify the following is configured in the Default Domain Policy.

Open "Group Policy Management".

Navigate to "Group Policy Objects" in the Domain being reviewed (Forest >> Domains >> Domain).

Right-click on the "Default Domain Policy".

Select "Edit".

Navigate to

```
Computer Configuration >> Policies >> Windows Settings >> Security Settings
>> Account Policies >> Kerberos Policy
```

If the value for "Maximum lifetime for user ticket" is "0" or greater than "10" hours, this is a finding.

Remediation:

Configure the policy value in the Default Domain Policy for

```
Computer Configuration >> Policies >> Windows Settings >> Security Settings
>> Account Policies >> Kerberos Policy >> "Maximum lifetime for user ticket"
```

to a maximum of "10" hours but not "0", which equates to "Ticket doesn't expire".

Additional Information:

CCI-001941

Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (8)
- NIST SP 800-53 Revision 5 :: IA-2 (8)

CCI-001942

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (9)

1.150 WN16-DC-000050 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.

```
GROUP ID: V-224968
RULE ID: SV-224968r958494
```

Rationale:

This setting determines the period of time (in days) during which a user's Ticket Granting Ticket (TGT) may be renewed. This security configuration limits the amount of time an attacker has to crack the TGT and gain access.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Audit:

This applies to domain controllers. It is NA for other systems.

Verify the following is configured in the Default Domain Policy.

Open "Group Policy Management".

Navigate to "Group Policy Objects" in the Domain being reviewed (Forest >> Domains >> Domain).

Right-click on the "Default Domain Policy".

Select "Edit".

Navigate to

```
Computer Configuration >> Policies >> Windows Settings >> Security Settings
>> Account Policies >> Kerberos Policy
```

If the "Maximum lifetime for user ticket renewal" is greater than "7" days, this is a finding.

Remediation:

Configure the policy value in the Default Domain Policy for

```
Computer Configuration >> Policies >> Windows Settings >> Security Settings
>> Account Policies >> Kerberos Policy >> "Maximum lifetime for user ticket
renewal"
```

to a maximum of "7" days or less.

Additional Information:

CCI-001941

Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (8)
- NIST SP 800-53 Revision 5 :: IA-2 (8)

CCI-001942

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (9)

1.151 WN16-DC-000060 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The computer clock synchronization tolerance must be limited to 5 minutes or less.

```
GROUP ID: V-224969
RULE ID: SV-224969r958494
```

Rationale:

This setting determines the maximum time difference (in minutes) that Kerberos will tolerate between the time on a client's clock and the time on a server's clock while still considering the two clocks synchronous. In order to prevent replay attacks, Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in sync as much as possible.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Audit:

This applies to domain controllers. It is NA for other systems.

Verify the following is configured in the Default Domain Policy.

Open "Group Policy Management".

Navigate to "Group Policy Objects" in the Domain being reviewed (Forest >> Domains >> Domain).

Right-click on the "Default Domain Policy".

Select "Edit".

Navigate to

```
Computer Configuration >> Policies >> Windows Settings >> Security Settings
>> Account Policies >> Kerberos Policy
```

If the "Maximum tolerance for computer clock synchronization" is greater than "5" minutes, this is a finding.

Remediation:

Configure the policy value in the Default Domain Policy for

```
Computer Configuration >> Windows Settings >> Security Settings >> Account
Policies >> Kerberos Policy >> "Maximum tolerance for computer clock
synchronization"
```

to a maximum of "5" minutes or less.

Additional Information:

CCI-001941

Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (8)
- NIST SP 800-53 Revision 5 :: IA-2 (8)

CCI-001942

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (9)

1.152 WN16-DC-000070 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I

Description:

Permissions on the Active Directory data files must only allow System and Administrators access.

```
GROUP ID: V-224970
RULE ID: SV-224970r958726
```

Rationale:

Improper access permissions for directory data-related files could allow unauthorized users to read, modify, or delete directory data or audit trails.

Audit:

This applies to domain controllers. It is NA for other systems.

Run "Regedit".

Navigate to

```
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters"
```

Note the directory locations in the values for:

Database log files path

DSA Database file

By default, they will be \Windows\NTDS.

If the locations are different, the following will need to be run for each.

Open "Command Prompt (Admin)".

Navigate to the NTDS directory (\Windows\NTDS by default).

Run "icacls .".

If the permissions on each file are not as restrictive as the following, this is a finding.

- NT AUTHORITY\SYSTEM:(I)(F)
- BUILTIN\Administrators:(I)(F)

(I) - permission inherited from parent container
(F) - full access

Remediation:

Maintain the permissions on NTDS database and log files as follows:

- NT AUTHORITY\SYSTEM:(I)(F)
- BUILTIN\Administrators:(I)(F)

(I) - permission inherited from parent container
(F) - full access

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.153 WN16-DC-000080 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I

Description:

The Active Directory SYSVOL directory must have the proper access control permissions.

```
GROUP ID: V-224971
RULE ID: SV-224971r958726
```

Rationale:

Improper access permissions for directory data files could allow unauthorized users to read, modify, or delete directory data.

The SYSVOL directory contains public files (to the domain) such as policies and logon scripts. Data in shared subdirectories are replicated to all domain controllers in a domain.

Audit:

This applies to domain controllers. It is NA for other systems.

Open a command prompt.

Run "net share".

Make note of the directory location of the SYSVOL share.

By default, this will be \Windows\SYSVOL\sysvol. For this requirement, permissions will be verified at the first SYSVOL directory level.

If any standard user accounts or groups have greater than "Read & execute" permissions, this is a finding.

The default permissions noted below meet this requirement.

Open "Command Prompt".

Run "icacls c:\Windows\SYSVOL".

The following results should be displayed:

- NT AUTHORITY\Authenticated Users:(RX)
- NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(GR,GE)
- BUILTIN\Server Operators:(RX)
- BUILTIN\Server Operators:(OI)(CI)(IO)(GR,GE)
- BUILTIN\Administrators:(M,WDAC,WO)
- BUILTIN\Administrators:(OI)(CI)(IO)(F)
- NT AUTHORITY\SYSTEM:(F)
- NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
- BUILTIN\Administrators:(M,WDAC,WO)
- CREATOR OWNER:(OI)(CI)(IO)(F)

(RX) - Read & execute
Run "icacls /help" to view definitions of other permission codes.

Remediation:

Maintain the permissions on the SYSVOL directory. Do not allow greater than "Read & execute" permissions for standard user accounts or groups. The defaults below meet this requirement.

C:\Windows\SYSVOL

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

- Authenticated Users - Read & execute - This folder, subfolder, and files
- Server Operators - Read & execute- This folder, subfolder, and files
- Administrators - Special - This folder only (Special = Basic Permissions: all selected except Full control)
- CREATOR OWNER - Full control - Subfolders and files only
- Administrators - Full control - Subfolders and files only
- SYSTEM - Full control - This folder, subfolders, and files

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.154 WN16-DC-000090 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I

Description:

Active Directory Group Policy objects must have proper access control permissions.

```
GROUP ID: V-224972
RULE ID: SV-224972r958726
```

Rationale:

When directory service database objects do not have appropriate access control permissions, it may be possible for malicious users to create, read, update, or delete the objects and degrade or destroy the integrity of the data. When the directory service is used for identification, authentication, or authorization functions, a compromise of the database objects could lead to a compromise of all systems relying on the directory service.

For Active Directory (AD), the Group Policy objects require special attention. In a distributed administration model (i.e., help desk), Group Policy objects are more likely to have access permissions changed from the secure defaults. If inappropriate access permissions are defined for Group Policy objects, this could allow an intruder to change the security policy applied to all domain client computers (workstations and servers).

Audit:

This applies to domain controllers. It is NA for other systems.

Review the permissions on Group Policy objects.

Open "Group Policy Management" (available from various menus or run "gpmc.msc").

Navigate to "Group Policy Objects" in the domain being reviewed (Forest >> Domains >> Domain).

For each Group Policy object:

Select the Group Policy object item in the left pane.

Select the "Delegation" tab in the right pane.

Select the "Advanced" button.

Select each Group or user name.

View the permissions.

If any standard user accounts or groups have "Allow" permissions greater than "Read" and "Apply group policy", this is a finding.

Other access permissions that allow the objects to be updated are considered findings unless specifically documented by the ISSO.

The default permissions noted below satisfy this requirement.

The permissions shown are at the summary level. More detailed permissions can be viewed by selecting the next "Advanced" button, the desired Permission entry, and the "Edit" button.

Authenticated Users - Read, Apply group policy, Special permissions

The special permissions for Authenticated Users are for Read-type Properties. If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties, this is a finding.

The special permissions for the following default groups are not the focus of this requirement and may include a wide range of permissions and properties.

- CREATOR OWNER - Special permissions
- SYSTEM - Read, Write, Create all child objects, Delete all child objects, Special permissions
- Domain Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions
- Enterprise Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions
- ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

The Domain Admins and Enterprise Admins will not have the "Delete all child objects" permission on the two default Group Policy objects: Default Domain Policy and Default Domain Controllers Policy. They will have this permission on organization created Group Policy objects.

Remediation:

Maintain the permissions on Group Policy objects to not allow greater than "Read" and "Apply group policy" for standard user accounts or groups. The default permissions below meet this requirement.

Authenticated Users - Read, Apply group policy, Special permissions

The special permissions for Authenticated Users are for Read-type Properties.

- CREATOR OWNER - Special permissions
- SYSTEM - Read, Write, Create all child objects, Delete all child objects, Special permissions
- Domain Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions
- Enterprise Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions
- ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

Document any other access permissions that allow the objects to be updated with the ISSO.
The Domain Admins and Enterprise Admins will not have the "Delete all child objects" permission on the two default Group Policy objects: Default Domain Policy and Default Domain Controllers Policy. They will have this permission on created Group Policy objects.

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.155 WN16-DC-000100 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I

Description:

The Active Directory Domain Controllers Organizational Unit (OU) object must have the proper access control permissions.

```
GROUP ID: V-224973
RULE ID: SV-224973r958726
```

Rationale:

When Active Directory objects do not have appropriate access control permissions, it may be possible for malicious users to create, read, update, or delete the objects and degrade or destroy the integrity of the data. When the directory service is used for identification, authentication, or authorization functions, a compromise of the database objects could lead to a compromise of all systems that rely on the directory service.

The Domain Controllers OU object requires special attention as the Domain Controllers are central to the configuration and management of the domain. Inappropriate access permissions defined for the Domain Controllers OU could allow an intruder or unauthorized personnel to make changes that could lead to the compromise of the domain.

Audit:

This applies to domain controllers. It is NA for other systems.

Review the permissions on the Domain Controllers OU.

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Select "Advanced Features" in the "View" menu if not previously selected.

Select the "Domain Controllers" OU (folder in folder icon).

Right-click and select "Properties".

Select the "Security" tab.

If the permissions on the Domain Controllers OU do not restrict changes to System, Domain Admins, Enterprise Admins and Administrators, this is a finding.

The default permissions listed below satisfy this requirement.

Domains supporting Microsoft Exchange will have additional Exchange related permissions on the Domain Controllers OU. These may include some change related permissions and are not a finding.

The permissions shown are at the summary level. More detailed permissions can be viewed by selecting the "Advanced" button, the desired Permission entry, and the "View" or "Edit" button.

Except where noted otherwise, the special permissions may include a wide range of permissions and properties and are acceptable for this requirement.

- CREATOR OWNER - Special permissions
- SELF - Special permissions
- Authenticated Users - Read, Special permissions

The special permissions for Authenticated Users are Read types.
If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties, this is a finding.
SYSTEM - Full Control
Domain Admins - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions

- Enterprise Admins - Full Control
- Key Admins - Special permissions
- Enterprise Key Admins - Special permissions
- Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions
- Pre-Windows 2000 Compatible Access - Special permissions

The Special permissions for Pre-Windows 2000 Compatible Access are Read types.
If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties, this is a finding.
ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

Remediation:

Limit the permissions on the Domain Controllers OU to restrict changes to System, Domain Admins, Enterprise Admins and Administrators.

The default permissions listed below satisfy this requirement.

Domains supporting Microsoft Exchange will have additional Exchange related permissions on the Domain Controllers OU. These may include some change related permissions.

- CREATOR OWNER - Special permissions
- SELF - Special permissions
- Authenticated Users - Read, Special permissions

The special permissions for Authenticated Users are Read types.

- SYSTEM - Full Control
- Domain Admins - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions
- Enterprise Admins - Full Control
- Key Admins - Special permissions
- Enterprise Key Admins - Special permissions
- Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions
- Pre-Windows 2000 Compatible Access - Special permissions
- The special permissions for Pre-Windows 2000 Compatible Access are Read types.
- ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.156 WN16-DC-000110 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I

Description:

Domain-created Active Directory Organizational Unit (OU) objects must have proper access control permissions.

```
GROUP ID: V-224974
RULE ID: SV-224974r958726
```

Rationale:

When directory service database objects do not have appropriate access control permissions, it may be possible for malicious users to create, read, update, or delete the objects and degrade or destroy the integrity of the data. When the directory service is used for identification, authentication, or authorization functions, a compromise of the database objects could lead to a compromise of all systems that rely on the directory service.

For Active Directory, the OU objects require special attention. In a distributed administration model (i.e., help desk), OU objects are more likely to have access permissions changed from the secure defaults. If inappropriate access permissions are defined for OU objects, it could allow an intruder to add or delete users in the OU. This could result in unauthorized access to data or a denial of service to authorized users.

Audit:

This applies to domain controllers. It is NA for other systems.

Review the permissions on domain-defined OUs.

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

For each OU that is defined (folder in folder icon) excluding the Domain Controllers OU:

Right-click the OU and select "Properties".

Select the "Security" tab.

If the permissions on the OU are not at least as restrictive as those below, this is a finding.

The permissions shown are at the summary level. More detailed permissions can be viewed by selecting the "Advanced" button, the desired Permission entry, and the "Edit" or "View" button.

Except where noted otherwise, the special permissions may include a wide range of permissions and properties and are acceptable for this requirement.

CREATOR OWNER - Special permissions

Self - Special permissions

Authenticated Users - Read, Special permissions

The Special permissions for Authenticated Users are Read type. If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties, this is a finding.

- SYSTEM - Full Control
- Domain Admins - Full Control
- Enterprise Admins - Full Control
- Key Admins - Special permissions
- Enterprise Key Admins - Special permissions
- Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions
- Pre-Windows 2000 Compatible Access - Special permissions

The Special permissions for Pre-Windows 2000 Compatible Access are for Read types. If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties, this is a finding.
ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions
If an ISSO-approved distributed administration model (help desk or other user support staff) is implemented, permissions above Read may be allowed for groups documented by the ISSO.

If any OU with improper permissions includes identification or authentication data (e.g., accounts, passwords, or password hash data) used by systems to determine access control, the severity is CAT I (e.g., OUs that include user accounts, including service/application accounts).
If an OU with improper permissions does not include identification and authentication data used by systems to determine access control, the severity is CAT II (e.g., Workstation, Printer OUs).

Remediation:

Maintain the permissions on domain-defined OUs to be at least as restrictive as the defaults below.

Document any additional permissions above Read with the ISSO if an approved distributed administration model (help desk or other user support staff) is implemented.

- CREATOR OWNER - Special permissions
- Self - Special permissions
- Authenticated Users - Read, Special permissions
- The special permissions for Authenticated Users are Read type.
- SYSTEM - Full Control
- Domain Admins - Full Control
- Enterprise Admins - Full Control
- Key Admins - Special permissions
- Enterprise Key Admins - Special permissions
- Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions
- Pre-Windows 2000 Compatible Access - Special permissions
- The special permissions for Pre-Windows 2000 Compatible Access are for Read types.
- ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.157 WN16-DC-000120 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Data files owned by users must be on a different logical partition from the directory server data files.

```
GROUP ID: V-224975
RULE ID: SV-224975r958524
```

Rationale:

When directory service data files, especially for directories used for identification, authentication, or authorization, reside on the same logical partition as user-owned files, the directory service data may be more vulnerable to unauthorized access or other availability compromises. Directory service and user-owned data files sharing a partition may be configured with less restrictive permissions in order to allow access to the user data.

The directory service may be vulnerable to a denial of service attack when user-owned files on a common partition are expanded to an extent preventing the directory service from acquiring more space for directory or audit data.

Audit:

This applies to domain controllers. It is NA for other systems.

Run "Regedit".

Navigate to

```
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters"
```

Note the directory locations in the values for "DSA Database file".

Open "Command Prompt".

Enter

```
"net share"
```

Note the logical drive(s) or file system partition for any organization-created data shares.

Ignore system shares (e.g., NETLOGON, SYSVOL, and administrative shares ending in $). User shares that are hidden (ending with $) should not be ignored.

If user shares are located on the same logical partition as the directory server data files, this is a finding.

Remediation:

Move shares used to store files owned by users to a different logical partition than the directory server data files.

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53A :: SC-4.1
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4

1.158 WN16-DC-000130 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Domain controllers must run on a machine dedicated to that function.

```
GROUP ID: V-224976
RULE ID: SV-224976r958478
```

Rationale:

Executing application servers on the same host machine with a directory server may substantially weaken the security of the directory server. Web or database server applications usually require the addition of many programs and accounts, increasing the attack surface of the computer.

Some applications require the addition of privileged accounts, providing potential sources of compromise. Some applications (such as Microsoft Exchange) may require the use of network ports or services conflicting with the directory server. In this case, non-standard ports might be selected, and this could interfere with intrusion detection or prevention services.

Audit:

This applies to domain controllers, It is NA for other systems.

Review the installed roles the domain controller is supporting.

Start "Server Manager".

Select "AD DS" in the left pane and the server name under "Servers" to the right.

Select "Add (or Remove) Roles and Features" from "Tasks" in the "Roles and Features" section. (Cancel before any changes are made.)

Determine if any additional server roles are installed. A basic domain controller setup will include the following:

- Active Directory Domain Services
- DNS Server
- File and Storage Services

If any roles not requiring installation on a domain controller are installed, this is a finding.
A Domain Name System (DNS) server integrated with the directory server (e.g., AD-integrated DNS) is an acceptable application. However, the DNS server must comply with the DNS STIG security requirements.
Run "Programs and Features".
Review installed applications.
If any applications are installed that are not required for the domain controller, this is a finding.

