CIS Cisco IOS Switch NDM STIG Benchmark

v1.0.0 – 07-02-2025

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

Cisco IOS Switch NDM Secure Technical Implementation Guide (STIG)
Version: 3 Release: 5 Benchmark
Date: 02 Jul 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 Cisco IOS Switch NDM 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:

- **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 servers and workstations.

- **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 servers and workstations.

- **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 servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Cisco IOS Switch NDM

Recommendations

1 STIG RULES

Cisco IOS Switch

Cisco IOS Switch NDM Secure Technical Implementation Guide (STIG)

Version: 3 Release: 5 Benchmark

Date: 02 Jul 2025

CLASSIFICATION unclassified

1.1 CISC-ND-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to limit the number of concurrent management sessions to an organization-defined number.

```
GROUP ID: V-220570
RULE ID: SV-220570r960735
```

Rationale:

Device management includes the ability to control the number of administrators and management sessions that manage a device. Limiting the number of allowed administrators and sessions per administrator based on account type, role, or access type is helpful in limiting risks related to DoS attacks.

This requirement addresses concurrent sessions for administrative accounts and does not address concurrent sessions by a single administrator via multiple administrative accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system. At a minimum, limits must be set for SSH, HTTPS, account of last resort, and root account sessions.

Audit:

Note: This requirement is not applicable to file transfer actions such as FTP, SCP, and SFTP.
Review the switch configuration to determine if concurrent management sessions are limited as show in the example below:
ip http secure-server
ip http max-connections 2
…
…
…
For platforms that support the session-limit command:
line vty 0 4
session-limit 2
transport input ssh
For platforms that do not support the session-limit command, the sessions can also be limited by reducing the number of active vty lines as shown in the example below:
line vty 0 1
transport input ssh
line vty 2 4
transport input none
If the switch is not configured to limit the number of concurrent management sessions, this is a finding.

Remediation:

Configure the switch to limit the number of concurrent management sessions to an organization-defined number as shown in the example below:
SW4(config)#ip http max-connections 2
SW4(config)#line vty 0 1
SW4(config)#transport input ssh
SW4(config)#line vty 2 4
SW4(config)#transport input none

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.2 CISC-ND-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to automatically audit account creation.

```
GROUP ID: V-220571
RULE ID: SV-220571r960777
```

Rationale:

Upon gaining access to a network device, an attacker will often first attempt to create a persistent method of reestablishing access. One way to accomplish this is to create a new account. Notification of account creation helps to mitigate this risk.

Auditing account creation provides the necessary reconciliation that account management procedures are being followed. Without this audit trail, personnel without the proper authorization may gain access to critical network nodes.

Audit:

Review the switch configuration to determine if it automatically audits account creation. The configuration should look similar to the example below:
archive
log config
logging enable
Note: Configuration changes can be viewed using the show archive log config all command.
If account creation is not automatically audited, this is a finding.

Remediation:

Configure the switch to log account creation using the following commands:
SW4(config)#archive
SW4(config-archive)#log config
SW4(config-archive-log-cfg)#logging enable
SW4(config-archive-log-cfg)#end

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)

1.3 CISC-ND-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to automatically audit account modification.

```
GROUP ID: V-220572
RULE ID: SV-220572r960780
```

Rationale:

Because the accounts in the network device are privileged or system-level accounts, account management is vital to the security of the network device. Account management by a designated authority ensures access to the network device is being controlled in a secure manner by granting access to only authorized personnel with the appropriate and necessary privileges.

Auditing account modification, along with an automatic notification to appropriate individuals, will provide the necessary reconciliation that account management procedures are being followed. If modifications to management accounts are not audited, reconciliation of account management procedures cannot be tracked.

Audit:

Review the switch configuration to determine if it automatically audits account modification. The configuration should look similar to the example below:
archive
log config
logging enable
Note: Configuration changes can be viewed using the show archive log config all command.
If account modification is not automatically audited, this is a finding.

Remediation:

Configure the switch to log account modification using the following commands:
SW4(config)#archive
SW4(config-archive)#log config
SW4(config-archive-log-cfg)#logging enable
SW4(config-archive-log-cfg)#end

Additional Information:

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)

1.4 CISC-ND-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to automatically audit account disabling actions.

```
GROUP ID: V-220573
RULE ID: SV-220573r960783
```

Rationale:

Account management, as a whole, ensures access to the network device is being controlled in a secure manner by granting access to only authorized personnel. Auditing account disabling actions will support account management procedures.

When device management accounts are disabled, user or service accessibility may be affected. Auditing also ensures authorized active accounts remain enabled and available for use when required.

Audit:

Review the switch configuration to determine if it automatically audits account disabling. The configuration should look similar to the example below:
archive
log config
logging enable
Note: Configuration changes can be viewed using the show archive log config all command.
If account disabling is not automatically audited, this is a finding.