Remediation:

Remove additional roles or applications such as web, database, and email from the domain controller.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53A :: CM-7.1 (ii)
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a

1.159 WN16-DC-000140 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Separate, NSA-approved (Type 1) cryptography must be used to protect the directory data in transit for directory service implementations at a classified confidentiality level when replication data traverses a network cleared to a lower level than the data.

```
GROUP ID: V-224977
RULE ID: SV-224977r987791
```

Rationale:

Directory data that is not appropriately encrypted is subject to compromise. Commercial-grade encryption does not provide adequate protection when the classification level of directory data in transit is higher than the level of the network.

Audit:

This applies to domain controllers. It is NA for other systems.

Review the organization network diagram(s) or documentation to determine the level of classification for the network(s) over which replication data is transmitted.

Determine the classification level of the Windows domain controller.

If the classification level of the Windows domain controller is higher than the level of the networks, review the organization network diagram(s) and directory implementation documentation to determine if NSA-approved encryption is used to protect the replication network traffic.

If the classification level of the Windows domain controller is higher than the level of the network traversed and NSA-approved encryption is not used, this is a finding.

Remediation:

Configure NSA-approved (Type 1) cryptography to protect the directory data in transit for directory service implementations at a classified confidentiality level that transfer replication data through a network cleared to a lower level than the data.

Additional Information:

CCI-002450

Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4 :: SC-13
- NIST SP 800-53 Revision 5 :: SC-13 b

1.160 WN16-DC-000150 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I

Description:

Directory data (outside the root DSE) of a non-public directory must be configured to prevent anonymous access.

```
GROUP ID: V-224978
RULE ID: SV-224978r991589
```

Rationale:

To the extent that anonymous access to directory data (outside the root DSE) is permitted, read access control of the data is effectively disabled. If other means of controlling access (such as network restrictions) are compromised, there may be nothing else to protect the confidentiality of sensitive directory data.

Audit:

This applies to domain controllers. It is NA for other systems.

Open "Command Prompt" (not elevated).

Run "ldp.exe".

From the "Connection menu", select "Bind".

Clear the User, Password, and Domain fields.

Select "Simple bind" for the Bind type and click "OK".

Confirmation of anonymous access will be displayed at the end:

res = ldap_simple_bind_s

Authenticated as: 'NT AUTHORITY\ANONYMOUS LOGON'

From the "Browse" menu, select "Search".

In the Search dialog, enter the DN of the domain naming context (generally something like "dc=disaost,dc=mil") in the Base DN field.

Clear the Attributes field and select "Run".

Error messages should display related to Bind and user not authenticated.

If attribute data is displayed, anonymous access is enabled to the domain naming context and this is a finding.

The following network controls allow the finding severity to be downgraded to a CAT II since these measures lower the risk associated with anonymous access.

Network hardware ports at the site are subject to 802.1x authentication or MAC address restrictions.

Premise firewall or host restrictions prevent access to ports 389, 636, 3268, and 3269 from client hosts not explicitly identified by domain (.mil) or IP address.

Remediation:

Configure directory data (outside the root DSE) of a non-public directory to prevent anonymous access.

For AD, there are multiple configuration items that could enable anonymous access.

Changing the access permissions on the domain naming context object (from the secure defaults) could enable anonymous access. If the check procedures indicate this is the cause, the process that was used to change the permissions should be reversed. This could have been through the Windows Support Tools ADSI Edit console (adsiedit.msc).

The dsHeuristics option is used. This is addressed in check V-8555 in the AD Forest STIG.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.161 WN16-DC-000160 (Manual)

Profile Applicability:

- DC SEVERITY: CAT III

Description:

The directory service must be configured to terminate LDAP-based network connections to the directory server after 5 minutes of inactivity.

```
GROUP ID: V-224979
RULE ID: SV-224979r970703
```

Rationale:

The failure to terminate inactive network connections increases the risk of a successful attack on the directory server. The longer an established session is in progress, the more time an attacker has to hijack the session, implement a means to passively intercept data, or compromise any protections on client access. For example, if an attacker gains control of a client computer, an existing (already authenticated) session with the directory server could allow access to the directory. The lack of confidentiality protection in LDAP-based sessions increases exposure to this vulnerability.

Audit:

This applies to domain controllers. It is NA for other systems.

Open an elevated "Command Prompt" (run as administrator).

Enter "ntdsutil".

At the "ntdsutil:" prompt, enter "LDAP policies".

At the "ldap policy:" prompt, enter "connections".

At the "server connections:" prompt, enter "connect to server [host-name]"

(where [host-name] is the computer name of the domain controller).

At the "server connections:" prompt, enter "q".

At the "ldap policy:" prompt, enter "show values".

If the value for MaxConnIdleTime is greater than "300" (5 minutes) or is not specified, this is a finding.

Enter "q" at the "ldap policy:" and "ntdsutil:" prompts to exit.

Alternately, Dsquery can be used to display MaxConnIdleTime:

Open "Command Prompt (Admin)".

Enter the following command (on a single line).

dsquery * "cn=Default Query Policy,cn=Query-Policies,cn=Directory Service, cn=Windows NT,cn=Services,cn=Configuration,dc=[forest-name]" -attr LDAPAdminLimits

The quotes are required and dc=[forest-name] is the fully qualified LDAP name of the domain being reviewed (e.g., dc=disaost,dc=mil).

If the results do not specify a "MaxConnIdleTime" or it has a value greater than "300" (5 minutes), this is a finding.

Remediation:

Configure the directory service to terminate LDAP-based network connections to the directory server after 5 minutes of inactivity.

Open an elevated "Command prompt" (run as administrator).

Enter "ntdsutil".

At the "ntdsutil:" prompt, enter "LDAP policies".

At the "ldap policy:" prompt, enter "connections".

At the "server connections:" prompt, enter "connect to server [host-name]" (where [host-name] is the computer name of the domain controller).

At the "server connections:" prompt, enter "q".

At the "ldap policy:" prompt, enter "Set MaxConnIdleTime to 300".

Enter "Commit Changes" to save.

Enter "Show values" to verify changes.

Enter "q" at the "ldap policy:" and "ntdsutil:" prompts to exit.

Additional Information:

CCI-001133

Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53 :: SC-10
- NIST SP 800-53A :: SC-10.1 (ii)
- NIST SP 800-53 Revision 4 :: SC-10
- NIST SP 800-53 Revision 5 :: SC-10

1.162 WN16-DC-000170 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Active Directory Group Policy objects must be configured with proper audit settings.

```
GROUP ID: V-224980
RULE ID: SV-224980r958732
```

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes Group Policy objects. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

This applies to domain controllers. It is NA for other systems.

Review the auditing configuration for all Group Policy objects.

Open "Group Policy Management" (available from various menus or run "gpmc.msc").

Navigate to "Group Policy Objects" in the domain being reviewed (Forest >> Domains >> Domain).

For each Group Policy object:

Select the Group Policy object item in the left pane.

Select the "Delegation" tab in the right pane.

Select the "Advanced" button.

Select the "Advanced" button again and then the "Auditing" tab.

If the audit settings for any Group Policy object are not at least as inclusive as those below, this is a finding.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Applies to - This object and all descendant objects or Descendant groupPolicyContainer objects

The three Success types listed below are defaults inherited from the Parent Object. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference.

- Type - Success
- Principal - Everyone
- Access - Special (Permissions: Write all properties, Modify permissions; Properties: all "Write" type selected)
- Inherited from - Parent Object
- Applies to - Descendant groupPolicyContainer objects

Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - blank (Permissions: none selected; Properties: one instance - Write gPLink, one instance - Write gPOptions)
- Inherited from - Parent Object
- Applies to - Descendant Organization Unit Objects

Remediation:

Configure the audit settings for Group Policy objects to include the following.

This can be done at the Policy level in Active Directory to apply to all group policies.

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Select "Advanced Features" from the "View" Menu.

Navigate to [Domain] >> System >> Policies in the left panel.

Right click "Policies", select "Properties".

Select the "Security" tab.

Select the "Advanced" button.

Select the "Auditing" tab.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Applies to - This object and all descendant objects or Descendant groupPolicyContainer objects

The three Success types listed below are defaults inherited from the Parent Object. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference.

- Type - Success
- Principal - Everyone
- Access - Special (Permissions: Write all properties, Modify permissions; Properties: all "Write" type selected)
- Inherited from - Parent Object
- Applies to - Descendant groupPolicyContainer objects

Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - blank (Permissions: none selected; Properties: one instance - Write gPLink, one instance - Write gPOptions)
- Inherited from - Parent Object
- Applies to - Descendant Organization Unit Objects

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.163 WN16-DC-000180 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Active Directory Domain object must be configured with proper audit settings.

```
GROUP ID: V-224981
RULE ID: SV-224981r958732
```

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the Domain object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

This applies to domain controllers. It is NA for other systems.

Review the auditing configuration for the Domain object.

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

Select the domain being reviewed in the left pane.

Right-click the domain name and select "Properties".

Select the "Security" tab.

Select the "Advanced" button and then the "Auditing" tab.

If the audit settings on the Domain object are not at least as inclusive as those below, this is a finding.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Inherited from - None
- Applies to - This object only

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.
Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - None
- Applies to - Special
- Type - Success
- Principal - Domain Users
- Access - All extended rights
- Inherited from - None
- Applies to - This object only
- Type - Success
- Principal - Administrators
- Access - All extended rights
- Inherited from - None
- Applies to - This object only
- Type - Success
- Principal - Everyone

- Access - Special
- Inherited from - None
- Applies to - This object only
- (Access - Special = Permissions: Write all properties, Modify permissions, Modify owner)

Remediation:

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

Select the domain being reviewed in the left pane.

Right-click the domain name and select "Properties".

Select the "Security" tab.

Select the "Advanced" button and then the "Auditing" tab.

Configure the audit settings for Domain object to include the following.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Inherited from - None
- Applies to - This object only

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.
Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - None
- Applies to - Special
- Type - Success
- Principal - Domain Users
- Access - All extended rights
- Inherited from - None
- Applies to - This object only
- Type - Success
- Principal - Administrators
- Access - All extended rights
- Inherited from - None
- Applies to - This object only
- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- Applies to - This object only

- (Access - Special = Permissions: Write all properties, Modify permissions, Modify owner.)

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.164 WN16-DC-000190 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Active Directory Infrastructure object must be configured with proper audit settings.

```
GROUP ID: V-224982
RULE ID: SV-224982r958732
```

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the Infrastructure object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

This applies to domain controllers. It is NA for other systems.

Review the auditing configuration for Infrastructure object.

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

Select the domain being reviewed in the left pane.

Right-click the "Infrastructure" object in the right pane and select "Properties".

Select the "Security" tab.

Select the "Advanced" button and then the "Auditing" tab.

If the audit settings on the Infrastructure object are not at least as inclusive as those below, this is a finding.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Inherited from - None

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- (Access - Special = Permissions: Write all properties, All extended rights, Change infrastructure master)

Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)

Remediation:

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

Select the domain being reviewed in the left pane.

Right-click the "Infrastructure" object in the right pane and select "Properties".

Select the "Security" tab.

Select the "Advanced" button and then the "Auditing" tab.

Configure the audit settings for Infrastructure object to include the following.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Inherited from - None

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- (Access - Special = Permissions: Write all properties, All extended rights, Change infrastructure master)

Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.165 WN16-DC-000200 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Active Directory Domain Controllers Organizational Unit (OU) object must be configured with proper audit settings.

```
GROUP ID: V-224983
RULE ID: SV-224983r958732
```

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the Domain Controller OU object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

This applies to domain controllers. It is NA for other systems.

Review the auditing configuration for the Domain Controller OU object.

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

Select the "Domain Controllers OU" under the domain being reviewed in the left pane.

Right-click the "Domain Controllers OU" object and select "Properties".

Select the "Security" tab.

Select the "Advanced" button and then the "Auditing" tab.

If the audit settings on the Domain Controllers OU object are not at least as inclusive as those below, this is a finding.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Inherited from - None
- Applies to - This object and all descendant objects

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- Applies to - This object only
- (Access - Special = Permissions: all create, delete and modify permissions)

- Type - Success
- Principal - Everyone
- Access - Write all properties
- Inherited from - None
- Applies to - This object and all descendant objects

Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - (blank)

- Inherited from - (CN of domain)
- Applies to - Descendant Organizational Unit objects

Remediation:

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

Select the "Domain Controllers OU" under the domain being reviewed in the left pane.

Right-click the "Domain Controllers OU" object and select "Properties".

Select the "Security" tab.

Select the "Advanced" button and then the "Auditing" tab.

Configure the audit settings for Domain Controllers OU object to include the following.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Inherited from - None

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- Applies to - This object only
- (Access - Special = Permissions: all create, delete and modify permissions)

- Type - Success
- Principal - Everyone
- Access - Write all properties
- Inherited from - None
- Applies to - This object and all descendant objects

Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)
- Applies to - Descendant Organizational Unit objects

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.166 WN16-DC-000210 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Active Directory AdminSDHolder object must be configured with proper audit settings.

```
GROUP ID: V-224984
RULE ID: SV-224984r958732
```

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the AdminSDHolder object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

This applies to domain controllers. It is NA for other systems.

Review the auditing configuration for the "AdminSDHolder" object.

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

Select "System" under the domain being reviewed in the left pane.

Right-click the "AdminSDHolder" object in the right pane and select "Properties".

Select the "Security" tab.

Select the "Advanced" button and then the "Auditing" tab.

If the audit settings on the "AdminSDHolder" object are not at least as inclusive as those below, this is a finding.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Inherited from - None
- Applies to - This object only

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- Applies to - This object only
- (Access - Special = Write all properties, Modify permissions, Modify owner)

Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)
- Applies to - Descendant Organizational Unit objects

Remediation:

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

Select "System" under the domain being reviewed in the left pane.

Right-click the "AdminSDHolder" object in the right pane and select "Properties".

Select the "Security" tab.

Select the "Advanced" button and then the "Auditing" tab.

Configure the audit settings for AdminSDHolder object to include the following.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Inherited from - None
- Applies to - This object only

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- Applies to - This object only
- (Access - Special = Write all properties, Modify permissions, Modify owner)

Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)
- Applies to - Descendant Organizational Unit objects

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.167 WN16-DC-000220 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Active Directory RID Manager$ object must be configured with proper audit settings.

```
GROUP ID: V-224985
RULE ID: SV-224985r958732
```

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the RID Manager$ object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

This applies to domain controllers. It is NA for other systems.

Review the auditing configuration for the "RID Manager$" object.

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

Select "System" under the domain being reviewed in the left pane.

Right-click the "RID Manager$" object in the right pane and select "Properties".

Select the "Security" tab.

Select the "Advanced" button and then the "Auditing" tab.

If the audit settings on the "RID Manager$" object are not at least as inclusive as those below, this is a finding.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Inherited from - None

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- (Access - Special = Write all properties, All extended rights, Change RID master)

Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)

Remediation:

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Ensure "Advanced Features" is selected in the "View" menu.

Select "System" under the domain being reviewed in the left pane.

Right-click the "RID Manager$" object in the right pane and select "Properties".

Select the "Security" tab.

Select the "Advanced" button and then the "Auditing" tab.

Configure the audit settings for RID Manager$ object to include the following.

- Type - Fail
- Principal - Everyone
- Access - Full Control
- Inherited from - None

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- (Access - Special = Write all properties, All extended rights, Change RID master)

Two instances with the following summary information will be listed.

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.168 WN16-DC-000230 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit Account Management - Computer Account Management successes.

```
GROUP ID: V-224986
RULE ID: SV-224986r958368
```

Rationale:

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.

Computer Account Management records events such as creating, changing, deleting, renaming, disabling, or enabling computer accounts.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Audit:

This applies to domain controllers. It is NA for other systems.

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

Account Management >> Computer Account Management - Success

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Advanced
Audit Policy Configuration >> System Audit Policies >> Account Management >>
"Audit Computer Account Management"
```

with "Success" selected.

References:

1. CIS Recommendation: Audit Computer Account Management
2. GRID: MS-00000200

Additional Information:

CCI-000018

Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c

CCI-001403

Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-001404

Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-001405

Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-002130

Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

1.169 WN16-DC-000240 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.

```
GROUP ID: V-224987
RULE ID: SV-224987r958732
```

Rationale:

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 Directory Service Access records events related to users accessing an Active Directory object.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

This applies to domain controllers. It is NA for other systems.

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

DS Access >> Directory Service Access - Success

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Advanced
Audit Policy Configuration >> System Audit Policies >> DS Access >>
"Directory Service Access"
```

with "Success" selected.

References:

1. CIS Recommendation: Directory Service Access
2. GRID: MS-00000207

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.170 WN16-DC-000250 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.

```
GROUP ID: V-224988
RULE ID: SV-224988r958732
```

Rationale:

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 Directory Service Access records events related to users accessing an Active Directory object.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

This applies to domain controllers. It is NA for other systems.

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

DS Access >> Directory Service Access - Failure

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Advanced
Audit Policy Configuration >> System Audit Policies >> DS Access >>
"Directory Service Access"
```

with "Failure" selected.

References:

1. CIS Recommendation: Directory Service Access
2. GRID: MS-00000207

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.171 WN16-DC-000260 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.

```
GROUP ID: V-224989
RULE ID: SV-224989r958732
```

Rationale:

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 Directory Service Changes records events related to changes made to objects in Active Directory Domain Services.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Audit:

This applies to domain controllers. It is NA for other systems.

Security Option "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" must be set to "Enabled" (WN16-SO-000050) for the detailed auditing subcategories to be effective.

Use the AuditPol tool to review the current Audit Policy configuration:

Open an elevated "Command Prompt" (run as administrator).

Enter

```
"AuditPol /get /category:*"
```

Compare the AuditPol settings with the following.

If the system does not audit the following, this is a finding.

DS Access >> Directory Service Changes - Success

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Advanced
Audit Policy Configuration >> System Audit Policies >> DS Access >>
"Directory Service Changes"
```

with "Success" selected.

References:

1. CIS Recommendation: Directory Service Changes
2. GRID: MS-00000208

Additional Information:

CCI-000172

Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c

CCI-002234

Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.172 WN16-DC-000280 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Domain controllers must have a PKI server certificate.

```
GROUP ID: V-224991
RULE ID: SV-224991r958448
```

Rationale:

Domain controllers are part of the chain of trust for PKI authentications. Without the appropriate certificate, the authenticity of the domain controller cannot be verified. Domain controllers must have a server certificate to establish authenticity as part of PKI authentications in the domain.

Audit:

This applies to domain controllers. It is NA for other systems.

Run "MMC".

Select "Add/Remove Snap-in" from the "File" menu.

Select "Certificates" in the left pane and click the "Add >" button.

Select "Computer Account" and click "Next".

Select the appropriate option for "Select the computer you want this snap-in to manage" and click "Finish".

Click "OK".

Select and expand the Certificates (Local Computer) entry in the left pane.

Select and expand the Personal entry in the left pane.

Select the Certificates entry in the left pane.

If no certificate for the domain controller exists in the right pane, this is a finding.

Remediation:

Obtain a server certificate for the domain controller.

Additional Information:

CCI-000185

For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53A :: IA-5 (2).1
- NIST SP 800-53 Revision 4 :: IA-5 (2) (a)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (b) (1)

1.173 WN16-DC-000290 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I

Description:

Domain Controller PKI certificates must be issued by the DoD PKI or an approved External Certificate Authority (ECA).

```
GROUP ID: V-224992
RULE ID: SV-224992r958448
```

Rationale:

A PKI implementation depends on the practices established by the Certificate Authority (CA) to ensure the implementation is secure. Without proper practices, the certificates issued by a CA have limited value in authentication functions. The use of multiple CAs from separate PKI implementations results in interoperability issues. If servers and clients do not have a common set of root CA certificates, they are not able to authenticate each other.

Audit:

This applies to domain controllers. It is NA for other systems.

Run "MMC".

Select "Add/Remove Snap-in" from the "File" menu.

Select "Certificates" in the left pane and click the "Add >" button.

Select "Computer Account" and click "Next".

Select the appropriate option for "Select the computer you want this snap-in to manage" and click "Finish".

Click "OK".

Select and expand the Certificates (Local Computer) entry in the left pane.

Select and expand the Personal entry in the left pane.

Select the Certificates entry in the left pane.

In the right pane, examine the "Issued By" field for the certificate to determine the issuing CA.

If the "Issued By" field of the PKI certificate being used by the domain controller does not indicate the issuing CA is part of the DoD PKI or an approved ECA, this is a finding.

If the certificates in use are issued by a CA authorized by the Component's CIO, this is a CAT II finding.

There are multiple sources from which lists of valid DoD CAs and approved ECAs can be obtained:

The Global Directory Service (GDS) website provides an online source. The address for this site is https://crl.gds.disa.mil.

DoD Public Key Enablement (PKE) Engineering Support maintains the InstallRoot utility to manage DoD supported root certificates on Windows computers, which includes a list of authorized CAs. The utility package can be downloaded from the PKI and PKE Tools page on IASE:

http://iase.disa.mil/pki-pke/function_pages/tools.html

Remediation:

Obtain a server certificate for the domain controller issued by the DoD PKI or an approved ECA.

Additional Information:

CCI-000185

For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53A :: IA-5 (2).1
- NIST SP 800-53 Revision 4 :: IA-5 (2) (a)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (b) (1)

1.174 WN16-DC-000300 (Manual)

Profile Applicability:

- DC SEVERITY: CAT I

Description:

PKI certificates associated with user accounts must be issued by the DoD PKI or an approved External Certificate Authority (ECA).

```
GROUP ID: V-224993
RULE ID: SV-224993r958448
```

Rationale:

A PKI implementation depends on the practices established by the Certificate Authority (CA) to ensure the implementation is secure. Without proper practices, the certificates issued by a CA have limited value in authentication functions.

Audit:

This applies to domain controllers. It is NA for other systems.

Review user account mappings to PKI certificates.

Open "Windows PowerShell".

Enter

```
"Get-ADUser -Filter * | FT Name, UserPrincipalName, Enabled"
```

Exclude disabled accounts (e.g., DefaultAccount, Guest) and the krbtgt account.

If the User Principal Name (UPN) is not in the format of an individual's identifier for the certificate type and for the appropriate domain suffix, this is a finding.

For standard NIPRNet certificates the individual's identifier is in the format of an Electronic Data Interchange - Personnel Identifier (EDI-PI).

Alt Tokens and other certificates may use a different UPN format than the EDI-PI which vary by organization. Verified these with the organization.

```
NIPRNet Example:
Name - User Principal Name
User1 - 1234567890@mil
```

See PKE documentation for other network domain suffixes.

If the mappings are to certificates issued by a CA authorized by the Component's CIO, this is a CAT II finding.

Remediation:

Map user accounts to PKI certificates using the appropriate User Principal Name (UPN) for the network. See PKE documentation for details.

Additional Information:

CCI-000185

For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53A :: IA-5 (2).1
- NIST SP 800-53 Revision 4 :: IA-5 (2) (a)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (b) (1)

1.175 WN16-DC-000310 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Active Directory user accounts, including administrators, must be configured to require the use of a Common Access Card (CAC), Personal Identity Verification (PIV)-compliant hardware token, or Alternate Logon Token (ALT) for user authentication.

```
GROUP ID: V-224994
RULE ID: SV-224994r958484
```

Rationale:

Smart cards such as the CAC support a two-factor authentication technique. This provides a higher level of trust in the asserted identity than use of the username and password for authentication.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055, SRG-OS-000375-GPOS-00160

Audit:

This applies to domain controllers. It is NA for other systems.

Open "PowerShell".

Enter the following:

```
"Get-ADUser -Filter {(Enabled -eq $True) -and (SmartcardLogonRequired -eq
$False)} | FT Name"
```

("DistinguishedName" may be substituted for "Name" for more detailed output.)

If any user accounts, including administrators, are listed, this is a finding.

Alternately:

To view sample accounts in "Active Directory Users and Computers" (available from various menus or run "dsa.msc"):

Select the Organizational Unit (OU) where the user accounts are located. (By default, this is the Users node; however, accounts may be under other organization-defined OUs.)

Right-click the sample user account and select "Properties".

Select the "Account" tab.

If any user accounts, including administrators, do not have "Smart card is required for interactive logon" checked in the "Account Options" area, this is a finding.

Remediation:

Configure all user accounts, including administrator accounts, in Active Directory to enable the option "Smart card is required for interactive logon".

Run "Active Directory Users and Computers" (available from various menus or run "dsa.msc"):

Select the OU where the user accounts are located. (By default this is the Users node; however, accounts may be under other organization-defined OUs.)

Right-click the user account and select "Properties".

Select the "Account" tab.

Check "Smart card is required for interactive logon" in the "Account Options" area.

Additional Information:

CCI-000765

Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53 :: IA-2 (1)
- NIST SP 800-53A :: IA-2 (1).1
- NIST SP 800-53 Revision 4 :: IA-2 (1)
- NIST SP 800-53 Revision 5 :: IA-2 (1)

CCI-000766

Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53 :: IA-2 (2)
- NIST SP 800-53A :: IA-2 (2).1
- NIST SP 800-53 Revision 4 :: IA-2 (2)
- NIST SP 800-53 Revision 5 :: IA-2 (2)

CCI-000767

The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53 :: IA-2 (3)
- NIST SP 800-53A :: IA-2 (3).1
- NIST SP 800-53 Revision 4 :: IA-2 (3)

CCI-000768

The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53 :: IA-2 (4)
- NIST SP 800-53A :: IA-2 (4).1
- NIST SP 800-53 Revision 4 :: IA-2 (4)

CCI-001948

The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 4 :: IA-2 (11)

1.176 WN16-DC-000320 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Domain controllers must require LDAP access signing.

```
GROUP ID: V-224995
RULE ID: SV-224995r958908
```

Rationale:

Unsigned network traffic is susceptible to man-in-the-middle attacks, where an intruder captures packets between the server and the client and modifies them before forwarding them to the client. In the case of an LDAP server, this means that an attacker could cause a client to make decisions based on false records from the LDAP directory. The risk of an attacker pulling this off can be decreased by implementing strong physical security measures to protect the network infrastructure. Furthermore, implementing Internet Protocol security (IPsec) authentication header mode (AH), which performs mutual authentication and packet integrity for Internet Protocol (IP) traffic, can make all types of man-in-the-middle attacks extremely difficult.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Audit:

This applies to domain controllers. It is NA for other systems.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\NTDS\Parameters\

Value Name: LDAPServerIntegrity

Value Type: REG_DWORD
Value: 0x00000002 (2)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Domain controller: LDAP server signing
requirements"
```

to "Require signing".

References:

1. CIS Recommendation: Domain controller: LDAP server signing requirements
2. GRID: MS-00000516

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.177 WN16-DC-000330 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

Domain controllers must be configured to allow reset of machine account passwords.

```
GROUP ID: V-224996
RULE ID: SV-224996r991589
```

Rationale:

Enabling this setting on all domain controllers in a domain prevents domain members from changing their computer account passwords. If these passwords are weak or compromised, the inability to change them may leave these computers vulnerable.

Audit:

This applies to domain controllers. It is NA for other systems.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\

Value Name: RefusePasswordChange

Value Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Domain controller: Refuse machine account
password changes"
```

to "Disabled".

References:

1. CIS Recommendation: Domain controller: Refuse machine account password changes
2. GRID: MS-00000519

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.178 WN16-DC-000340 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.

```
GROUP ID: V-224997
RULE ID: SV-224997r958472
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the "Access this computer from the network" right may access resources on the system, and this right must be limited to those requiring it.

Audit:

This applies to domain controllers. It is NA for other systems.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Access this computer from the network" right, this is a finding.

- Administrators
- Authenticated Users
- Enterprise Domain Controllers

For server core installations, run the following command:
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
Review the text file.
If any SIDs other than the following are granted the "SeNetworkLogonRight" user right, this is a finding.
S-1-5-32-544 (Administrators)
S-1-5-11 (Authenticated Users)
S-1-5-9 (Enterprise Domain Controllers)
If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Access this computer from the network" to include only the following accounts or groups:

- Administrators
- Authenticated Users
- Enterprise Domain Controllers

References:

1. CIS Recommendation: Access this computer from the network
2. GRID: MS-00000013

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.179 WN16-DC-000350 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Add workstations to domain user right must only be assigned to the Administrators group.

```
GROUP ID: V-224998
RULE ID: SV-224998r958726
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the "Add workstations to domain" right may add computers to a domain. This could result in unapproved or incorrectly configured systems being added to a domain.

Audit:

This applies to domain controllers. It is NA for other systems.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Add workstations to domain" right, this is a finding.

- Administrators

For server core installations, run the following command:
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
Review the text file.
If any SIDs other than the following are granted the "SeMachineAccountPrivilege" user right, this is a finding.
S-1-5-32-544 (Administrators)

Remediation:

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Add workstations to domain" to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Add workstations to domain
2. GRID: MS-00000015

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.180 WN16-DC-000360 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.

```
GROUP ID: V-224999
RULE ID: SV-224999r958472
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the "Allow log on through Remote Desktop Services" user right can access a system through Remote Desktop.

Audit:

This applies to domain controllers, it is NA for other systems.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Allow log on through Remote Desktop Services" user right, this is a finding.

- Administrators

For server core installations, run the following command:
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
Review the text file.
If any SIDs other than the following are granted the "SeRemoteInteractiveLogonRight" user right, this is a finding.
S-1-5-32-544 (Administrators)

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Allow log on through Remote Desktop
Services"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Allow log on through Remote Desktop Services
2. GRID: MS-00000018

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.181 WN16-DC-000370 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.

```
GROUP ID: V-225000
RULE ID: SV-225000r958472
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Deny access to this computer from the network" user right defines the accounts that are prevented from logging on from the network.

The Guests group must be assigned this right to prevent unauthenticated access.

Audit:

This applies to domain controllers. A separate version applies to other systems.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If the following accounts or groups are not defined for the "Deny access to this computer from the network" user right, this is a finding.

- Guests Group

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If the following SIDs are not defined for the "SeDenyNetworkLogonRight" user right, this is a finding.

S-1-5-32-546 (Guests)

Remediation:

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:

- Guests Group

References:

1. CIS Recommendation: Deny access to this computer from the network
2. GRID: MS-00000028

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.182 WN16-DC-000380 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.

```
GROUP ID: V-225001
RULE ID: SV-225001r958472
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Deny log on as a batch job" user right defines accounts that are prevented from logging on to the system as a batch job, such as Task Scheduler.

The Guests group must be assigned to prevent unauthenticated access.

Audit:

This applies to domain controllers. A separate version applies to other systems.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If the following accounts or groups are not defined for the "Deny log on as a batch job" user right, this is a finding.

- Guests Group

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If the following SID(s) are not defined for the "SeDenyBatchLogonRight" user right, this is a finding.

S-1-5-32-546 (Guests)

Remediation:

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:

- Guests Group

References:

1. CIS Recommendation: Deny log on as a batch job
2. GRID: MS-00000029

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.183 WN16-DC-000390 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.

```
GROUP ID: V-225002
RULE ID: SV-225002r958472
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Deny log on as a service" user right defines accounts that are denied logon as a service.

Incorrect configurations could prevent services from starting and result in a denial of service.

Audit:

This applies to domain controllers. A separate version applies to other systems.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups are defined for the "Deny log on as a service" user right, this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs are granted the "SeDenyServiceLogonRight" user right, this is a finding.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Deny log on as a service"
```

to include no entries (blank).

References:

1. CIS Recommendation: Deny log on as a service
2. GRID: MS-00000030

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.184 WN16-DC-000400 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.

```
GROUP ID: V-225003
RULE ID: SV-225003r958472
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Deny log on locally" user right defines accounts that are prevented from logging on interactively.

The Guests group must be assigned this right to prevent unauthenticated access.

Audit:

This applies to domain controllers. A separate version applies to other systems.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If the following accounts or groups are not defined for the "Deny log on locally" user right, this is a finding.

- Guests Group

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If the following SID(s) are not defined for the "SeDenyInteractiveLogonRight" user right, this is a finding.

S-1-5-32-546 (Guests)

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Deny log on locally"
```

to include the following:

- Guests Group

References:

1. CIS Recommendation: Deny log on locally
2. GRID: MS-00000031

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.185 WN16-DC-000401 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I

Description:

Windows Server 2016 must be configured for name-based strong mappings for certificates.

```
GROUP ID:V-271430
RULE ID:SV-271430r1059573
```

Rationale:

Weak mappings give rise to security vulnerabilities and demand hardening measures. Certificate names must be correctly mapped to the intended user account in Active Directory. A lack of strong name-based mappings allows certain weak certificate mappings, such as Issuer/Subject AltSecID and User Principal Names (UPN) mappings, to be treated as strong mappings.

Audit:

This requirement is not applicable for Member Servers.

Note: This requirement is a permanent finding for server 2016 domain controllers per DOD CIO Memo Upgrading of MS Domain Controller OS to MS Server 2019 or Later (CIO000911-23).

If the server is acting as a domain controller, this is a finding.

Remediation:

For servers acting as a domain controller, upgrade the operating system to Microsoft Server 2019 or greater.

References:

1. CIS Recommendation: Deny log on through Remote Desktop Services
2. GRID: MS-00000032

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3
- NIST SP 800-53A :: AC-3.1

1.186 WN16-DC-000410 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.

```
GROUP ID: V-225004
RULE ID: SV-225004r958672
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Deny log on through Remote Desktop Services" user right defines the accounts that are prevented from logging on using Remote Desktop Services.

The Guests group must be assigned this right to prevent unauthenticated access.

Audit:

This applies to domain controllers. A separate version applies to other systems.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If the following accounts or groups are not defined for the "Deny log on through Remote Desktop Services" user right, this is a finding.

- Guests Group

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If the following SID(s) are not defined for the "SeDenyRemoteInteractiveLogonRight" user right, this is a finding.

S-1-5-32-546 (Guests)

Remediation:

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:

- Guests Group

Additional Information:

CCI-002314

Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)

1.187 WN16-DC-000420 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.

```
GROUP ID: V-225005
RULE ID: SV-225005r958726
```

Rationale:

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 allow unauthorized users to impersonate other users.

Audit:

This applies to domain controllers. A separate version applies to other systems.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Enable computer and user accounts to be trusted for delegation" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeEnableDelegationPrivilege" user right, this is a finding.

S-1-5-32-544 (Administrators)

Remediation:

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 include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Enable computer and user accounts to be trusted for delegation
2. GRID: MS-00000033

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.188 WN16-DC-000430 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II

Description:

The password for the krbtgt account on a domain must be reset at least every 180 days.

```
GROUP ID: V-225006
RULE ID: SV-225006r991589
```

Rationale:

The krbtgt account acts as a service account for the Kerberos Key Distribution Center (KDC) service. The account and password are created when a domain is created and the password is typically not changed. If the krbtgt account is compromised, attackers can create valid Kerberos Ticket Granting Tickets (TGT).

The password must be changed twice to effectively remove the password history.Changing once, waiting for replication to complete and the amount of time equal to or greater than the maximum Kerberos ticket lifetime, and changing again reduces the risk of issues.

Audit:

This requirement is applicable to domain controllers; it is NA for other systems.

Open "Windows PowerShell".

Enter

```
"Get-ADUser krbtgt -Property PasswordLastSet"
```

If the "PasswordLastSet" date is more than 180 days old, this is a finding.

Remediation:

Reset the password for the krbtgt account a least every 180 days. The password must be changed twice to effectively remove the password history. Changing once, waiting for replication to complete and changing again reduces the risk of issues. Changing twice in rapid succession forces clients to re-authenticate (including application services) but is desired if a compromise is suspected.

PowerShell scripts are available to accomplish this such as at the following link:

https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51

Open "Active Directory Users and Computers" (available from various menus or run "dsa.msc").

Select "Advanced Features" in the "View" menu if not previously selected.

Select the "Users" node.

Right click on the krbtgt account and select "Reset password".

Enter a password that meets password complexity requirements.

Clear the "User must change password at next logon" check box.

The system will automatically change this to a system generated complex password.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.189 WN16-MS-000010 (Manual)

Profile Applicability:

- MS SEVERITY: CAT I

Description:

Only administrators responsible for the member server or standalone or nondomain-joined system must have Administrator rights on the system.

```
GROUP ID: V-225007
RULE ID: SV-225007r958726
```

Rationale:

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 using only accounts with the minimum level of authority necessary.

For domain-joined member servers, the Domain Admins group must be replaced by a domain member server administrator group (refer to AD.0003 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 built-in Administrators group.

Audit:

This applies to member servers and standalone or nondomain-joined systems. A separate version applies to domain controllers.

Open "Computer Management".

Navigate to "Groups" under "Local Users and Groups".

Review the local "Administrators" group.

Only administrator groups or accounts responsible for administration of the system may be members of the group.