Remediation:

Configure the switch to log account disabling using the following commands:
SW4(config)#archive
SW4(config-archive)#log config
SW4(config-archive-log-cfg)#logging enable
SW4(config-archive-log-cfg)#end

Additional Information:

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)

1.5 CISC-ND-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to automatically audit account removal actions.

```
GROUP ID: V-220574
RULE ID: SV-220574r960786
```

Rationale:

Account management, as a whole, ensures access to the network device is being controlled in a secure manner by granting access to only authorized personnel. Auditing account removal actions will support account management procedures.

When device management accounts are terminated, user or service accessibility may be affected. Auditing also ensures authorized active accounts remain enabled and available for use when required.

Audit:

Review the switch configuration to determine if it automatically audits account removal. The configuration should look similar to the example below:
archive
log config
logging enable
Note: Configuration changes can be viewed using the show archive log config all command.
If account removal is not automatically audited, this is a finding.

Remediation:

Configure the switch to log account removal using the following commands:
SW4(config)#archive
SW4(config-archive)#log config
SW4(config-archive-log-cfg)#logging enable
SW4(config-archive-log-cfg)#end

Additional Information:

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)

1.6 CISC-ND-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to enforce approved authorizations for controlling the flow of management information within the device based on control policies.

```
GROUP ID: V-220575
RULE ID: SV-220575r1107154
```

Rationale:

A mechanism to detect and prevent unauthorized communication flow must be configured or provided as part of the system design. If management information flow is not enforced based on approved authorizations, the network device may become compromised. Information flow control regulates where management information is allowed to travel within a network device. The flow of all management information must be monitored and controlled so it does not introduce any unacceptable risk to the network device or data.

Application-specific examples of enforcement occur in systems that employ rule sets or establish configuration settings that restrict information system services or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics).

Applications providing information flow control must be able to enforce approved authorizations for controlling the flow of management information within the system in accordance with applicable policy.

Audit:

Review the Cisco switch configuration to verify that administrative access to the switch is allowed only from hosts residing in the management network.
Step 1: Verify that the line vty has an ACL inbound applied as shown in the example below:
line vty 0 1
access-class MANAGEMENT_NET in
transport input ssh
Step 2: Verify that the ACL permits only hosts from the management network to access the switch.
ip access-list extended MANAGEMENT_NET
permit ip x.x.x.0 0.0.0.255 any
deny ip any any log-input
If the Cisco switch is not configured to enforce approved authorizations for controlling the flow of management information within the device based on control policies, this is a finding.

Remediation:

Configure the Cisco switch to restrict management access to specific IP addresses via SSH as shown in the example below:
SW2(config)#ip access-list extended MANAGEMENT_NET
SW2(config-ext-nacl)#permit x.x.x.0 0.0.0.255
SW2(config-ext-nacl)#exit
SW2(config)#line vty 0 1
SW2(config-line)#transport input ssh
SW2(config-line)#access-class MANAGEMENT_NET in
SW2(config-line)#end

Additional Information:

CCI-001368 Enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

CCI-004192 Protect nonlocal maintenance sessions by separating the maintenance session from other network sessions with the system by logically separated communications paths.

- NIST SP 800-53 Revision 5::MA-4 (4) (b) (2)

1.7 CISC-ND-000150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to enforce the limit of three consecutive invalid logon attempts, after which time it must lock out the user account from accessing the device for 15 minutes.

```
GROUP ID: V-220576
RULE ID: SV-220576r960840
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced.

Audit:

Review the Cisco switch configuration to verify that it enforces the limit of three consecutive invalid logon attempts as shown in the example below:
login block-for 900 attempts 3 within 120
Note: The configuration example above will block any logon attempt for 15 minutes after three consecutive invalid logon attempts within a two-minute period.
If the Cisco switch is not configured to enforce the limit of three consecutive invalid logon attempts, this is a finding.

Remediation:

Configure the Cisco switch to enforce the limit of three consecutive invalid logon attempts as shown in the example below:
SW2(config)#login block-for 900 attempts 3 within 120

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

1.8 CISC-ND-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the device.

```
GROUP ID: V-220577
RULE ID: SV-220577r960843
```

Rationale:

Display of the DoD-approved use notification before granting access to the network device ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users.

Audit:

Review the Cisco switch configuration to verify that it displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the device as shown in the example below:
banner login ^C
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.
^C
If the Cisco switch is not configured to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the device, this is a finding.

Remediation:

Configure the Cisco switch to display the Standard Mandatory DoD Notice and Consent Banner before granting access as shown in the following example:
SW1(config)#banner login #
Enter TEXT message. End with the character '#'.
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. #
SW1(config)#end

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

1.9 CISC-ND-000210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco device must be configured to audit all administrator activity.

```
GROUP ID: V-220578
RULE ID: SV-220578r960864
```

Rationale:

This requirement supports non-repudiation of actions taken by an administrator and is required to maintain the integrity of the configuration management process. All configuration changes to the network device are logged, and administrators authenticate with two-factor authentication before gaining administrative access. Together, these processes will ensure the administrators can be held accountable for the configuration changes they implement.

To meet this requirement, the network device must log administrator access and activity.

Audit:

Review the Cisco switch configuration to verify that it logs administrator activity as shown in the example below:
hostname R1
!
logging userinfo
!
…
…
…
archive
log config
logging enable
!
Note: The logging userinfo global configuration command will generate a log when a user increases his or her privilege level.
If logging of administrator activity is not configured, this is a finding.

Remediation:

Configure the switch to log administrator activity as shown in the example below:
SW1(config)#logging userinfo
SW1(config)#archive
SW1(config-archive)#log config
SW1(config-archive-log-cfg)#logging enable
SW1(config-archive-log-cfg)#end

Additional Information:

CCI-000166 Provide irrefutable evidence that an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

- NIST SP 800-53::AU-10
- NIST SP 800-53A::AU-10.1
- NIST SP 800-53 Revision 4::AU-10
- NIST SP 800-53 Revision 5::AU-10

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)

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

1.10 CISC-ND-000280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must produce audit records containing information to establish when (date and time) the events occurred.

```
GROUP ID: V-220580
RULE ID: SV-220580r960894
```

Rationale:

It is essential for security personnel to know what is being done, what was attempted, where it was done, when it was done, and by whom it was done to compile an accurate risk assessment.

Logging the date and time of each detected event provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured network device. To establish and correlate the series of events leading up to an outage or attack, it is imperative the date and time are recorded in all log records.

Audit:

Verify that the switch is configured to include the date and time on all log records as shown in the configuration example below:
service timestamps log datetime localtime
If time stamps are not configured, this is a finding.

Remediation:

Configure the switch to include the date and time on all log records as shown in the example below:
SW1(config)#service timestamps log datetime localtime

Additional Information:

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- 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 b

1.11 CISC-ND-000290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must produce audit records containing information to establish where the events occurred.

```
GROUP ID: V-220581
RULE ID: SV-220581r960897
```

Rationale:

To compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know where events occurred, such as device hardware components, device software modules, session identifiers, filenames, host names, and functionality.

Associating information about where the event occurred within the network device provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured device.

Audit:

Review the deny statements in all interface ACLs to determine if the log-input parameter has been configured as shown in the example below.
Note: log-input can only apply to interface bound ACLs.
ip access-list extended BLOCK_INBOUND
deny icmp any any log-input
If the switch is not configured with the log-input parameter after any deny statements to note where packets have been dropped via an ACL, this is a finding.

Remediation:

Configure the log-input parameter after any deny statements to provide the location as to where packets have been dropped via an ACL:
SW1(config)#ip access-list extended BLOCK_INBOUND
SW1(config-ext-nacl)#deny icmp any any log-input

Additional Information:

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- 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 c

1.12 CISC-ND-000380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to protect audit information from unauthorized modification.

```
GROUP ID: V-220583
RULE ID: SV-220583r960933
```

Rationale:

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit network device activity.

If audit data were to become compromised, forensic analysis and discovery of the true source of potentially malicious system activity would be impossible.

To ensure the veracity of audit data, the network device must protect audit information from unauthorized modification.

This requirement can be achieved through multiple methods, which will depend on system architecture and design. Some commonly employed methods include ensuring log files receive the proper file system permissions and limiting log data locations.

Network devices providing a user interface to audit data will leverage user permissions and roles identifying the user accessing the data and the corresponding user rights to make access decisions regarding the modification of audit data.

Audit:

Review the Cisco switch configuration to verify that it is configured to protect audit information.
Step 1: If persistent logging is enabled as shown in the example below, go to Step 2. Otherwise, this requirement is not applicable.
logging persistent url disk0:/logfile size 134217728 filesize 16384
Step 2: Verify that the switch is not configured with a privilege level other than "15" to allow access to the file system as shown in the example below:
file privilege 10
Note: The default privilege level required for access to the file system is "15"; hence, the command file privilege "15" will not be shown in the configuration.
If the switch is configured with a privilege level other than "15" to allow access to the file system, this is a finding.

Remediation:

If persistent logging is enabled, configure the switch to only allow administrators with privilege level "15" access to the file system as shown in the example below:
SW4(config)#file privilege 15

Additional Information:

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

1.13 CISC-ND-000330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to generate audit records containing the full-text recording of privileged commands.

```
GROUP ID: V-220582
RULE ID: SV-220582r960909
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. The additional information required is dependent on the type of information (i.e., sensitivity of the data and the environment within which it resides). At a minimum, the organization must audit full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Review the Cisco switch configuration to verify that it generates audit records of configuration changes. The configuration example below will log all configuration changes:
archive
log config
logging enable
Note: Configuration changes can be viewed using the show archive log config all command.
If the Cisco switch is not configured to generate audit records of configuration changes, this is a finding.