For domain-joined member servers, the Domain Admins group must be replaced by a domain member server administrator group.

Standard user accounts must not be members of the local Administrator group.

If accounts that do not have responsibility for administration of the system are members of the local Administrators group, this is a finding.

If the built-in Administrator account or other required administrative accounts are found on the system, this is not a finding.

Remediation:

Configure the local "Administrators" group to include only administrator groups or accounts responsible for administration of the system.

For domain-joined member servers, replace the Domain Admins group with a domain member server administrator group.

Remove any standard user accounts.

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.190 WN16-MS-000020 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.

```
GROUP ID:V-225008
RULE ID:SV-225008r958518
```

Rationale:

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 local administrator accounts will prevent the elevated privileges of these accounts from being used over the network.

Audit:

This applies to member servers. For domain controllers and standalone or nondomain-joined systems, this is NA.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive:  HKEY_LOCAL_MACHINE
Registry Path:  \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value Name:  LocalAccountTokenFilterPolicy

Type:  REG_DWORD
Value: 0x00000000 (0)
```

This setting may cause issues with some network scanning tools if local administrative accounts are used remotely. Scans should use domain accounts where possible. If a local administrative account must be used, temporarily enabling the privileged token by configuring the registry value to "1" may be required.

Remediation:

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.

References:

1. CIS Recommendation: Apply UAC restrictions to local accounts on network logons
2. GRID: MS-00000240

Additional Information:

CCI-001084

Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)

1.191 WN16-MS-000030 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

Local users on domain-joined computers must not be enumerated.

```
GROUP ID:V-225009
RULE ID:SV-225009r958478
```

Rationale:

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.

Audit:

This applies to member servers. For domain controllers and standalone or nondomain-joined systems, this is NA.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\System\

Value Name: EnumerateLocalUsers

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> System >> Logon >>
"Enumerate local users on domain-joined computers"
```

to "Disabled".

References:

1. CIS Recommendation: Enumerate local users on domain-joined computers
2. GRID: MS-00000348

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.192 WN16-MS-000040 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.

```
GROUP ID:V-225010
RULE ID:SV-225010r971545
```

Rationale:

Unauthenticated RPC clients may allow anonymous access to sensitive information. Configuring RPC to restrict unauthenticated RPC clients from connecting to the RPC server will prevent anonymous connections.

Audit:

This applies to member servers and standalone or nondomain-joined systems. It is NA for domain controllers.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive:  HKEY_LOCAL_MACHINE
Registry Path:  \SOFTWARE\Policies\Microsoft\Windows NT\Rpc\

Value Name:  RestrictRemoteClients

Type:  REG_DWORD
Value:  0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> System >> Remote
Procedure Call >> "Restrict Unauthenticated RPC clients"
```

to "Enabled" with "Authenticated" selected.

References:

1. CIS Recommendation: Restrict Unauthenticated RPC clients
2. GRID: MS-00000362

Additional Information:

CCI-001967

Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4 :: IA-3 (1)
- NIST SP 800-53 Revision 5 :: IA-3 (1)

1.193 WN16-MS-000050 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

Caching of logon credentials must be limited.

```
GROUP ID:V-225011
RULE ID:SV-225011r991589
```

Rationale:

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.

Audit:

This applies to member servers. For domain controllers and standalone or nondomain-joined systems, this is NA.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive:  HKEY_LOCAL_MACHINE
Registry Path:  \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\

Value Name:  CachedLogonsCount

Value Type:  REG_SZ
Value:  4 (or less)
```

Remediation:

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 "4" logons or less.

References:

1. CIS Recommendation: Interactive Logon: Number of previous logons to cache (in case Domain Controller is not available)
2. GRID: MS-00000077

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.194 WN16-MS-000120 (Automated)

Profile Applicability:

- MS SEVERITY: CAT I

Description:

Windows Server 2016 must be running Credential Guard on domain-joined member servers.

```
GROUP ID:V-225012
RULE ID:SV-225012r991589
```

Rationale:

Credential Guard uses virtualization-based security to protect data 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 the operating system and can only be accessed by privileged system software.

Audit:

For domain controllers and standalone or nondomain-joined systems, this is NA.

Open "PowerShell" with elevated privileges (run as administrator).

Enter the following:

```
"Get-CimInstance -ClassName Win32_DeviceGuard -Namespace
root\Microsoft\Windows\DeviceGuard"
```

If "SecurityServicesRunning" does not include a value of "1" (e.g., "{1, 2}"), this is a finding.

Alternately:

Run "System Information".

Under "System Summary", verify the following:

If "Device Guard Security Services Running" does not list "Credential Guard", this is a finding.

The policy settings referenced in the Fix section will configure the following registry value. However, due to hardware requirements, the registry value alone does not ensure proper function.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\DeviceGuard\

Value Name: LsaCfgFlags
Value Type: REG_DWORD
Value: 0x00000001 (1) (Enabled with UEFI lock)
```

A Microsoft article on Credential Guard system requirement can be found at the following link:

https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements

Remediation:

Configure the policy value for

```
Computer Configuration >> Administrative Templates >> System >> Device Guard
>> "Turn On Virtualization Based Security"
```

to "Enabled" with "Enabled with UEFI lock" selected for "Credential Guard Configuration".

A Microsoft article on Credential Guard system requirement can be found at the following link:

https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements

Severity Override Guidance: The AO can allow the severity override if they have reviewed the overall protection provided to the affected servers that are not capable of complying with the Credential Guard requirement. Items that should be reviewed/considered for compliance or mitigation for non-Credential Guard compliance are:

The use of Microsoft Local Administrator Password Solution (LAPS) or similar products to control different local administrative passwords for all affected affected servers. This is to include a strict password change requirement (60 days or less).

….

Strict separation of roles and duties. Server administrator credentials cannot be used on Windows 10 desktop to administer it. Documentation of all exceptions should be supplied.

….

Use of a Privileged Access Workstation (PAW) and adherence to the Clean Source principle for administering affected affected servers.

….

Boundary Protection that is currently in place to protect from vulnerabilities in the network/servers.

….

Windows Defender rule block credential stealing from LSASS.exe is applied. This rule can only be applied if Windows Defender is in use.

….

The overall number of vulnerabilities that are unmitigated on the network/servers.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.195 WN16-MS-000310 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.

```
GROUP ID:V-225013
RULE ID:SV-225013r958726
```

Rationale:

The Windows Security Account Manager (SAM) stores users' passwords. Restricting Remote Procedure Call (RPC) connections to the SAM to Administrators helps protect those credentials.

Audit:

This applies to member servers and standalone or nondomain-joined systems. It is NA for domain controllers.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\

Value Name: RestrictRemoteSAM

Value Type: REG_SZ
Value: O:BAG:BAD:(A;;RC;;;BA)
```

Remediation:

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.

References:

1. CIS Recommendation: Network access: Restrict clients allowed to make remote calls to SAM
2. GRID: MS-00000100

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.196 WN16-MS-000340 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

The "Access this computer from the network" user right must only be assigned to the Administrators and Authenticated Users groups on member servers.

```
GROUP ID: V-225014
RULE ID: SV-225014r958472
```

Rationale:

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 this right must be limited to those requiring it.

Audit:

This applies to member servers and standalone or nondomain-joined systems. A separate version applies to domain controllers.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Access this computer from the network" user right, this is a finding.

- Administrators
- Authenticated Users

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeNetworkLogonRight" user right, this is a finding.

- S-1-5-32-544 (Administrators)
- S-1-5-11 (Authenticated Users)

If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Access this computer from the network"
```

to include only the following accounts or groups:

- Administrators
- Authenticated Users

References:

1. CIS Recommendation: Access this computer from the network
2. GRID: MS-00000013

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.197 WN16-MS-000370 (Manual)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

The "Deny access to this computer from the network" user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and from unauthenticated access on all systems.

```
GROUP ID: V-225015
RULE ID: SV-225015r958472
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Deny access to this computer from the network" user 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.

Audit:

This applies to member servers and standalone or nondomain-joined systems. A separate version applies to domain controllers.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If the following accounts or groups are not defined for the "Deny access to this computer from the network" user right, this is a finding.

Domain Systems Only:

- Enterprise Admins group
- Domain Admins group
- "Local account and member of Administrators group" or "Local account" (see Note below)

All Systems:

- Guests group

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If the following SIDs are not defined for the "SeDenyNetworkLogonRight" user right, this is a finding.

Domain Systems Only:

- S-1-5-root domain-519 (Enterprise Admins)
- S-1-5-domain-512 (Domain Admins)
- S-1-5-114 ("Local account and member of Administrators group") or S-1-5-113 ("Local account")

All Systems:

- S-1-5-32-546 (Guests)

Note: These are built-in security groups. "Local account" is more restrictive but may cause issues on servers such as systems that provide failover clustering.

Remediation:

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 and member of Administrators group" or "Local account" (see Note below)

All Systems:

- Guests group

Note: These are built-in security groups. "Local account" is more restrictive but may cause issues on servers such as systems that provide failover clustering.

References:

1. CIS Recommendation: Deny access to this computer from the network
2. GRID: MS-00000028

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.198 WN16-MS-000380 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

The "Deny log on as a batch job" user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.

```
GROUP ID: V-225016
RULE ID: SV-225016r958472
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Deny log on as a batch job" user right defines accounts that are prevented from logging on to the system as a batch job, such as Task Scheduler.

In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.

The Guests group must be assigned to prevent unauthenticated access.

Audit:

This applies to member servers and standalone or nondomain-joined systems. A separate version applies to domain controllers.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If the following accounts or groups are not defined for the "Deny log on as a batch job" user right, this is a finding.

Domain Systems Only:

- Enterprise Admins Group
- Domain Admins Group

All Systems:

- Guests Group

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If the following SIDs are not defined for the "SeDenyBatchLogonRight" user right, this is a finding.

Domain Systems Only:

- S-1-5-root domain-519 (Enterprise Admins)
- S-1-5-domain-512 (Domain Admins)

All Systems:

- S-1-5-32-546 (Guests)

Remediation:

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 Admins Group
- Domain Admins Group

All Systems:

- Guests Group

References:

1. CIS Recommendation: Deny log on as a batch job
2. GRID: MS-00000029

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.199 WN16-MS-000390 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

The "Deny log on as a service" user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.

```
GROUP ID: V-225017
RULE ID: SV-225017r958472
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Deny log on as a service" user right defines accounts that are denied logon 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 denial of service.

Audit:

This applies to member servers. A separate version applies to domain controllers.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If the following accounts or groups are not defined for the "Deny log on as a service" user right on domain-joined systems, this is a finding.

- Enterprise Admins Group
- Domain Admins Group

If any accounts or groups are defined for the "Deny log on as a service" user right on nondomain-joined systems, this is a finding.
For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If the following SIDs are not defined for the "SeDenyServiceLogonRight" user right on domain-joined systems, this is a finding.

```
S-1-5-root domain-519 (Enterprise Admins)
S-1-5-domain-512 (Domain Admins)
```

Remediation:

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:

- Enterprise Admins Group
- Domain Admins Group

References:

1. CIS Recommendation: Deny log on as a service
2. GRID: MS-00000030

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.200 WN16-MS-000400 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

The "Deny log on locally" user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.

```
GROUP ID: V-225018
RULE ID: SV-225018r958472
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Deny log on locally" user 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.

Audit:

This applies to member servers and standalone or nondomain-joined systems. A separate version applies to domain controllers.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If the following accounts or groups are not defined for the "Deny log on locally" user right, this is a finding.

Domain Systems Only:

- Enterprise Admins Group
- Domain Admins Group

All Systems:

- Guests Group

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If the following SIDs are not defined for the "SeDenyInteractiveLogonRight" user right, this is a finding.

Domain Systems Only:

- S-1-5-root domain-519 (Enterprise Admins)
- S-1-5-domain-512 (Domain Admins)

All Systems:

- S-1-5-32-546 (Guests)

Remediation:

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

All Systems:

- Guests Group

References:

1. CIS Recommendation: Deny log on locally
2. GRID: MS-00000031

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.201 WN16-MS-000410 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

The "Deny log on through Remote Desktop Services" user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.

```
GROUP ID: V-225019
RULE ID: SV-225019r958672
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Deny log on through Remote Desktop Services" user right defines the accounts that are prevented from logging on using Remote Desktop Services.

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.

Audit:

This applies to member servers and standalone or nondomain-joined systems. A separate version applies to domain controllers.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If the following accounts or groups are not defined for the "Deny log on through Remote Desktop Services" user right, this is a finding.

Domain Systems Only:

- Enterprise Admins group
- Domain Admins group
- Local account (see Note below)

All Systems:

- Guests group

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If the following SIDs are not defined for the "SeDenyRemoteInteractiveLogonRight" user right, this is a finding.

Domain Systems Only:

- S-1-5-root domain-519 (Enterprise Admins)
- S-1-5-domain-512 (Domain Admins)
- S-1-5-113 ("Local account")

All Systems:

- S-1-5-32-546 (Guests)

Note: "Local account" is referring to the Windows built-in security group.

Remediation:

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:

Domain Systems Only:

- Enterprise Admins group
- Domain Admins group
- Local account (see Note below)

All Systems:

- Guests group

Note: "Local account" is referring to the Windows built-in security group.

References:

1. CIS Recommendation: Deny log on through Remote Desktop Services
2. GRID: MS-00000032

Additional Information:

CCI-002314

Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)

1.202 WN16-MS-000420 (Automated)

Profile Applicability:

- MS SEVERITY: CAT II

Description:

The "Enable computer and user accounts to be trusted for delegation" user right must not be assigned to any groups or accounts on member servers.

```
GROUP ID: V-225020
RULE ID: SV-225020r958726
```

Rationale:

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 allow unauthorized users to impersonate other users.

Audit:

This applies to member servers and standalone or nondomain-joined systems. A separate version applies to domain controllers.

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups are granted the "Enable computer and user accounts to be trusted for delegation" user right, this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs are granted the "SeEnableDelegationPrivilege" user right, this is a finding.

Remediation:

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).

References:

1. CIS Recommendation: Enable computer and user accounts to be trusted for delegation
2. GRID: MS-00000033

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.203 WN16-PK-000010 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The DoD Root CA certificates must be installed in the Trusted Root Store.

```
GROUP ID: V-225021
RULE ID: SV-225021r958448
```

Rationale:

To ensure secure DoD websites and DoD-signed code are properly validated, the system must trust the DoD Root Certificate Authorities (CAs). The DoD root certificates will ensure that the trust chain is established for server certificates issued from the DoD CAs.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182

Audit:

The certificates and thumbprints referenced below apply to unclassified systems; refer to PKE documentation for other networks.

Open "Windows PowerShell" as an administrator.

Execute the following command:

```
Get-ChildItem -Path Cert:Localmachine\root | Where Subject -Like "*DoD*" | FL
Subject, Thumbprint, NotAfter
```

If the following certificate "Subject" and "Thumbprint" information is not displayed, this is finding.

```
Subject: CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U.S. Government, C=US
Thumbprint: D73CA91102A2204A36459ED32213B467D7CE97FB
NotAfter: 12/30/2029
Subject: CN=DoD Root CA 4, OU=PKI, OU=DoD, O=U.S. Government, C=US
Thumbprint: B8269F25DBD937ECAFD4C35A9838571723F2D026
NotAfter: 7/25/2032
Subject: CN=DoD Root CA 5, OU=PKI, OU=DoD, O=U.S. Government, C=US
Thumbprint: 4ECB5CC3095670454DA1CBD410FC921F46B8564B
NotAfter: 6/14/2041
Subject: CN=DoD Root CA 6, OU=PKI, OU=DoD, O=U.S. Government, C=US
Thumbprint: D37ECF61C0B4ED88681EF3630C4E2FC787B37AEF
Valid to: Friday, January 24, 2053
```

Alternately, use the Certificates MMC snap-in:

Run "MMC".

Select "File", "Add/Remove Snap-in".

Select "Certificates" and click "Add".

Select "Computer account" and click "Next".

Select "Local computer: (the computer this console is running on)" and click "Finish".

Click "OK".

Expand "Certificates" and navigate to "Trusted Root Certification Authorities >> Certificates".

For each of the DoD Root CA certificates noted below:

Right-click on the certificate and select "Open".

Select the "Details" tab.

Scroll to the bottom and select "Thumbprint".

If the DoD Root CA certificates below are not listed or the value for the "Thumbprint" field is not as noted, this is a finding.

```
DoD Root CA 3
Thumbprint: D73CA91102A2204A36459ED32213B467D7CE97FB
Valid to: Sunday, December 30, 2029
DoD Root CA 4
Thumbprint: B8269F25DBD937ECAFD4C35A9838571723F2D026
Valid to: Sunday, July 25, 2032
DoD Root CA 5
Thumbprint: 4ECB5CC3095670454DA1CBD410FC921F46B8564B
Valid to: Friday, June 14, 2041
DoD Root CA 6
Thumbprint: D37ECF61C0B4ED88681EF3630C4E2FC787B37AEF
Valid to: Friday, January 24, 2053
```

Remediation:

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/.

Additional Information:

CCI-000185

For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53A :: IA-5 (2).1
- NIST SP 800-53 Revision 4 :: IA-5 (2) (a)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (b) (1)

CCI-002470

Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4 :: SC-23 (5)
- NIST SP 800-53 Revision 5 :: SC-23 (5)

1.204 WN16-PK-000020 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

```
GROUP ID: V-225022
RULE ID: SV-225022r958448
```

Rationale:

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.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182

Audit:

Verify the DoD Interoperability cross-certificates are installed on unclassified systems as Untrusted Certificates.

Run "PowerShell" as an administrator.

Execute the following command:

```
Get-ChildItem -Path Cert:Localmachine\disallowed | Where {$_.Issuer -Like
"*DoD Interoperability*" -and $_.Subject -Like "*DoD*"} | FL Subject, Issuer,
Thumbprint, NotAfter
```

If the following certificate "Subject", "Issuer", and "Thumbprint" information is not displayed, this is a finding.

```
Subject: CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U.S. Government, C=US
Issuer: CN=DoD Interoperability Root CA 2, OU=PKI, OU=DoD, O=U.S. Government,
C=US
Thumbprint: 49CBE933151872E17C8EAE7F0ABA97FB610F6477
NotAfter: 11/16/2024 9:57:16 AM
```

Alternately use the Certificates MMC snap-in:

Run "MMC".

Select "File", "Add/Remove Snap-in".

Select "Certificates", click "Add".

Select "Computer account", click "Next".