Remediation:

Configure the Cisco switch to log all configuration changes as shown in the example below:
SW4(config)#archive
SW4(config-archive)#log config
SW4(config-archive-log-cfg)#logging enable
SW4(config-archive-log-cfg)#end

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)

1.14 CISC-ND-000390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to protect audit information from unauthorized deletion.

```
GROUP ID: V-220584
RULE ID: SV-220584r960936
```

Rationale:

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

If audit data were to become compromised, forensic analysis and discovery of the true source of potentially malicious system activity would be impossible.

To ensure the veracity of audit data, the network device must protect audit information from unauthorized deletion. This requirement can be achieved through multiple methods, which will depend on system architecture and design. Some commonly employed methods include ensuring log files receive the proper file system permissions using file system protections, restricting access, and backing up log data to ensure it is retained.

Network devices providing a user interface to audit data will leverage user permissions and roles identifying the user accessing the data and the corresponding user rights to make access decisions regarding the deletion of audit data.

Audit:

Review the Cisco switch configuration to verify that it protects audit information from unauthorized deletion.
Step 1: If persistent logging is enabled as shown in the example below, go to Step 2. Otherwise, this requirement is not applicable.
logging persistent url disk0:/logfile size 134217728 filesize 16384
Step 2: Verify that the switch is not configured with a privilege level other than "15" to allow access to the file system as shown in the example below:
file privilege 10
Note: The default privilege level required for access to the file system is "15"; hence, the command file privilege "15" will not be shown in the configuration.
If the switch is configured with a privilege level other than "15" to allow access to the file system, this is a finding.

Remediation:

If persistent logging is enabled, configure the switch to only allow administrators with privilege level "15" access to the file system as shown in the example below:
SW4(config)#file privilege 15

Additional Information:

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

1.15 CISC-ND-000460 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to limit privileges to change the software resident within software libraries.

```
GROUP ID: V-220585
RULE ID: SV-220585r960960
```

Rationale:

Changes to any software components of the network device can have significant effects on the overall security of the network. Therefore, only qualified and authorized individuals should be allowed administrative access to the network device for implementing any changes or upgrades.

If the network device were to enable unauthorized users to make changes to software libraries, those changes could be implemented without undergoing testing, validation, and approval.

Audit:

Review the Cisco switch configuration to verify that it limits software change privileges.
Step 1: If persistent logging is enabled as shown in the example below, go to Step 2. Otherwise, this requirement is not applicable.
logging persistent url disk0:/logfile size 134217728 filesize 16384
Step 2: Verify that the switch is not configured with a privilege level other than "15" to allow access to the file system as shown in the example below:
file privilege 10
Note: The default privilege level required for access to the file system is "15"; hence, the command file privilege "15" will not be shown in the configuration.
If the switch is configured with a privilege level other than "15" to allow access to the file system, this is a finding.

Remediation:

If persistent logging is enabled, configure the switch to only allow administrators with privilege level "15" access to the file system as shown in the example below:
SW4(config)#file privilege 15

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.16 CISC-ND-000470 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must be configured to prohibit the use of all unnecessary and non-secure functions and services.

```
GROUP ID: V-220586
RULE ID: SV-220586r1043177
```

Rationale:

Network devices are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., email and web services); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the network device must support the organizational requirements providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved. Some network devices have capabilities enabled by default; if these capabilities are not necessary, they must be disabled. If a particular capability is used, it must be documented and approved.

Audit:

Verify that the switch does not have any unnecessary or nonsecure ports, protocols, and services enabled.
For example, the following commands should not be in the configuration:
boot network
ip boot server
ip bootp server
ip dns server
ip identd
ip finger
ip http server
ip rcmd rcp-enable
ip rcmd rsh-enable
service config
service finger
service tcp-small-servers
service udp-small-servers
service pad
service call-home
Note: Certain legacy devices may require 'service call-home' be enabled to support Smart Licensing as they do not support the newer smart transport configuration. Those devices do not incur a finding for having call-home enabled for Smart Licensing.
If any unnecessary or nonsecure ports, protocols, or services are enabled, this is a finding.

Remediation:

Disable the following services if enabled as shown in the example below:
SW2(config)#no boot network
SW2(config)#no ip boot server
SW2(config)#no ip bootp server
SW2(config)#no ip dns server
SW2(config)#no ip identd
SW2(config)#no ip finger
SW2(config)#no ip http server
SW2(config)#no ip rcmd rcp-enable
SW2(config)#no ip rcmd rsh-enable
SW2(config)#no service config
SW2(config)#no service finger
SW2(config)#no service tcp-small-servers
SW2(config)#no service udp-small-servers
SW2(config)#no service pad
SW2(config)#no service call-home
SW2(config)#end

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

1.17 CISC-ND-000490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured with only one local account to be used as the account of last resort in the event the authentication server is unavailable.

```
GROUP ID: V-220587
RULE ID: SV-220587r1051115
```

Rationale:

Authentication for administrative (privileged-level) access to the device is required at all times. An account can be created on the device's local database for use when the authentication server is down or connectivity between the device and the authentication server is not operable. This account is referred to as the account of last resort since it is intended to be used as a last resort and when immediate administrative access is absolutely necessary.

The account of last resort logon credentials must be stored in a sealed envelope and kept in a safe. The safe must be periodically audited to verify the envelope remains sealed. The signature of the auditor and the date of the audit should be added to the envelope as a record.

An alternative to using a sealed envelope in a safe would be credential files, separated by technology, located in a secured location on a file server, with the files only accessible to those administrators authorized to use the accounts of last resort, and access to that location monitored by a central log server.

Administrators should secure the credentials and disable the root account (if possible) when not needed for system administration functions.

Audit:

Step 1: Review the Cisco switch configuration to verify that a local account for last resort has been configured with a privilege level that will enable the administrator to troubleshoot connectivity to the authentication server.
username xxxxxxxxxxx privilege 10 common-criteria-policy PASSWORD_POLICY password xxxxxxxxxx
Note: The configured Common Criteria policy must be used when creating or changing the local account password as shown in the example above.
Step 2: Verify that local is defined after radius or tacacs+ in the authentication order as shown in the example below:
aaa authentication login default group tacacs+ local
If the Cisco switch is not configured with only one local account to be used as the account of last resort in the event the authentication server is unavailable, this is a finding.

Remediation:

Step 1: Configure a local account with the necessary privilege level to troubleshoot network outage and restore operations as shown in the following example:
SW2(config)#username xxxxxxxxxxx privilege 10 common-criteria-policy PASSWORD_POLICY password xxxxxxxxxx
Step 2: Configure the authentication order to use the local account if the authentication server is not reachable as shown in the following example:
SW2(config)#aaa authentication login default group tacacs+ local

Additional Information:

CCI-001358 Establish privileged user accounts in accordance with a role-based access scheme; or an attribute-based access scheme.

- NIST SP 800-53::AC-2 (7) (a)
- NIST SP 800-53A::AC-2 (7).1 (i)
- NIST SP 800-53 Revision 4::AC-2 (7) (a)
- NIST SP 800-53 Revision 5::AC-2 (7) (a)

CCI-002111 The organization identifies and selects the organization-defined information system account types of information system accounts which support organizational missions/business functions.

- NIST SP 800-53 Revision 4::AC-2 a

1.18 CISC-ND-000550 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to enforce a minimum 15-character password length.

```
GROUP ID: V-220589
RULE ID: SV-220589r1015280
```

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password.

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Audit:

Review the Cisco switch configuration to verify that it enforces a minimum 15-character password length as shown in the example below:
aaa new-model
!
!
aaa common-criteria policy PASSWORD_POLICY
min-length 15
If the Cisco switch is not configured to enforce a minimum 15-character password length, this is a finding.

Remediation:

Configure the Cisco switch to enforce a minimum 15-character password length as shown in the example below:
SW1(config)#aaa common-criteria policy PASSWORD_POLICY
SW1(config-cc-policy)#min-length 15
SW1(config-cc-policy)#exit

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000205 The information system enforces minimum password length.

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

1.19 CISC-ND-000570 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to enforce password complexity by requiring that at least one uppercase character be used.

```
GROUP ID: V-220590
RULE ID: SV-220590r1015281
```

Rationale:

Use of a complex passwords helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password is, the greater the number of possible combinations that need to be tested before the password is compromised.

Multifactor authentication (MFA) is required for all administrative and user accounts on network devices, except for an account of last resort and (where applicable) a root account. Passwords should only be used when MFA using PKI is not available and for the account of last resort and root account.

Audit:

Review the Cisco switch configuration to verify that it requires the use of at least one uppercase character as shown in the example below:
aaa new-model
!
!
aaa common-criteria policy PASSWORD_POLICY
upper-case 1
If the Cisco switch is not configured to enforce password complexity by requiring that at least one uppercase character be used, this is a finding.