Select "Local computer: (the computer this console is running on)", click "Finish".

Click "OK".

Expand "Certificates" and navigate to Untrusted Certificates >> Certificates.

For each certificate with "DoD Root CA…" under "Issued To" and "DoD Interoperability Root CA…" under "Issued By":

Right-click on the certificate and select "Open".

Select the "Details" tab.

Scroll to the bottom and select "Thumbprint".

If the certificates below are not listed or the value for the "Thumbprint" field is not as noted, this is a finding.

If an expired certificate ("Valid to" date) is not listed in the results, this is not a finding.

```
Subject: CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U.S. Government, C=US
Issuer: CN=DoD Interoperability Root CA 2, OU=PKI, OU=DoD, O=U.S. Government,
C=US
Thumbprint: 49CBE933151872E17C8EAE7F0ABA97FB610F6477
NotAfter: 11/16/2024 9:57:16 AM
```

Remediation:

Install the DoD Interoperability Root CA cross-certificates on unclassified systems.

```
Issued To - Issued By - Thumbprint
DoD Root CA 3 - DoD Interoperability Root CA 2 -
49CBE933151872E17C8EAE7F0ABA97FB610F6477
```

The certificates can be installed using the InstallRoot tool. The tool and user guide are available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. Certificate bundles published by the PKI can be found at https://crl.gds.disa.mil/.

Additional Information:

CCI-000185

For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53A :: IA-5 (2).1
- NIST SP 800-53 Revision 4 :: IA-5 (2) (a)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (b) (1)

CCI-002440

Manage cryptographic keys when cryptography employed within the system in accordance with organization-defined requirements for key storage.

- NIST SP 800-53 Revision 4 :: SC-12
- NIST SP 800-53 Revision 5 :: SC-12

1.205 WN16-PK-000030 (Manual)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

```
GROUP ID: V-225023
RULE ID: SV-225023r958448
```

Rationale:

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.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182

Audit:

Verify the US DoD CCEB Interoperability Root CA cross-certificate is installed on unclassified systems as an Untrusted Certificate.

Run "PowerShell" as an administrator.

Execute the following command:

```
Get-ChildItem -Path Cert:Localmachine\disallowed | Where Issuer -Like "*CCEB Interoperability*" | FL Subject, Issuer, Thumbprint, NotAfter
```

If the following certificate "Subject", "Issuer", and "Thumbprint" information is not displayed, this is a finding.

```
Subject: CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U.S. Government, C=US
Issuer: CN=US DoD CCEB Interoperability Root CA 2, OU=PKI, OU=DoD, O=U.S. Government, C=US
Thumbprint: 9B74964506C7ED9138070D08D5F8B969866560C8
NotAfter: 7/18/2025
```

Alternately use the Certificates MMC snap-in:

Run "MMC".

Select "File", "Add/Remove Snap-in".

Select "Certificates", click "Add".

Select "Computer account", click "Next".

Select "Local computer: (the computer this console is running on)", click "Finish".

Click "OK".

Expand "Certificates" and navigate to "Untrusted Certificates >> Certificates".

For each certificate with "US DoD CCEB Interoperability Root CA …" under "Issued By":

Right-click on the certificate and select "Open".

Select the "Details" tab.

Scroll to the bottom and select "Thumbprint".

If the certificate below is not listed or the value for the "Thumbprint" field is not as noted, this is a finding.

```
Subject: CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U.S. Government, C=US
Issuer: CN=US DoD CCEB Interoperability Root CA 2, OU=PKI, OU=DoD, O=U.S.
Government, C=US
Thumbprint: 9B74964506C7ED9138070D08D5F8B969866560C8
NotAfter: 7/18/2025
```

Remediation:

Install the US DoD CCEB Interoperability Root CA cross-certificate on unclassified systems.


```
Subject: CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U.S. Government, C=US
Issuer: CN=US DoD CCEB Interoperability Root CA 2, OU=PKI, OU=DoD, O=U.S.
Government, C=US
Thumbprint: 9B74964506C7ED9138070D08D5F8B969866560C8
NotAfter: 7/18/2025
```


The certificates can be installed using the InstallRoot tool. The tool and user guide are available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. Certificate bundles published by the PKI can be found at https://crl.gds.disa.mil/.

Additional Information:

CCI-000185

For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53A :: IA-5 (2).1
- NIST SP 800-53 Revision 4 :: IA-5 (2) (a)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (b) (1)

CCI-002470

Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4 :: SC-23 (5)
- NIST SP 800-53 Revision 5 :: SC-23 (5)

1.206 WN16-SO-000010 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 built-in guest account must be disabled.

```
GROUP ID: V-225024
RULE ID: SV-225024r958504
```

Rationale:

A system faces an increased vulnerability threat if the built-in guest account is not disabled. This 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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> Security Options
```

If the value for "Accounts: Guest account status" is not set to "Disabled", this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "EnableGuestAccount" equals "1" in the file, this is a finding.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Accounts: Guest account status"
```

to "Disabled".

References:

1. CIS Recommendation: Accounts: Guest account status
2. GRID: MS-00000054

Additional Information:

CCI-000804

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

- NIST SP 800-53 :: IA-8
- NIST SP 800-53A :: IA-8.1
- NIST SP 800-53 Revision 4 :: IA-8
- NIST SP 800-53 Revision 5 :: IA-8

1.207 WN16-SO-000020 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Local accounts with blank passwords must be restricted to prevent access from the network.

```
GROUP ID: V-225025
RULE ID: SV-225025r991589
```

Rationale:

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 does exist, enabling this setting will prevent network access, limiting the account to local console logon only.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\

Value Name: LimitBlankPasswordUse

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Accounts: Limit local account use of blank passwords to console logon only
2. GRID: MS-00000055

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.208 WN16-SO-000030 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 built-in administrator account must be renamed.

```
GROUP ID: V-225026
RULE ID: SV-225026r991589
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> Security Options
```

If the value for "Accounts: Rename administrator account" is not set to a value other than "Administrator", this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "NewAdministratorName" is not something other than "Administrator" in the file, this is a finding.

Remediation:

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".

References:

1. CIS Recommendation: Accounts: Rename administrator account
2. GRID: MS-00000056

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.209 WN16-SO-000040 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 built-in guest account must be renamed.

```
GROUP ID: V-225027
RULE ID: SV-225027r991589
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> Security Options
```

If the value for "Accounts: Rename guest account" is not set to a value other than "Guest", this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "NewGuestName" is not something other than "Guest" in the file, this is a finding.

Remediation:

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"
```

References:

1. CIS Recommendation: Accounts: Rename guest account
2. GRID: MS-00000057

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.210 WN16-SO-000050 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Audit policy using subcategories must be enabled.

```
GROUP ID: V-225028
RULE ID: SV-225028r958442
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\

Value Name: SCENoApplyLegacyAuditPolicy

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings
2. GRID: MS-00000058

Additional Information:

CCI-000169

Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a

1.211 WN16-SO-000080 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.

```
GROUP ID: V-225029
RULE ID: SV-225029r958908
```

Rationale:

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.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\

Value Name: RequireSignOrSeal

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Domain member: Digitally encrypt or sign secure channel data (always)
2. GRID: MS-00000064

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.212 WN16-SO-000090 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The setting Domain member: Digitally encrypt secure channel data (when possible) must be configured to enabled.

```
GROUP ID: V-225030
RULE ID: SV-225030r958908
```

Rationale:

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.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\

Value Name: SealSecureChannel

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Domain member: Digitally encrypt secure channel data (when possible)
2. GRID: MS-00000065

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.213 WN16-SO-000100 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The setting Domain member: Digitally sign secure channel data (when possible) must be configured to Enabled.

```
GROUP ID: V-225031
RULE ID: SV-225031r958908
```

Rationale:

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.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\

Value Name: SignSecureChannel

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Domain member: Digitally sign secure channel data (when possible)
2. GRID: MS-00000066

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.214 WN16-SO-000110 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The computer account password must not be prevented from being reset.

```
GROUP ID: V-225032
RULE ID: SV-225032r971545
```

Rationale:

Computer account passwords are changed automatically on a regular basis. Disabling automatic password changes can make the system more vulnerable to malicious access. Frequent password changes can be a significant safeguard for the system. A new password for the computer account will be generated every 30 days.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\

Value Name: DisablePasswordChange

Value Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Domain member: Disable machine account
password changes"
```

to "Disabled".

References:

1. CIS Recommendation: Domain member: Disable machine account password changes
2. GRID: MS-00000067

Additional Information:

CCI-001967

Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4 :: IA-3 (1)
- NIST SP 800-53 Revision 5 :: IA-3 (1)

1.215 WN16-SO-000120 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The maximum age for machine account passwords must be configured to 30 days or less.

```
GROUP ID: V-225033
RULE ID: SV-225033r991589
```

Rationale:

Computer account passwords are changed automatically on a regular basis. This setting controls the maximum password age that a machine account may have. This must be set to no more than 30 days, ensuring the machine changes its password monthly.

Audit:

This is the default configuration for this setting (30 days).

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\

Value Name: MaximumPasswordAge

Value Type: REG_DWORD
Value: 0x0000001e (30) (or less, but not 0)
```

Remediation:

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).

References:

1. CIS Recommendation: Domain member: Maximum machine account password age
2. GRID: MS-00000068

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.216 WN16-SO-000130 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to require a strong session key.

```
GROUP ID: V-225034
RULE ID: SV-225034r958908
```

Rationale:

A computer connecting to a domain controller will establish a secure channel. The secure channel connection may be subject to compromise, such as hijacking or eavesdropping, if strong session keys are not used to establish the connection. Requiring strong session keys enforces 128-bit encryption between systems.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\

Value Name: RequireStrongKey

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

This setting may prevent a system from being joined to a domain if not configured consistently between systems.

Remediation:

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".

References:

1. CIS Recommendation: Domain member: Require strong (Windows 2000 or later) session key
2. GRID: MS-00000069

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.217 WN16-SO-000140 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.

```
GROUP ID: V-225035
RULE ID: SV-225035r958402
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: InactivityTimeoutSecs

Value Type: REG_DWORD
Value: 0x00000384 (900) (or less, excluding "0" which is effectively
disabled)
```

Remediation:

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.

References:

1. CIS Recommendation: Interactive logon: Machine inactivity limit
2. GRID: MS-00000074

Additional Information:

CCI-000057

Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a

1.218 WN16-SO-000150 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The required legal notice must be configured to display before console logon.

```
GROUP ID: V-225036
RULE ID: SV-225036r958390
```

Rationale:

Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: LegalNoticeText

Value Type: REG_SZ
Value: See message text below
```

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.

Remediation:

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.

References:

1. CIS Recommendation: Interactive logon: Message text for users attempting to log on
2. GRID: MS-00000075

Additional Information:

CCI-000048

Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53 :: AC-8 a
- NIST SP 800-53A :: AC-8.1 (ii)
- NIST SP 800-53 Revision 4 :: AC-8 a
- NIST SP 800-53 Revision 5 :: AC-8 a

CCI-000050

Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53 :: AC-8 b
- NIST SP 800-53A :: AC-8.1 (iii)
- NIST SP 800-53 Revision 4 :: AC-8 b
- NIST SP 800-53 Revision 5 :: AC-8 b

CCI-001384

For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53A :: AC-8.2 (i)
- NIST SP 800-53 Revision 4 :: AC-8 c 1
- NIST SP 800-53 Revision 5 :: AC-8 c 1

CCI-001385

For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53A :: AC-8.2 (ii)
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2

CCI-001386

For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53A :: AC-8.2 (ii)
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2

CCI-001387

For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53A :: AC-8.2 (ii)
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2

CCI-001388

For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53A :: AC-8.2 (iii)
- NIST SP 800-53 Revision 4 :: AC-8 c 3
- NIST SP 800-53 Revision 5 :: AC-8 c 3

1.219 WN16-SO-000160 (Automated)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

The Windows dialog box title for the legal banner must be configured with the appropriate text.

```
GROUP ID: V-225037
RULE ID: SV-225037r958390
```

Rationale:

Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: LegalNoticeCaption

Value Type: REG_SZ
Value: See message title options below
```

"DoD Notice and Consent Banner", "US Department of Defense Warning Statement", or an organization-defined equivalent.

If an organization-defined title is used, it can in no case contravene or modify the language of the banner text required in WN16-SO-000150.

Automated tools may only search for the titles defined above. If an organization-defined title is used, a manual review will be required.

Remediation:

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 an organization-defined equivalent.

If an organization-defined title is used, it can in no case contravene or modify the language of the message text required in WN16-SO-000150.

References:

1. CIS Recommendation: Interactive logon: Message title for users attempting to log on
2. GRID: MS-00000076

Additional Information:

CCI-000048

Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53 :: AC-8 a
- NIST SP 800-53A :: AC-8.1 (ii)
- NIST SP 800-53 Revision 4 :: AC-8 a
- NIST SP 800-53 Revision 5 :: AC-8 a

CCI-001384

For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53A :: AC-8.2 (i)
- NIST SP 800-53 Revision 4 :: AC-8 c 1
- NIST SP 800-53 Revision 5 :: AC-8 c 1

CCI-001385

For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53A :: AC-8.2 (ii)
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2

CCI-001386

For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53A :: AC-8.2 (ii)
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2

CCI-001387

For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53A :: AC-8.2 (ii)
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2

CCI-001388

For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53A :: AC-8.2 (iii)
- NIST SP 800-53 Revision 4 :: AC-8 c 3
- NIST SP 800-53 Revision 5 :: AC-8 c 3

1.220 WN16-SO-000180 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Smart Card removal option must be configured to Force Logoff or Lock Workstation.

```
GROUP ID: V-225038
RULE ID: SV-225038r991589
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\

Value Name: scremoveoption

Value Type: REG_SZ
Value: 1 (Lock Workstation) or 2 (Force Logoff)
```

If configuring this on servers causes issues, such as terminating users' remote sessions, and the organization has a policy in place that any other sessions on the servers, such as administrative console logons, are manually locked or logged off when unattended or not in use, this would be acceptable. This must be documented with the ISSO.

Remediation:

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".

References:

1. CIS Recommendation: Interactive logon: Smart card removal behavior
2. GRID: MS-00000080

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.221 WN16-SO-000190 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.

```
GROUP ID: V-225039
RULE ID: SV-225039r958908
```

Rationale:

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.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\

Value Name: RequireSecuritySignature

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Microsoft network client: Digitally sign
communications (always)"
```

to "Enabled".

References:

1. CIS Recommendation: Microsoft network client: Digitally sign communications (always)
2. GRID: MS-00000081

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.222 WN16-SO-000200 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.

```
GROUP ID: V-225040
RULE ID: SV-225040r958908
```

Rationale:

The server message block (SMB) protocol provides the basis for many network operations. If this policy is enabled, the SMB client will request packet signing when communicating with an SMB server that is enabled or required to perform SMB packet signing.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\

Value Name: EnableSecuritySignature

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Microsoft network client: Digitally sign
communications (if server agrees)"
```

to "Enabled".

References:

1. CIS Recommendation: Microsoft network client: Digitally sign communications (if server agrees)
2. GRID: MS-00000082

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.223 WN16-SO-000210 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.

```
GROUP ID: V-225041
RULE ID: SV-225041r987796
```

Rationale:

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 determine if there is a way to support encrypted password authentication.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\

Value Name: EnablePlainTextPassword

Value Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

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".

References:

1. CIS Recommendation: Microsoft Network Client: Send unencrypted password to third-party SMB servers
2. GRID: MS-00000083

Additional Information:

CCI-000197

For password-based authentication, transmit passwords only over cryptographically-protected channels.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 5 :: IA-5 (1) (c)

1.224 WN16-SO-000230 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.

```
GROUP ID: V-225042
RULE ID: SV-225042r958908
```

Rationale:

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.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\

Value Name: RequireSecuritySignature

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Microsoft network server: Digitally sign
communications (always)"
```

to "Enabled".

References:

1. CIS Recommendation: Microsoft network server: Digitally sign communications (always)
2. GRID: MS-00000085

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.225 WN16-SO-000240 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.

```
GROUP ID: V-225043
RULE ID: SV-225043r958908
```

Rationale:

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 negotiate SMB packet signing as requested by the client.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\

Value Name: EnableSecuritySignature

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Microsoft network server: Digitally sign
communications (if client agrees)"
```

to "Enabled".

References:

1. CIS Recommendation: Microsoft network server: Digitally sign communications (if client agrees)
2. GRID: MS-00000086

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.226 WN16-SO-000250 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Anonymous SID/Name translation must not be allowed.

```
GROUP ID: V-225044
RULE ID: SV-225044r991589
```

Rationale:

Allowing anonymous SID/Name translation can provide sensitive information for accessing a system. Only authorized users must be able to perform such translations.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> Security Options
```

If the value for "Network access: Allow anonymous SID/Name translation" is not set to "Disabled", this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas SecurityPolicy /CFG C:\Path\FileName.Txt
```

If "LSAAnonymousNameLookup" equals "1" in the file, this is a finding.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Network access: Allow anonymous SID/Name
translation"
```

to "Disabled".

References:

1. CIS Recommendation: Network access: Allow anonymous SID/Name translation
2. GRID: MS-00000091

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.227 WN16-SO-000260 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.

```
GROUP ID: V-225045
RULE ID: SV-225045r991589
```

Rationale:

Anonymous enumeration of SAM accounts allows anonymous logon users (null session connections) to list all accounts names, thus providing a list of potential points to attack the system.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\

Value Name: RestrictAnonymousSAM

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Network access: Do not allow anonymous enumeration of SAM accounts
2. GRID: MS-00000093

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.228 WN16-SO-000270 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Anonymous enumeration of shares must not be allowed.

```
GROUP ID: V-225046
RULE ID: SV-225046r958524
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\

Value Name: RestrictAnonymous

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Network access: Do not allow anonymous enumeration of SAM accounts and shares
2. GRID: MS-00000092

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53A :: SC-4.1
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4

1.229 WN16-SO-000290 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.

```
GROUP ID: V-225047
RULE ID: SV-225047r991589
```

Rationale:

Access by anonymous users must be restricted. If this setting is enabled, anonymous users have the same rights and permissions as the built-in Everyone group. Anonymous users must not have these permissions or rights.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\

Value Name: EveryoneIncludesAnonymous

Value Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

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".