Remediation:

Configure the Cisco switch to enforce password complexity by requiring that at least one uppercase character be used as shown in the example below:
SW1(config)#aaa common-criteria policy PASSWORD_POLICY
SW1(config-cc-policy)#upper-case 1
SW1(config-cc-policy)#exit

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

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

1.20 CISC-ND-000590 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to enforce password complexity by requiring that at least one numeric character be used.

```
GROUP ID: V-220592
RULE ID: SV-220592r1015283
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Multifactor authentication (MFA) is required for all administrative and user accounts on network devices, except for an account of last resort and (where applicable) a root account. Passwords should only be used when MFA using PKI is not available and for the account of last resort and root account.

Audit:

Review the Cisco switch configuration to verify that it requires the use of at least one numeric character as shown in the example below:
aaa new-model
!
!
aaa common-criteria policy PASSWORD_POLICY
numeric-count 1
If the Cisco switch is not configured to enforce password complexity by requiring that at least one numeric character be used, this is a finding.

Remediation:

Configure the Cisco switch to enforce password complexity by requiring that at least one numeric character be used as shown in the example below:
SW1(config)#aaa common-criteria policy PASSWORD_POLICY
SW1(config-cc-policy)#numeric-count 1
SW1(config-cc-policy)#exit

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

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

1.21 CISC-ND-000580 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to enforce password complexity by requiring that at least one lowercase character be used.

```
GROUP ID: V-220591
RULE ID: SV-220591r1015282
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Multifactor authentication (MFA) is required for all administrative and user accounts on network devices, except for an account of last resort and (where applicable) a root account. Passwords should only be used when MFA using PKI is not available and for the account of last resort and root account.

Audit:

Review the Cisco switch configuration to verify that it requires the use of at least one lowercase character as shown in the example below:
aaa new-model
!
!
aaa common-criteria policy PASSWORD_POLICY
lower-case 1
If the Cisco switch is not configured to enforce password complexity by requiring that at least one lowercase character be used, this is a finding.

Remediation:

Configure the Cisco switch to enforce password complexity by requiring that at least one lowercase character be used as shown in the example below:
SW1(config)#aaa common-criteria policy PASSWORD_POLICY
SW1(config-cc-policy)#lower-case 1
SW1(config-cc-policy)#exit

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

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

1.22 CISC-ND-000600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to enforce password complexity by requiring that at least one special character be used.

```
GROUP ID: V-220593
RULE ID: SV-220593r1015284
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Multifactor authentication (MFA) is required for all administrative and user accounts on network devices, except for an account of last resort and (where applicable) a root account. Passwords should only be used when MFA using PKI is not available and for the account of last resort and root account.

Audit:

Review the Cisco switch configuration to verify that it requires the use of at least one special character as shown in the example below:
aaa new-model
!
!
aaa common-criteria policy PASSWORD_POLICY
special-case 1
If the Cisco switch is not configured to enforce password complexity by requiring that at least one special character be used, this is a finding.

Remediation:

Configure the Cisco switch to enforce password complexity by requiring that at least one special character be used as shown in the example below:
SW1(config)#aaa common-criteria policy PASSWORD_POLICY
SW1(config-cc-policy)#special-case 1
SW1(config-cc-policy)#exit

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

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

1.23 CISC-ND-000610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to require that when a password is changed, the characters are changed in at least eight of the positions within the password.

```
GROUP ID: V-220594
RULE ID: SV-220594r1043189
```

Rationale:

If the application allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

Multifactor authentication (MFA) is required for all administrative and user accounts on network devices, except for an account of last resort and (where applicable) a root account. Passwords should only be used when MFA using PKI is not available and for the account of last resort and root account.

Audit:

Review the Cisco switch configuration to verify that, when a password is changed, it requires the characters to be changed in at least eight of the positions as shown in the example below:
aaa new-model
!
!
aaa common-criteria policy PASSWORD_POLICY
char-changes 8
If the Cisco switch is not configured to require that when a password is changed, the characters are changed in at least eight of the positions within the password, this is a finding.

Remediation:

Configure the Cisco switch to enforce password complexity by requiring that when a password is changed, the characters are changed in at least eight of the positions within the password as shown in the example below:
SW1(config)#aaa common-criteria policy PASSWORD_POLICY
SW1(config-cc-policy)#char-changes 8
SW1(config-cc-policy)#exit

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

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

1.24 CISC-ND-000620 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must only store cryptographic representations of passwords.

```
GROUP ID: V-220595
RULE ID: SV-220595r1015286
```

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Network devices must enforce cryptographic representations of passwords when storing passwords in databases, configuration files, and log files. Passwords must be protected at all times; using a strong one-way hashing encryption algorithm with a salt is the standard method for providing a means to validate a password without having to store the actual password.

Performance and time required to access are factors that must be considered, and the one-way hash is the most feasible means of securing the password and providing an acceptable measure of password security. If passwords are stored in clear text, they can be plainly read and easily compromised.

In many instances, verification that the user knows a password is performed using a password verifier. In its simplest form, a password verifier is a computational function that is capable of creating a hash of a password and determining if the value provided by the user matches the stored hash.

Audit:

Review the switch configuration to determine if passwords are encrypted as shown in the example below:
service password-encryption
…
…
…
Enable secret 5 xxxxxxxxxxxxxxxxxxxxxxxxxx
If the switch is not configured to encrypt passwords, this is a finding.

Remediation:

Configure the switch to encrypt all passwords:
SW4(config)#service password-encryption
SW4(config)#enable secret xxxxxxxxxxx
SW4(config)#end

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5::IA-5 (1) (d)

CCI-004910 Provide protected storage for cryptographic keys with organization-defined safeguards and/or hardware protected key store.

- NIST SP 800-53 Revision 5::SC-28 (3)

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)

1.25 CISC-ND-000720 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must be configured to terminate all network connections associated with device management after five minutes of inactivity.