References:

1. CIS Recommendation: Network access: Let Everyone permissions apply to anonymous users
2. GRID: MS-00000095

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.230 WN16-SO-000300 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Anonymous access to Named Pipes and Shares must be restricted.

```
GROUP ID: V-225048
RULE ID: SV-225048r958524
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\

Value Name: RestrictNullSessAccess

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Network access: Restrict anonymous access to Named Pipes and Shares
2. GRID: MS-00000099

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53A :: SC-4.1
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4

1.231 WN16-SO-000320 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.

```
GROUP ID: V-225049
RULE ID: SV-225049r991589
```

Rationale:

Services using Local System that use Negotiate when reverting to NTLM authentication may gain unauthorized access if allowed to authenticate anonymously versus using the computer identity.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\LSA\

Value Name: UseMachineId

Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Network security: Allow Local System to use
computer identity for NTLM"
```

to "Enabled".

References:

1. CIS Recommendation: Network security: Allow Local System to use computer identity for NTLM
2. GRID: MS-00000103

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.232 WN16-SO-000330 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

NTLM must be prevented from falling back to a Null session.

```
GROUP ID: V-225050
RULE ID: SV-225050r991589
```

Rationale:

NTLM sessions that are allowed to fall back to Null (unauthenticated) sessions may gain unauthorized access.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\LSA\MSV1_0\

Value Name: allownullsessionfallback

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "Network security: Allow LocalSystem NULL
session fallback"
```

to "Disabled".

References:

1. CIS Recommendation: Network security: Allow LocalSystem NULL session fallback
2. GRID: MS-00000104

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.233 WN16-SO-000340 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

PKU2U authentication using online identities must be prevented.

```
GROUP ID: V-225051
RULE ID: SV-225051r991589
```

Rationale:

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.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\LSA\pku2u\

Value Name: AllowOnlineID

Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

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".

References:

1. CIS Recommendation: Network security: Allow PKU2U authentication requests to this computer to use online identities
2. GRID: MS-00000105

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.234 WN16-SO-000350 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.

```
GROUP ID: V-225052
RULE ID: SV-225052r971535
```

Rationale:

Certain encryption types are no longer considered secure. The DES and RC4 encryption suites must not be used for Kerberos encryption.

Note: Organizations with domain controllers running earlier versions of Windows where RC4 encryption is enabled, selecting "The other domain supports Kerberos AES Encryption" on domain trusts, may be required to allow client communication across the trust relationship.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameter
s\

Value Name: SupportedEncryptionTypes

Value Type: REG_DWORD
Value: 0x7ffffff8 (2147483640)
```

Remediation:

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
Note: Organizations with domain controllers running earlier versions of Windows where RC4 encryption is enabled, selecting "The other domain supports Kerberos AES Encryption" on domain trusts, may be required to allow client communication across the trust relationship.

References:

1. CIS Recommendation: Network security: Configure encryption types allowed for Kerberos
2. GRID: MS-00000106

Additional Information:

CCI-000803

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53 :: IA-7
- NIST SP 800-53A :: IA-7.1
- NIST SP 800-53 Revision 4 :: IA-7
- NIST SP 800-53 Revision 5 :: IA-7

1.235 WN16-SO-000360 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.

```
GROUP ID: V-225053
RULE ID: SV-225053r982199
```

Rationale:

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 a LAN Manager hash of the password is stored in the SAM the next time the password is changed.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\

Value Name: NoLMHash

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: Network security: Do not store LAN Manager hash value on next password change
2. GRID: MS-00000107

Additional Information:

CCI-000196

The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)

1.236 WN16-SO-000380 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.

```
GROUP ID: V-225054
RULE ID: SV-225054r991589
```

Rationale:

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 standalone or nondomain-joined computers that are running later versions.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\

Value Name: LmCompatibilityLevel

Value Type: REG_DWORD
Value: 0x00000005 (5)
```

Remediation:

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".

References:

1. CIS Recommendation: Network security: LAN Manager authentication level
2. GRID: MS-00000109

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.237 WN16-SO-000390 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.

```
GROUP ID: V-225055
RULE ID: SV-225055r991589
```

Rationale:

This setting controls the signing requirements for LDAP clients. This must be set to "Negotiate signing" or "Require signing", depending on the environment and type of LDAP server in use.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\LDAP\

Value Name: LDAPClientIntegrity

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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.

References:

1. CIS Recommendation: Network security: LDAP client signing requirements
2. GRID: MS-00000110

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.238 WN16-SO-000400 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.

```
GROUP ID: V-225056
RULE ID: SV-225056r991589
```

Rationale:

Microsoft has implemented a variety of security support providers for use with Remote Procedure Call (RPC) sessions. All of the options must be enabled to ensure the maximum security level.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\

Value Name: NTLMMinClientSec

Value Type: REG_DWORD
Value: 0x20080000 (537395200)
```

Remediation:

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).

References:

1. CIS Recommendation: Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
2. GRID: MS-00000111

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.239 WN16-SO-000410 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.

```
GROUP ID: V-225057
RULE ID: SV-225057r991589
```

Rationale:

Microsoft has implemented a variety of security support providers for use with Remote Procedure Call (RPC) sessions. All of the options must be enabled to ensure the maximum security level.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\

Value Name: NTLMMinServerSec

Value Type: REG_DWORD
Value: 0x20080000 (537395200)
```

Remediation:

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"
```
```o "Require NTLMv2 session security" and "Require 128-bit encryption" (all
options selected).
```

References:

1. CIS Recommendation: Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
2. GRID: MS-00000112

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.240 WN16-SO-000420 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Users must be required to enter a password to access private keys stored on the computer.

```
GROUP ID: V-225058
RULE ID: SV-225058r958450
```

Rationale:

If the private key is discovered, an attacker can use the key to authenticate as an authorized user and gain access to the network infrastructure.

The cornerstone of the PKI is the private key used to encrypt or digitally sign information.

If the private key is stolen, this will lead to the compromise of the authentication and non-repudiation gained through PKI because the attacker can use the private key to digitally sign documents and pretend to be the authorized user.

Both the holders of a digital certificate and the issuing authority must protect the computers, storage devices, or whatever they use to keep the private keys.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Cryptography\

Value Name: ForceKeyProtection

Type: REG_DWORD
Value: 0x00000002 (2)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "System cryptography: Force strong key
protection for user keys stored on the computer"
```

to "User must enter a password each time they use a key".

Additional Information:

CCI-000186

For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53A :: IA-5 (2).1
- NIST SP 800-53 Revision 4 :: IA-5 (2) (b)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (a) (1)

1.241 WN16-SO-000430 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.

```
GROUP ID: V-225059
RULE ID: SV-225059r958408
```

Rationale:

This setting ensures 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.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000478-GPOS-00223

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\

Value Name: Enabled

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Clients with this setting enabled will not be able to communicate via digitally encrypted or signed protocols with servers that do not support these algorithms. Both the browser and web server must be configured to use TLS; otherwise. the browser will not be able to connect to a secure site.

Remediation:

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".

Additional Information:

CCI-000068

Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)

CCI-002450

Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4 :: SC-13
- NIST SP 800-53 Revision 5 :: SC-13 b

1.242 WN16-SO-000450 (Automated)

Profile Applicability:

- DC SEVERITY: CAT III
- MS SEVERITY: CAT III

Description:

The default permissions of global system objects must be strengthened.

```
GROUP ID: V-225060
RULE ID: SV-225060r991589
```

Rationale:

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 Discretionary Access Control List (DACL) that specifies who can access the objects with what permissions. When this policy is enabled, the default DACL is stronger, allowing non-administrative users to read shared objects but not to modify shared objects they did not create.

Audit:

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Control\Session Manager\

Value Name: ProtectionMode

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: System objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links)
2. GRID: MS-00000119

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.243 WN16-SO-000460 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

User Account Control approval mode for the built-in Administrator must be enabled.

```
GROUP ID: V-225061
RULE ID: SV-225061r1050790
```

Rationale:

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.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Audit:

UAC requirements are NA for Server Core installations (this is the default installation option for Windows Server 2016 versus Server with Desktop Experience) as well as Nano Server.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: FilterAdministratorToken

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: User Account Control: Admin Approval Mode for the Built-in Administrator account
2. GRID: MS-00000120

Additional Information:

CCI-002038

The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11
- NIST SP 800-53 Revision 5 :: IA-11

1.244 WN16-SO-000470 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.

```
GROUP ID: V-225062
RULE ID: SV-225062r958518
```

Rationale:

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting prevents User Interface Accessibility programs from disabling the secure desktop for elevation prompts.

Audit:

UAC requirements are NA for Server Core installations (this is the default installation option for Windows Server 2016 versus Server with Desktop Experience) as well as Nano Server.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: EnableUIADesktopToggle

Value Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> Security Options >> "User Account Control: Allow UIAccess
applications to prompt for elevation without using the secure desktop"
```

to "Disabled".

Additional Information:

CCI-001084

Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3

1.245 WN16-SO-000480 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.

```
GROUP ID: V-225063
RULE ID: SV-225063r958518
```

Rationale:

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.

Audit:

UAC requirements are NA for Server Core installations (this is default installation option for Windows Server 2016 versus Server with Desktop Experience) as well as Nano Server.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: ConsentPromptBehaviorAdmin

Value Type: REG_DWORD
Value: 0x00000002 (2) (Prompt for consent on the secure desktop)
0x00000001 (1) (Prompt for credentials on the secure desktop)
```

Remediation:

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".

The more secure option for this setting, "Prompt for credentials on the secure desktop", would also be acceptable.

References:

1. CIS Recommendation: User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
2. GRID: MS-00000121

Additional Information:

CCI-001084

Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3

1.246 WN16-SO-000490 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

User Account Control must automatically deny standard user requests for elevation.

```
GROUP ID: V-225064
RULE ID: SV-225064r1050790
```

Rationale:

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting controls the behavior of elevation when requested by a standard user account.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Audit:

UAC requirements are NA for Server Core installations (this is the default installation option for Windows Server 2016 versus Server with Desktop Experience) as well as Nano Server.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: ConsentPromptBehaviorUser

Value Type: REG_DWORD
Value: 0x00000000 (0)
```

Remediation:

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".

References:

1. CIS Recommendation: User Account Control: Behavior of the elevation prompt for standard users
2. GRID: MS-00000122

Additional Information:

CCI-002038

The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11
- NIST SP 800-53 Revision 5 :: IA-11

1.247 WN16-SO-000500 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

User Account Control must be configured to detect application installations and prompt for elevation.

```
GROUP ID: V-225065
RULE ID: SV-225065r958518
```

Rationale:

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.

Audit:

UAC requirements are NA for Server Core installations (this is the default installation option for Windows Server 2016 versus Server with Desktop Experience) as well as Nano Server.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: EnableInstallerDetection

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: User Account Control: Detect application installations and prompt for elevation
2. GRID: MS-00000123

Additional Information:

CCI-001084

Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3

1.248 WN16-SO-000510 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

User Account Control must only elevate UIAccess applications that are installed in secure locations.

```
GROUP ID: V-225066
RULE ID: SV-225066r958518
```

Rationale:

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.

Audit:

UAC requirements are NA for Server Core installations (this is the default installation option for Windows Server 2016 versus Server with Desktop Experience) as well as Nano Server.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: EnableSecureUIAPaths

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: User Account Control: Only elevate UIAccess applications that are installed in secure locations
2. GRID: MS-00000124

Additional Information:

CCI-001084

Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3

1.249 WN16-SO-000520 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

User Account Control must run all administrators in Admin Approval Mode, enabling UAC.

```
GROUP ID: V-225067
RULE ID: SV-225067r1050790
```

Rationale:

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting enables UAC.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Audit:

UAC requirements are NA for Server Core installations (this is the default installation option for Windows Server 2016 versus Server with Desktop Experience) as well as Nano Server.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: EnableLUA

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: User Account Control: Run all administrators in Admin Approval Mode
2. GRID: MS-00000125

Additional Information:

CCI-002038

The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11
- NIST SP 800-53 Revision 5 :: IA-11

1.250 WN16-SO-000530 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

User Account Control must virtualize file and registry write failures to per-user locations.

```
GROUP ID: V-225068
RULE ID: SV-225068r958518
```

Rationale:

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.

Audit:

UAC requirements are NA for Server Core installations (this is the default installation option for Windows Server 2016 versus Server with Desktop Experience) as well as Nano Server.

If the following registry value does not exist or is not configured as specified, this is a finding.

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: EnableVirtualization

Value Type: REG_DWORD
Value: 0x00000001 (1)
```

Remediation:

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".

References:

1. CIS Recommendation: User Account Control: Virtualize file and registry write failures to per-user locations
2. GRID: MS-00000127

Additional Information:

CCI-001084

Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3

1.251 WN16-UC-000030 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

Zone information must be preserved when saving attachments.

```
GROUP ID: V-225069
RULE ID: SV-225069r991589
```

Rationale:

Attachments from outside sources may contain malicious code. Preserving zone of origin (Internet, intranet, local, restricted) information on file attachments allows Windows to determine risk.

Audit:

The default behavior is for Windows to mark file attachments with their zone information.

If the registry Value Name below does not exist, this is not a finding.

If it exists and is configured with a value of "2", this is not a finding.

If it exists and is configured with a value of "1", this is a finding.

```
Registry Hive: HKEY_CURRENT_USER
Registry Path:
\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Attachments\

Value Name: SaveZoneInformation

Value Type: REG_DWORD
Value: 0x00000002 (2) (or if the Value Name does not exist)
```

Remediation:

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".

References:

1. CIS Recommendation: Do not preserve zone information in file attachments
2. GRID: MS-00000559

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b

1.252 WN16-UR-000010 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.

```
GROUP ID: V-225070
RULE ID: SV-225070r958726
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to Local

```
Computer Policy >> Computer Configuration >> Windows Settings >> Security
Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups are granted the "Access Credential Manager as a trusted caller" user right, this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs are granted the "SeTrustedCredManAccessPrivilege" user right, this is a finding.

Remediation:

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).

References:

1. CIS Recommendation: Access Credential Manager as a trusted caller
2. GRID: MS-00000012

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.253 WN16-UR-000030 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

The Act as part of the operating system user right must not be assigned to any groups or accounts.

```
GROUP ID: V-225071
RULE ID: SV-225071r958726
```

Rationale:

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 the user is authorized to access. Any accounts with this right can take complete control of a system.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups (to include administrators), are granted the "Act as part of the operating system" user right, this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs are granted the "SeTcbPrivilege" user right, this is a finding.

If an application requires this user right, this would not be a finding.

Vendor documentation must support the requirement for having the user right.

The requirement must be documented with the ISSO.

The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Passwords for accounts with this user right must be protected as highly privileged accounts.

Remediation:

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).

References:

1. CIS Recommendation: Act as part of the operating syste
2. GRID: MS-00000014

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.254 WN16-UR-000050 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Allow log on locally user right must only be assigned to the Administrators group.

```
GROUP ID: V-225072
RULE ID: SV-225072r958472
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Allow log on locally" user right, this is a finding.

- Administrators

For server core installations, run the following command:
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
Review the text file.
If any SIDs other than the following are granted the "SeInteractiveLogonRight" user right, this is a finding.

- S-1-5-32-544 (Administrators)

If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Allow log on locally"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Allow log on locally
2. GRID: MS-00000017

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53A :: AC-3.1
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3

1.255 WN16-UR-000070 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Back up files and directories user right must only be assigned to the Administrators group.

```
GROUP ID: V-225073
RULE ID: SV-225073r958726
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Back up files and directories" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeBackupPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Back up files and directories"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Back up files and directories
2. GRID: MS-00000019

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.256 WN16-UR-000080 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Create a pagefile user right must only be assigned to the Administrators group.

```
GROUP ID: V-225074
RULE ID: SV-225074r958726
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Create a pagefile" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeCreatePagefilePrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Create a pagefile"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Create a pagefile
2. GRID: MS-00000022

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.257 WN16-UR-000090 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

The Create a token object user right must not be assigned to any groups or accounts.

```
GROUP ID: V-225091
RULE ID: SV-225091r958726
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups are granted the "Create a token object" user right, this is a finding.

If an application requires this user right, this would not be a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs are granted the "SeCreateTokenPrivilege" user right, this is a finding.

Vendor documentation must support the requirement for having the user right.

The requirement must be documented with the ISSO.

The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Passwords for application accounts with this user right must be protected as highly privileged accounts.

Remediation:

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).

References:

1. CIS Recommendation: Create a token object
2. GRID: MS-00000023

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.258 WN16-UR-000100 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.

```
GROUP ID: V-225076
RULE ID: SV-225076r958726
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Create global objects" user right, this is a finding.

- Administrators
- Service
- Local Service
- Network Service

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeCreateGlobalPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)
- S-1-5-6 (Service)
- S-1-5-19 (Local Service)
- S-1-5-20 (Network Service)

If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Create global objects"
```

to include only the following accounts or groups:

- Administrators
- Service
- Local Service
- Network Service

References:

1. CIS Recommendation: Create global objects
2. GRID: MS-00000024

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.259 WN16-UR-000110 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Create permanent shared objects user right must not be assigned to any groups or accounts.

```
GROUP ID: V-225077
RULE ID: SV-225077r958726
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups are granted the "Create permanent shared objects" user right, this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs are granted the "SeCreatePermanentPrivilege" user right, this is a finding.

Remediation:

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).

References:

1. CIS Recommendation: Create permanent shared objects
2. GRID: MS-00000025

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.260 WN16-UR-000120 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Create symbolic links user right must only be assigned to the Administrators group.

```
GROUP ID: V-225078
RULE ID: SV-225078r958726
```

Rationale:

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 expose the system to attack.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Create symbolic links" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeCreateSymbolicLinkPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

Systems that have the Hyper-V role will also have "Virtual Machines" given this user right (this may be displayed as "NT Virtual Machine\Virtual Machines", SID S-1-5-83-0). This is not a finding.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Create symbolic links"
```

to include only the following accounts or groups:

- Administrators

Systems that have the Hyper-V role will also have "Virtual Machines" given this user right. If this needs to be added manually, enter it as "NT Virtual Machine\Virtual Machines".

References:

1. CIS Recommendation: Create symbolic links
2. GRID: MS-00000026

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.261 WN16-UR-000130 (Automated)

Profile Applicability:

- DC SEVERITY: CAT I
- MS SEVERITY: CAT I

Description:

The Debug programs user right must only be assigned to the Administrators group.

```
GROUP ID: V-225079
RULE ID: SV-225079r958726
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Debug programs" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeDebugPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).
Passwords for application accounts with this user right must be protected as highly privileged accounts.

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Debug programs"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Debug programs
2. GRID: MS-00000027

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.262 WN16-UR-000200 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Force shutdown from a remote system user right must only be assigned to the Administrators group.

```
GROUP ID: V-225080
RULE ID: SV-225080r958726
```

Rationale:

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 denial of service.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Force shutdown from a remote system" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeRemoteShutdownPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

Remediation:

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Force shutdown from a remote system" to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Force shutdown from a remote system
2. GRID: MS-00000034

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.263 WN16-UR-000210 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Generate security audits user right must only be assigned to Local Service and Network Service.

```
GROUP ID: V-225081
RULE ID: SV-225081r958726
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Generate security audits" user right specifies users and processes that can generate Security Log audit records, which must only be the system service accounts defined.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Generate security audits" user right, this is a finding.

- Local Service
- Network Service

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeAuditPrivilege" user right, this is a finding.

- S-1-5-19 (Local Service)
- S-1-5-20 (Network Service)

If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Generate security audits" to include only the following accounts or groups:

- Local Service
- Network Service

References:

1. CIS Recommendation: Generate security audits
2. GRID: MS-00000035

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.264 WN16-UR-000220 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.

```
GROUP ID: V-225082
RULE ID: SV-225082r958726
```

Rationale:

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 use this to elevate privileges.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Impersonate a client after authentication" user right, this is a finding.

- Administrators
- Service
- Local Service
- Network Service

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeImpersonatePrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)
- S-1-5-6 (Service)
- S-1-5-19 (Local Service)
- S-1-5-20 (Network Service)

If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Impersonate a client after
authentication"
```

to include only the following accounts or groups:

- Administrators
- Service
- Local Service
- Network Service

References:

1. CIS Recommendation: Impersonate a client after authentication
2. GRID: MS-00000036

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.265 WN16-UR-000230 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Increase scheduling priority user right must only be assigned to the Administrators group.

```
GROUP ID: V-225083
RULE ID: SV-225083r958726
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the "Increase scheduling priority" user right can change a scheduling priority, causing performance issues or a denial of service.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Increase scheduling priority" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeIncreaseBasePriorityPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Increase scheduling priority"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Increase scheduling priority
2. GRID: MS-00000037

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.266 WN16-UR-000240 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Load and unload device drivers user right must only be assigned to the Administrators group.

```
GROUP ID: V-225084
RULE ID: SV-225084r958726
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The "Load and unload device drivers" user right allows a user to load device drivers dynamically on a system. This could be used by an attacker to install malicious code.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Load and unload device drivers" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeLoadDriverPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Load and unload device drivers"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Load and unload device drivers
2. GRID: MS-00000038

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.267 WN16-UR-000250 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Lock pages in memory user right must not be assigned to any groups or accounts.

```
GROUP ID: V-225085
RULE ID: SV-225085r958726
```

Rationale:

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 denial of service.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups are granted the "Lock pages in memory" user right, this is a finding.

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs are granted the "SeLockMemoryPrivilege" user right, this is a finding.

If an application requires this user right, this would not be a finding.

Vendor documentation must support the requirement for having the user right.

The requirement must be documented with the ISSO.

The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

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).

References:

1. CIS Recommendation: Lock pages in memory
2. GRID: MS-00000039

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.268 WN16-UR-000260 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Manage auditing and security log user right must only be assigned to the Administrators group.

```
GROUP ID: V-225086
RULE ID: SV-225086r958434
```

Rationale:

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the "Manage auditing and security log" user right can manage the security log and change auditing configurations. This could be used to clear evidence of tampering.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000063-GPOS-00032, SRG-OS-000337-GPOS-00129

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Manage auditing and security log" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeSecurityPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

If the organization has an Auditors group, the assignment of this group to the user right would not be a finding.
If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Manage auditing and security log" to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Manage auditing and security log
2. GRID: MS-00000042

Additional Information:

CCI-000162

Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53A :: AU-9.1
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a

CCI-000163

Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53A :: AU-9.1
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a

CCI-000164

Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53A :: AU-9.1
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a

CCI-000171

Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53 :: AU-12 b
- NIST SP 800-53A :: AU-12.1 (iii)
- NIST SP 800-53 Revision 4 :: AU-12 b
- NIST SP 800-53 Revision 5 :: AU-12 b

CCI-001914

Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 4 :: AU-12 (3)
- NIST SP 800-53 Revision 5 :: AU-12 (3)

1.269 WN16-UR-000270 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Modify firmware environment values user right must only be assigned to the Administrators group.

```
GROUP ID: V-225087
RULE ID: SV-225087r958726
```

Rationale:

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 denial of service.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Modify firmware environment values" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeSystemEnvironmentPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Modify firmware environment values"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Modify firmware environment values
2. GRID: MS-00000044

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.270 WN16-UR-000280 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Perform volume maintenance tasks user right must only be assigned to the Administrators group.

```
GROUP ID: V-225088
RULE ID: SV-225088r958726
```

Rationale:

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. This could be used to delete volumes, resulting in data loss or a denial of service.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If an application requires this user right, this is not a finding.

Vendor documentation must support the requirement for having the user right.

The requirement must be documented with the ISSO.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeManageVolumePrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> Perform volume maintenance tasks
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Perform volume maintenance tasks
2. GRID: MS-00000045

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.271 WN16-UR-000290 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Profile single process user right must only be assigned to the Administrators group.

```
GROUP ID: V-225089
RULE ID: SV-225089r958726
```

Rationale:

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 use this to identify processes to attack.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Profile single process" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeProfileSingleProcessPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Profile single process"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Profile single process
2. GRID: MS-00000046

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.272 WN16-UR-000300 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Restore files and directories user right must only be assigned to the Administrators group.

```
GROUP ID: V-225092
RULE ID: SV-225092r958726
```

Rationale:

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 overwrite more current data.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Restore files and directories" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeRestorePrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Restore files and directories"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Restore files and directories
2. GRID: MS-00000049

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.273 WN16-UR-000310 (Automated)

Profile Applicability:

- DC SEVERITY: CAT II
- MS SEVERITY: CAT II

Description:

The Take ownership of files or other objects user right must only be assigned to the Administrators group.

```
GROUP ID: V-225093
RULE ID: SV-225093r958726
```

Rationale:

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.

Audit:

Verify the effective setting in Local Group Policy Editor.

Run "gpedit.msc".

Navigate to

```
Local Computer Policy >> Computer Configuration >> Windows Settings >>
Security Settings >> Local Policies >> User Rights Assignment
```

If any accounts or groups other than the following are granted the "Take ownership of files or other objects" user right, this is a finding.

- Administrators

For server core installations, run the following command:

```
Secedit /Export /Areas User_Rights /cfg c:\path\filename.txt
```

Review the text file.

If any SIDs other than the following are granted the "SeTakeOwnershipPrivilege" user right, this is a finding.

- S-1-5-32-544 (Administrators)

If an application requires this user right, this would not be a finding.
Vendor documentation must support the requirement for having the user right.
The requirement must be documented with the ISSO.
The application account must meet requirements for application account passwords, such as length (WN16-00-000060) and required frequency of changes (WN16-00-000070).

Remediation:

Configure the policy value for

```
Computer Configuration >> Windows Settings >> Security Settings >> Local
Policies >> User Rights Assignment >> "Take ownership of files or other
objects"
```

to include only the following accounts or groups:

- Administrators

References:

1. CIS Recommendation: Take ownership of files or other objects
2. GRID: MS-00000052

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	WN16-00-000010 (Manual)	☐	☐
1.2	WN16-00-000030 (Manual)	☐	☐
1.3	WN16-00-000040 (Manual)	☐	☐
1.4	WN16-00-000050 (Manual)	☐	☐
1.5	WN16-00-000060 (Manual)	☐	☐
1.6	WN16-00-000070 (Manual)	☐	☐
1.7	WN16-00-000080 (Manual)	☐	☐
1.8	WN16-00-000090 (Manual)	☐	☐
1.9	WN16-00-000100 (Manual)	☐	☐
1.10	WN16-00-000110 (Manual)	☐	☐
1.11	WN16-00-000120 (Manual)	☐	☐
1.12	WN16-00-000140 (Manual)	☐	☐
1.13	WN16-00-000150 (Manual)	☐	☐
1.14	WN16-00-000160 (Manual)	☐	☐
1.15	WN16-00-000170 (Manual)	☐	☐
1.16	WN16-00-000180 (Manual)	☐	☐
1.17	WN16-00-000190 (Manual)	☐	☐
1.18	WN16-00-000200 (Manual)	☐	☐
1.19	WN16-00-000210 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	WN16-00-000220 (Manual)	☐	☐
1.21	WN16-00-000230 (Manual)	☐	☐
1.22	WN16-00-000240 (Manual)	☐	☐
1.23	WN16-00-000250 (Manual)	☐	☐
1.24	WN16-00-000270 (Manual)	☐	☐
1.25	WN16-00-000280 (Manual)	☐	☐
1.26	WN16-00-000290 (Manual)	☐	☐
1.27	WN16-00-000300 (Manual)	☐	☐
1.28	WN16-00-000310 (Manual)	☐	☐
1.29	WN16-00-000320 (Manual)	☐	☐
1.30	WN16-00-000330 (Manual)	☐	☐
1.31	WN16-00-000340 (Manual)	☐	☐
1.32	WN16-00-000350 (Manual)	☐	☐
1.33	WN16-00-000360 (Manual)	☐	☐
1.34	WN16-00-000370 (Manual)	☐	☐
1.35	WN16-00-000380 (Manual)	☐	☐
1.36	WN16-00-000390 (Manual)	☐	☐
1.37	WN16-00-000400 (Manual)	☐	☐
1.38	WN16-00-000410 (Manual)	☐	☐
1.39	WN16-00-000411 (Automated)	☐	☐
1.40	WN16-00-000412 (Automated)	☐	☐
1.41	WN16-00-000420 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	WN16-00-000430 (Manual)	☐	☐
1.43	WN16-00-000440 (Manual)	☐	☐
1.44	WN16-00-000450 (Manual)	☐	☐
1.45	WN16-00-000460 (Manual)	☐	☐
1.46	WN16-00-000470 (Manual)	☐	☐
1.47	WN16-00-000480 (Manual)	☐	☐
1.48	WN16-AC-000010 (Automated)	☐	☐
1.49	WN16-AC-000020 (Automated)	☐	☐
1.50	WN16-AC-000030 (Automated)	☐	☐
1.51	WN16-AC-000040 (Automated)	☐	☐
1.52	WN16-AC-000050 (Automated)	☐	☐
1.53	WN16-AC-000060 (Automated)	☐	☐
1.54	WN16-AC-000070 (Automated)	☐	☐
1.55	WN16-AC-000080 (Automated)	☐	☐
1.56	WN16-AC-000090 (Automated)	☐	☐
1.57	WN16-AU-000010 (Manual)	☐	☐
1.58	WN16-AU-000020 (Manual)	☐	☐
1.59	WN16-AU-000030 (Manual)	☐	☐
1.60	WN16-AU-000040 (Manual)	☐	☐
1.61	WN16-AU-000050 (Manual)	☐	☐
1.62	WN16-AU-000060 (Manual)	☐	☐
1.63	WN16-AU-000070 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	WN16-AU-000080 (Automated)	☐	☐
1.65	WN16-AU-000100 (Automated)	☐	☐
1.66	WN16-AU-000120 (Automated)	☐	☐
1.67	WN16-AU-000140 (Automated)	☐	☐
1.68	WN16-AU-000150 (Automated)	☐	☐
1.69	WN16-AU-000160 (Automated)	☐	☐
1.70	WN16-AU-000170 (Automated)	☐	☐
1.71	WN16-AU-000230 (Automated)	☐	☐
1.72	WN16-AU-000240 (Automated)	☐	☐
1.73	WN16-AU-000250 (Automated)	☐	☐
1.74	WN16-AU-000260 (Automated)	☐	☐
1.75	WN16-AU-000270 (Automated)	☐	☐
1.76	WN16-AU-000280 (Automated)	☐	☐
1.77	WN16-AU-000285 (Automated)	☐	☐
1.78	WN16-AU-000286 (Automated)	☐	☐
1.79	WN16-AU-000290 (Automated)	☐	☐
1.80	WN16-AU-000300 (Automated)	☐	☐
1.81	WN16-AU-000310 (Automated)	☐	☐
1.82	WN16-AU-000320 (Automated)	☐	☐
1.83	WN16-AU-000330 (Automated)	☐	☐
1.84	WN16-AU-000340 (Automated)	☐	☐
1.85	WN16-AU-000350 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	WN16-AU-000360 (Automated)	☐	☐
1.87	WN16-AU-000370 (Automated)	☐	☐
1.88	WN16-AU-000380 (Automated)	☐	☐
1.89	WN16-AU-000390 (Automated)	☐	☐
1.90	WN16-AU-000400 (Automated)	☐	☐
1.91	WN16-AU-000410 (Automated)	☐	☐
1.92	WN16-AU-000420 (Automated)	☐	☐
1.93	WN16-AU-000440 (Automated)	☐	☐
1.94	WN16-AU-000450 (Automated)	☐	☐
1.95	WN16-CC-000010 (Automated)	☐	☐
1.96	WN16-CC-000030 (Automated)	☐	☐
1.97	WN16-CC-000040 (Automated)	☐	☐
1.98	WN16-CC-000050 (Automated)	☐	☐
1.99	WN16-CC-000060 (Automated)	☐	☐
1.100	WN16-CC-000070 (Automated)	☐	☐
1.101	WN16-CC-000080 (Automated)	☐	☐
1.102	WN16-CC-000090 (Automated)	☐	☐
1.103	WN16-CC-000100 (Automated)	☐	☐
1.104	WN16-CC-000110 (Automated)	☐	☐
1.105	WN16-CC-000140 (Automated)	☐	☐
1.106	WN16-CC-000150 (Automated)	☐	☐
1.107	WN16-CC-000160 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	WN16-CC-000170 (Automated)	☐	☐
1.109	WN16-CC-000180 (Automated)	☐	☐
1.110	WN16-CC-000210 (Automated)	☐	☐
1.111	WN16-CC-000220 (Automated)	☐	☐
1.112	WN16-CC-000240 (Automated)	☐	☐
1.113	WN16-CC-000250 (Automated)	☐	☐
1.114	WN16-CC-000260 (Automated)	☐	☐
1.115	WN16-CC-000270 (Automated)	☐	☐
1.116	WN16-CC-000280 (Automated)	☐	☐
1.117	WN16-CC-000290 (Automated)	☐	☐
1.118	WN16-CC-000300 (Automated)	☐	☐
1.119	WN16-CC-000310 (Automated)	☐	☐
1.120	WN16-CC-000320 (Automated)	☐	☐
1.121	WN16-CC-000330 (Automated)	☐	☐
1.122	WN16-CC-000340 (Automated)	☐	☐
1.123	WN16-CC-000350 (Automated)	☐	☐
1.124	WN16-CC-000360 (Automated)	☐	☐
1.125	WN16-CC-000370 (Automated)	☐	☐
1.126	WN16-CC-000380 (Automated)	☐	☐
1.127	WN16-CC-000390 (Automated)	☐	☐
1.128	WN16-CC-000400 (Automated)	☐	☐
1.129	WN16-CC-000410 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.130	WN16-CC-000420 (Automated)	☐	☐
1.131	WN16-CC-000421 (Automated)	☐	☐
1.132	WN16-CC-000430 (Automated)	☐	☐
1.133	WN16-CC-000440 (Automated)	☐	☐
1.134	WN16-CC-000450 (Automated)	☐	☐
1.135	WN16-CC-000460 (Automated)	☐	☐
1.136	WN16-CC-000470 (Automated)	☐	☐
1.137	WN16-CC-000480 (Automated)	☐	☐
1.138	WN16-CC-000490 (Automated)	☐	☐
1.139	WN16-CC-000500 (Automated)	☐	☐
1.140	WN16-CC-000510 (Automated)	☐	☐
1.141	WN16-CC-000520 (Automated)	☐	☐
1.142	WN16-CC-000530 (Automated)	☐	☐
1.143	WN16-CC-000540 (Automated)	☐	☐
1.144	WN16-CC-000550 (Automated)	☐	☐
1.145	WN16-CC-000555 (Automated)	☐	☐
1.146	WN16-DC-000010 (Manual)	☐	☐
1.147	WN16-DC-000020 (Manual)	☐	☐
1.148	WN16-DC-000030 (Manual)	☐	☐
1.149	WN16-DC-000040 (Manual)	☐	☐
1.150	WN16-DC-000050 (Manual)	☐	☐
1.151	WN16-DC-000060 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.152	WN16-DC-000070 (Manual)	☐	☐
1.153	WN16-DC-000080 (Manual)	☐	☐
1.154	WN16-DC-000090 (Manual)	☐	☐
1.155	WN16-DC-000100 (Manual)	☐	☐
1.156	WN16-DC-000110 (Manual)	☐	☐
1.157	WN16-DC-000120 (Manual)	☐	☐
1.158	WN16-DC-000130 (Manual)	☐	☐
1.159	WN16-DC-000140 (Manual)	☐	☐
1.160	WN16-DC-000150 (Manual)	☐	☐
1.161	WN16-DC-000160 (Manual)	☐	☐
1.162	WN16-DC-000170 (Manual)	☐	☐
1.163	WN16-DC-000180 (Manual)	☐	☐
1.164	WN16-DC-000190 (Manual)	☐	☐
1.165	WN16-DC-000200 (Manual)	☐	☐
1.166	WN16-DC-000210 (Manual)	☐	☐
1.167	WN16-DC-000220 (Manual)	☐	☐
1.168	WN16-DC-000230 (Automated)	☐	☐
1.169	WN16-DC-000240 (Automated)	☐	☐
1.170	WN16-DC-000250 (Automated)	☐	☐
1.171	WN16-DC-000260 (Automated)	☐	☐
1.172	WN16-DC-000280 (Manual)	☐	☐
1.173	WN16-DC-000290 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.174	WN16-DC-000300 (Manual)	☐	☐
1.175	WN16-DC-000310 (Manual)	☐	☐
1.176	WN16-DC-000320 (Automated)	☐	☐
1.177	WN16-DC-000330 (Automated)	☐	☐
1.178	WN16-DC-000340 (Automated)	☐	☐
1.179	WN16-DC-000350 (Automated)	☐	☐
1.180	WN16-DC-000360 (Automated)	☐	☐
1.181	WN16-DC-000370 (Automated)	☐	☐
1.182	WN16-DC-000380 (Automated)	☐	☐
1.183	WN16-DC-000390 (Automated)	☐	☐
1.184	WN16-DC-000400 (Automated)	☐	☐
1.185	WN16-DC-000401 (Automated)	☐	☐
1.186	WN16-DC-000410 (Manual)	☐	☐
1.187	WN16-DC-000420 (Automated)	☐	☐
1.188	WN16-DC-000430 (Manual)	☐	☐
1.189	WN16-MS-000010 (Manual)	☐	☐
1.190	WN16-MS-000020 (Automated)	☐	☐
1.191	WN16-MS-000030 (Automated)	☐	☐
1.192	WN16-MS-000040 (Automated)	☐	☐
1.193	WN16-MS-000050 (Automated)	☐	☐
1.194	WN16-MS-000120 (Automated)	☐	☐
1.195	WN16-MS-000310 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.196	WN16-MS-000340 (Automated)	☐	☐
1.197	WN16-MS-000370 (Manual)	☐	☐
1.198	WN16-MS-000380 (Automated)	☐	☐
1.199	WN16-MS-000390 (Automated)	☐	☐
1.200	WN16-MS-000400 (Automated)	☐	☐
1.201	WN16-MS-000410 (Automated)	☐	☐
1.202	WN16-MS-000420 (Automated)	☐	☐
1.203	WN16-PK-000010 (Manual)	☐	☐
1.204	WN16-PK-000020 (Manual)	☐	☐
1.205	WN16-PK-000030 (Manual)	☐	☐
1.206	WN16-SO-000010 (Automated)	☐	☐
1.207	WN16-SO-000020 (Automated)	☐	☐
1.208	WN16-SO-000030 (Automated)	☐	☐
1.209	WN16-SO-000040 (Automated)	☐	☐
1.210	WN16-SO-000050 (Automated)	☐	☐
1.211	WN16-SO-000080 (Automated)	☐	☐
1.212	WN16-SO-000090 (Automated)	☐	☐
1.213	WN16-SO-000100 (Automated)	☐	☐
1.214	WN16-SO-000110 (Automated)	☐	☐
1.215	WN16-SO-000120 (Automated)	☐	☐
1.216	WN16-SO-000130 (Automated)	☐	☐
1.217	WN16-SO-000140 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.218	WN16-SO-000150 (Automated)	☐	☐
1.219	WN16-SO-000160 (Automated)	☐	☐
1.220	WN16-SO-000180 (Automated)	☐	☐
1.221	WN16-SO-000190 (Automated)	☐	☐
1.222	WN16-SO-000200 (Automated)	☐	☐
1.223	WN16-SO-000210 (Automated)	☐	☐
1.224	WN16-SO-000230 (Automated)	☐	☐
1.225	WN16-SO-000240 (Automated)	☐	☐
1.226	WN16-SO-000250 (Automated)	☐	☐
1.227	WN16-SO-000260 (Automated)	☐	☐
1.228	WN16-SO-000270 (Automated)	☐	☐
1.229	WN16-SO-000290 (Automated)	☐	☐
1.230	WN16-SO-000300 (Automated)	☐	☐
1.231	WN16-SO-000320 (Automated)	☐	☐
1.232	WN16-SO-000330 (Automated)	☐	☐
1.233	WN16-SO-000340 (Automated)	☐	☐
1.234	WN16-SO-000350 (Automated)	☐	☐
1.235	WN16-SO-000360 (Automated)	☐	☐
1.236	WN16-SO-000380 (Automated)	☐	☐
1.237	WN16-SO-000390 (Automated)	☐	☐
1.238	WN16-SO-000400 (Automated)	☐	☐
1.239	WN16-SO-000410 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.240	WN16-SO-000420 (Automated)	☐	☐
1.241	WN16-SO-000430 (Automated)	☐	☐
1.242	WN16-SO-000450 (Automated)	☐	☐
1.243	WN16-SO-000460 (Automated)	☐	☐
1.244	WN16-SO-000470 (Automated)	☐	☐
1.245	WN16-SO-000480 (Automated)	☐	☐
1.246	WN16-SO-000490 (Automated)	☐	☐
1.247	WN16-SO-000500 (Automated)	☐	☐
1.248	WN16-SO-000510 (Automated)	☐	☐
1.249	WN16-SO-000520 (Automated)	☐	☐
1.250	WN16-SO-000530 (Automated)	☐	☐
1.251	WN16-UC-000030 (Automated)	☐	☐
1.252	WN16-UR-000010 (Automated)	☐	☐
1.253	WN16-UR-000030 (Automated)	☐	☐
1.254	WN16-UR-000050 (Automated)	☐	☐
1.255	WN16-UR-000070 (Automated)	☐	☐
1.256	WN16-UR-000080 (Automated)	☐	☐
1.257	WN16-UR-000090 (Automated)	☐	☐
1.258	WN16-UR-000100 (Automated)	☐	☐
1.259	WN16-UR-000110 (Automated)	☐	☐
1.260	WN16-UR-000120 (Automated)	☐	☐
1.261	WN16-UR-000130 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.262	WN16-UR-000200 (Automated)	☐	☐
1.263	WN16-UR-000210 (Automated)	☐	☐
1.264	WN16-UR-000220 (Automated)	☐	☐
1.265	WN16-UR-000230 (Automated)	☐	☐
1.266	WN16-UR-000240 (Automated)	☐	☐
1.267	WN16-UR-000250 (Automated)	☐	☐
1.268	WN16-UR-000260 (Automated)	☐	☐
1.269	WN16-UR-000270 (Automated)	☐	☐
1.270	WN16-UR-000280 (Automated)	☐	☐
1.271	WN16-UR-000290 (Automated)	☐	☐
1.272	WN16-UR-000300 (Automated)	☐	☐
1.273	WN16-UR-000310 (Automated)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
08/26/2024	3.0.0	UPDATE - 18.9.50.1 (L2 -> L1) Ensure 'Enable Windows NTP Client' is set to 'Enabled' Ticket #18467
08/26/2024	3.0.0	UPDATE - 18.9.50.1 (L2 -> L1) Ensure 'Enable Windows NTP Server' is set to 'Disabled' Ticket #18468
08/26/2024	3.0.0	UPDATE - 9 Windows Firewall with Advanced Security TO Windows Defender Firewall with Advanced Security Ticket #18532
08/26/2024	3.0.0	UPDATE - 18.10.42.7 (L2 -> L1) Ensure 'Enable file hash computation feature' is set to 'Enabled' Ticket #19207
08/26/2024	3.0.0	ADD - 18.9.19 (L1) 'Configure security policy processing: Do not apply during periodic background processing' is set to 'False' Ticket #19358
08/26/2024	3.0.0	ADD - 18.9.19 (L1) 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'True' Ticket #19359
08/26/2024	3.0.0	REMOVE - 19.1.3 Accepted (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' Ticket #19361
08/26/2024	3.0.0	REMOVE - 19.1.3 Accepted (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' Ticket #19362