```
GROUP ID: V-220596
RULE ID: SV-220596r961068
```

Rationale:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. This does not mean that the device terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Audit:

Review the Cisco switch configuration to verify that all network connections associated with a device management have an idle timeout value set to five minutes or less as shown in the example below:
ip http secure-server
ip http timeout-policy idle 300 life nnnn requests nn
…
…
…
line con 0
exec-timeout 5 0
line vty 0 1
exec-timeout 5 0
If the Cisco switch is not configured to terminate all network connections associated with a device management after five minutes of inactivity, this is a finding.

Remediation:

Set the idle timeout value to five minutes or less on all configured login classes as shown in the example below:
SW1(config)#line vty 0 1
SW1(config-line)#exec-timeout 5 0
SW1(config-line)#exit
SW1(config)#line con 0
SW1(config-line)#exec-timeout 5 0
SW1(config-line)#exit
SW2(config)#ip http timeout-policy idle 300 life nnnn requests nn

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

1.26 CISC-ND-000880 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to automatically audit account enabling actions.

```
GROUP ID: V-220597
RULE ID: SV-220597r961290
```

Rationale:

Once an attacker establishes initial access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to enable a new or disabled account. Notification of account enabling is one method for mitigating this risk.

A comprehensive account management process will ensure an audit trail that documents the creation of application user accounts and notifies administrators and Information System Security Officers (ISSOs). Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

Audit:

Review the switch configuration to determine if it automatically audits account enabling. The configuration should look similar to the example below:
archive
log config
logging enable
Note: Configuration changes can be viewed using the show archive log config all command.
If account enabling is not automatically audited, this is a finding.

Remediation:

Configure the switch to log account enabling using the following commands:
SW4(config)#archive
SW4(config-archive)#log config
SW4(config-archive-log-cfg)#logging enable
SW4(config-archive-log-cfg)#end

Additional Information:

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)

1.27 CISC-ND-000980 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to allocate audit record storage capacity in accordance with organization-defined audit record storage requirements.

```
GROUP ID: V-220599
RULE ID: SV-220599r961392
```

Rationale:

To ensure that network devices have a sufficient storage capacity in which to write the audit logs, they need to be able to allocate audit record storage capacity. The task of allocating audit record storage capacity is usually performed during initial device setup if it is modifiable.

The value for the organization-defined audit record storage requirement will depend on the amount of storage available on the network device, the anticipated volume of logs, the frequency of transfer from the network device to centralized log servers, and other factors.

Audit:

Verify that the Cisco switch is configured with a logging buffer size. The configuration should look like the example below:
logging buffered xxxxxxxx informational
If a logging buffer size is not configured, this is a finding.
If the Cisco switch is not configured to allocate audit record storage capacity in accordance with organization-defined audit record storage requirements, this is a finding.

Remediation:

Configure the buffer size for logging as shown in the example below:
SW2(config)#logging buffered xxxxxxxx informational

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

1.28 CISC-ND-001000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to generate an alert for all audit failure events.

```
GROUP ID: V-220600
RULE ID: SV-220600r991868
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without a real-time alert, security personnel may be unaware of an impending failure of the audit capability and system operation may be adversely affected.

Alerts provide organizations with urgent messages. Real-time alerts provide these messages immediately (i.e., the time from event detection to alert occurs in seconds or less).

Audit:

Review the Cisco switch configuration to verify that it generates an alert for all audit failure events as shown in the example below:
logging trap critical
Note: The parameter "critical" can replaced with a lesser severity level (i.e., error, warning, notice, informational). Informational is the default severity level; hence, if the severity level is configured to informational, the logging trap command will not be shown in the configuration.
If the Cisco switch is not configured to generate an alert for all audit failure events, this is a finding.

Remediation:

Configure the Cisco switch to send critical to emergency log messages to the syslog server as shown in the example below:
SW4(config)#logging trap critical
Note: The parameter "critical" can replaced with a lesser severity level (i.e., error, warning, notice, informational).

Additional Information:

CCI-001858 Provide an alert in an organization-defined real-time-period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.

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

CCI-003831 Alert organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

- NIST SP 800-53 Revision 5::AU-9 b

1.29 CISC-ND-001030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to synchronize its clock with the primary and secondary time sources using redundant authoritative time sources.

```
GROUP ID: V-220601
RULE ID: SV-220601r1015287
```

Rationale:

The loss of connectivity to a particular authoritative time source will result in the loss of time synchronization (free-run mode) and increasingly inaccurate time stamps on audit events and other functions.