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
08/26/2024	3.0.0	REMOVE - 18.9.38 (L1) Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Audit' or higher (DC only) Ticket #19697
08/26/2024	3.0.0	ADD - 2.3.11 (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' Ticket #19740
08/26/2024	3.0.0	ADD - 2.3.11 (L1) Ensure 'Network security: Restrict NTLM: Audit NTLM authentication in this domain' is set to 'Enable all' (DC only) Ticket #19741
08/26/2024	3.0.0	ADD - 2.3.11 (L1) Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher Ticket #19742
08/26/2024	3.0.0	REMOVE - 2.3.4 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set Ticket #20103
08/26/2024	3.0.0	UPDATE - Section changes from Windows 11 Release 22H2 v3.0 Administrative Templates Ticket #20220
08/26/2024	3.0.0	UPDATE - Section changes from Windows 11 Release 23H2 Administrative Templates Ticket #20324
08/26/2024	3.0.0	ADD - 18.10.42.13 (L1) Ensure 'Scan packed executables' is set to 'Enabled' Ticket #20337

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
08/26/2024	3.0.0	UPDATE - 2.2 (L1) Ensure 'Allow log on locally' is set to 'Administrators' TO 'Administrators, ENTERPRISE DOMAIN CONTROLLERS' (DC only) Ticket #20339
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' TO 'MSS: (AutoAdminLogon) Enable Automatic Logon' Ticket #20355
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' TO 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' Ticket #20357
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' TO 'MSS: (DisableIPSourceRouting) IP source routing protection level' Ticket #20358
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' TO 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses' Ticket #20359
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' TO 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' Ticket #20360

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' TO 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' Ticket #20361
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' TO 'Enabled: 300,000 or 5 minutes' Ticket #20362
08/26/2024	3.0.0	REMOVE - 18.10.24 EMET Ticket #20472
08/26/2024	3.0.0	ADD - 18.4 (L1) Ensure 'Enable Certificate Padding' is set to 'Enabled' Ticket #20521
08/26/2024	3.0.0	REMOVE - 9.1 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' Ticket #20526
08/26/2024	3.0.0	REMOVE - 9.2 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' Ticket #20527
08/26/2024	3.0.0	REMOVE - 9.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' Ticket #20528
08/26/2024	3.0.0	REMOVE - 19.1.3 (L1) Ensure 'Enable screen saver' is set to 'Enabled' Ticket #20634

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
08/26/2024	3.0.0	UPDATE - 18.10.86 (L1 -> L2) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' Ticket #20717
08/26/2024	3.0.0	UPDATE - 18.10.86 (L1 -> L2) Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' Ticket #20718
08/26/2024	3.0.0	UPDATE - 18.6.14 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" for all NETLOGON and SYSVOL shares' TO add “Require Privacy” Ticket #20785
08/26/2024	3.0.0	UPDATE - Section 17 Auditpol commands Ticket #21446
08/26/2024	3.0.0	UPDATE - 2.2 Ensure 'Deny log on as a service' to include 'No one' (STIG DC only) Ticket #21984
08/26/2024	3.0.0	UPDATE - 18.10.75.2 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled' (STIG only) Ticket #21994
08/26/2024	3.0.0	UPDATE - 2.3.17 Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (STIG only) TO 'Prompt for consent on the secure desktop' or higher Ticket #21996
08/26/2024	3.0.0	UPDATE - Firewall UI path Ticket #22051

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
08/26/2024	3.0.0	REMOVE - 17.5 Ensure 'Audit Account Lockout' is set to include 'Success and Failure' (STIG only) Ticket #22260
08/26/2024	3.0.0	ADD - 17.6 Ensure 'Audit Removable Storage' is set to 'Success and Failure' Ticket #22261
08/26/2024	3.0.0	UPDATE - 20 Ensure 'DoD Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems Ticket #22262
08/26/2024	3.0.0	UPDATE - 20 Ensure 'Manually managed application account passwords are 15 characters in length' TO Ensure 'Manually managed application account passwords are 14 characters in length' Ticket #22263
08/26/2024	3.0.0	ADD - 18.10.86 Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' Ticket #22264
08/26/2024	3.0.0	ADD - 18.4 Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' Ticket #22265
08/26/2024	3.0.0	ADD - 20 Ensure 'DoD Root Certificate Authority (CA) certificates' are installed in the 'Trusted Root Store' Ticket #22291
08/26/2024	3.0.0	ADD - 20 Ensure 'US DoD CCEB Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems Ticket #22292

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
10/20/2023	2.0.0	REMOVE - 18.5.4 (L1) Ensure 'Configure DNS over HTTPS (DoH) name resolution' is set to 'Enabled: Allow DoH' or higher Ticket# 15653
10/20/2023	2.0.0	UPDATE - 18.9.89 'Allow Windows Ink Workspace' TO 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled' Ticket# 16103
10/20/2023	2.0.0	ADD - 18.9.47.5.1 'Configure Attack Surface Reduction rules' is set to 'Enable' Ticket# 17076
10/20/2023	2.0.0	UPDATE - Section changes from Windows 11 Release 22H2 Administrative Templates Ticket# 17124
10/20/2023	2.0.0	UPDATE – 18.10.87 (L1) 'Turn on PowerShell Transcription' is set to 'Disabled' TO 'Enabled' Ticket# 17516
10/20/2023	2.0.0	ADD - 1.2 (L1) Ensure 'Allow Administrator account lockout' is set to 'Enabled' Ticket# 17564
10/20/2023	2.0.0	REMOVE - 2.3.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' Ticket# 17565
10/20/2023	2.0.0	ADD - 18.4 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled' Ticket# 17566
10/20/2023	2.0.0	MOVE - 18.4 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' TO 18.7

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
		Ticket# 17567
10/20/2023	2.0.0	ADD - 18.4 (L1) Ensure 'LSA Protection' is set to 'Enabled' Ticket# 17568
10/20/2023	2.0.0	ADD - 18.6.4 (L1) Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks' Ticket# 17569
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled' Ticket# 17570
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP' Ticke # 17572
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default' Ticket# 17573
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP' Ticket# 17575
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections' is set to 'Enabled: Negotiate' or higher Ticket# 17576
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles'

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
		Ticket# 17577
10/20/2023	2.0.0	UPDATE - 18.10.43.6.1 (L1) Ensure 'Configure Attack Surface Reduction rules' with additional ASR rule for "Block abuse of exploited vulnerable signed drivers" Ticket# 17588
10/20/2023	2.0.0	ADD - 18.10.59 (L2) Ensure 'Allow search highlights' is set to 'Disabled' Ticket# 17591
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0' Ticket# 17715
10/20/2023	2.0.0	UPDATE - 9 Windows Firewall with Advanced Security TO Windows Defender Firewall with Advanced Security Ticket #18532
10/20/2023	2.0.0	UPDATE - 2016 STIG 17.4 (L1) Ensure 'Audit Directory Service Changes' is set to include 'Success' and 'Failure TO 'Success' Ticket #20003
10/20/2023	2.0.0	UPDATE - 2016 STIG 18.9.13.2 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' TO 'Enabled: any, but ALL' Ticket #20004
10/20/2023	2.0.0	REMOVE - 2016 STIG 18.4.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) Ticket #20006
10/20/2023	2.0.0	REMOVE - 2016 STIG 20.21 Ensure 'DoD Root Certificate Authority (CA) certificates' are installed in the 'Trusted Root Store'

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
		Ticket #20007
10/20/2023	2.0.0	REMOVE - 2016 STIG 20.69 Ensure 'US DoD CCEB Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems Ticket #20008
04/21/2022	1.4.0	REMOVE - 19.1.3 (L1) Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' Ticket #8782
04/21/2022	1.2.0	ADD - 5 (L1) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) Ticket# 13338
04/21/2022	1.2.0	ADD - 5 (L2) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only) Ticket# 13339
04/21/2022	1.2.0	ADD - 18.6 (L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' Ticket# 13340
04/21/2022	1.2.0	ADD - 18.6 (L1) Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' Ticket# 13341
04/21/2022	1.2.0	ADD - 18.6 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' Ticket# 13343
04/21/2022	1.2.0	ADD - 18.8.7 (L1) Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' Ticket# 13759

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
04/21/2022	1.2.0	ADD - Section changes from Windows 11 Release 21H2 Administrative Templates Ticket# 13968
04/21/2022	1.2.0	RENAME - 9 Windows Firewall with Advanced Security TO Windows Defender Firewall with Advanced Security Ticket# 14034
04/21/2022	1.2.0	RENAME & UPDATE - 18.9.17 (L1) Ensure 'Allow Telemetry' TO (L1) Ensure 'Allow Diagnostic Data' Ticket# 14035
04/21/2022	1.2.0	MOVE - 18.9.103 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' TO 18.9.108.1 Legacy Policies Ticket# 14043
04/21/2022	1.2.0	MOVE - 18.9.103 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' TO 18.9.108.2 Manage end user experience Ticket# 14044
04/21/2022	1.2.0	MOVE - 18.9.103 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' TO 18.9.108.2 Manage end user experience Ticket# 14045
04/21/2022	1.2.0	MOVE & UPDATE - 18.9.103.1 (L1) Ensure 'Manage preview builds' is set to 'Enabled: Disable preview builds' TO 18.9.108.4 (L1) Ensure 'Manage preview builds' is set to 'Disabled' Ticket# 14050
04/21/2022	1.2.0	MOVE & UPDATE - 18.9.103.1 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: Semi-Annual Channel, 180 or more days' TO 18.9.108.4 'Enabled: 180 or more days'

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
		Ticket# 14051
04/21/2022	1.2.0	ADD - 18.3 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' Ticket# 14578
04/21/2022	1.2.0	ADD - 18.5.4 (L1) Ensure 'Configure DNS over HTTPS (DoH) name resolution' is set to 'Enabled: Allow DoH' or higher Ticket# 14579
04/21/2022	1.2.0	ADD - 18.8.40 (L1) Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Audit' or higher (DC only) Ticket# 14580
04/21/2022	1.2.0	ADD - 18.9.14 (L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' Ticket# 14581
04/21/2022	1.2.0	ADD - 18.9.17 (L1) Ensure 'Enable OneSettings Auditing' is set to 'Enabled' Ticket# 14582
04/21/2022	1.2.0	ADD - 18.9.17 (L1) Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' Ticket# 14583
04/21/2022	1.2.0	ADD - 18.9.17 (L1) Ensure 'Limit Dump Collection' is set to 'Enabled' Ticket# 14584
04/21/2022	1.2.0	ADD - 18.9.47.9 (L1) Ensure 'Turn on script scanning' is set to 'Enabled' Ticket# 14585

Date	Version	Changes for this version
08/22/2025	4.0.0	REWRITE - Server 2016 STIG Ticket #25748
04/21/2022	1.2.0	ADD - 19.7.8 (L1) Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' Ticket# 14588
04/21/2022	1.2.0	ADD - 18.9.17 (L1) Ensure 'Disable OneSettings Downloads' is set to 'Enabled' Ticket# 14625
04/21/2022	1.2.0	UPDATE - 18.9.100 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' TO 'Enabled' Ticket# 14637
04/21/2022	1.2.0	UPDATE - 18.8.3 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled' TO 'Enabled' Ticket# 14638
7/30/2021	1.1.0	UPDATE - 1.1.2 (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' TO '365 or fewer days, but not 0' to match updated CIS Password Policy recommendations Ticket #12627
7/30/2021	1.1.0	ADD - Section changes from Windows 10 Release 21H1 Administrative Templates Ticket #12970
7/30/2021	1.1.0	UPDATE - 1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' TO '5 or fewer invalid logon attempt(s), but not 0' Ticket #13188
9/15/2020	1.0.0	Initial Public Release