Multiple time sources provide redundancy by including a secondary source. Time synchronization is usually a hierarchy; clients synchronize time to a local source while that source synchronizes its time to a more accurate source. The network device must use an authoritative time server and/or be configured to use redundant authoritative time sources. This requirement is related to the comparison done in CCI-001891.

DOD-approved solutions consist of a combination of a primary and secondary time source using a combination or multiple instances of the following: a time server designated for the appropriate DOD network (NIPRNet/SIPRNet); United States Naval Observatory (USNO) time servers; and/or the Global Positioning System (GPS). The secondary time source must be located in a different geographic region than the primary time source.

Audit:

Review the Cisco switch configuration to verify that it synchronizes its clock with redundant authoritative time sources as shown in the example below:
ntp server x.x.x.x
ntp server y.y.y.y
If the Cisco switch is not configured to synchronize its clock with redundant authoritative time sources, this is a finding.

Remediation:

Configure the Cisco switch to synchronize its clock with redundant authoritative time sources as shown in the example below:
SW2(config)#ntp server x.x.x.x
SW2(config)#ntp server y.y.y.y

Additional Information:

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-004928 Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (2) (a)

CCI-004922 Synchronize system clocks within and between systems or system components.

- NIST SP 800-53 Revision 5::SC-45

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-001893 The information system identifies a secondary authoritative time source that is located in a different geographic region than the primary authoritative time source.

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

1.30 CISC-ND-001130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to authenticate SNMP messages using a FIPS-validated Keyed-Hash Message Authentication Code (HMAC).

```
GROUP ID: V-220604
RULE ID: SV-220604r961506
```

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity. Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk.

A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area or wide area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet).

Because of the challenges of applying this requirement on a large scale, organizations are encouraged to only apply the requirement to those limited number (and type) of devices that truly need to support this capability.

Audit:

Review the Cisco switch configuration to verify that it authenticates SNMP messages using a FIPS-validated HMAC as shown in the example below:
snmp-server group V3GROUP v3 auth read V3READ write V3WRITE
snmp-server view V3READ iso included
snmp-server view V3WRITE iso included
snmp-server host x.x.x.x version 3 auth V3USER
Authentication used by the SNMP users can be viewed via the show snmp user command as shown in the example below:
R4#show snmp user
User name: V3USER
Engine ID: 800000090300C2042B540000
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: None
Group-name: V3GROUP
If the Cisco switch is not configured to authenticate SNMP messages using a FIPS-validated HMAC, this is a finding.

Remediation:

Configure the Cisco switch to authenticate SNMP messages as shown in the example below:
SW4(config)#snmp-server group V3GROUP v3 auth read V3READ write V3WRITE
SW4(config)#snmp-server user V3USER V3GROUP v3 auth sha xxxxxxx
SW4(config)#snmp-server view V3READ iso included
SW4(config)#snmp-server view V3WRITE iso included
SW4(config)#snmp-server host x.x.x.x version 3 auth V3USER

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)

1.31 CISC-ND-001140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to encrypt SNMP messages using a FIPS 140-2 approved algorithm.

```
GROUP ID: V-220605
RULE ID: SV-220605r961506
```

Rationale:

Without the strong encryption that is provided by the SNMP Version 3 User-based Security Model (USM), an unauthorized user can gain access to network management information that can be used to create a network outage.

Audit:

Review the Cisco switch configuration to verify that it encrypts SNMP messages using a FIPS 140-2 approved algorithm as shown in the example below:
snmp-server group V3GROUP v3 priv read V3READ write V3WRITE
snmp-server view V3READ iso included
snmp-server view V3WRITE iso included
snmp-server host x.x.x.x version 3 auth V3USER
Encryption used by the SNMP users can be viewed via the show snmp user command as shown in the example below:
R4#show snmp user
User name: V3USER
Engine ID: 800000090300C2042B540000
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES256
Group-name: V3GROUP
If the Cisco switch is not configured to encrypt SNMP messages using a FIPS 140-2 approved algorithm, this is a finding.

Remediation:

Configure the Cisco switch to encrypt SNMP messages using a FIPS 140-2 approved algorithm as shown in the example below:
SW4(config)#snmp-server group V3GROUP v3 priv read V3READ write V3WRITE
SW4(config)#snmp-server user V3USER V3GROUP v3 auth sha xxxxxx priv aes 256 xxxxxx

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)

1.32 CISC-ND-001150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to authenticate Network Time Protocol (NTP) sources using authentication that is cryptographically based.

```
GROUP ID: V-220606
RULE ID: SV-220606r1107157
```

Rationale:

If NTP is not authenticated, an attacker can introduce a rogue NTP server. This rogue server can then be used to send incorrect time information to network devices, which will make log timestamps inaccurate and affect scheduled actions.

NTP authentication is used to prevent this tampering by authenticating the time source.

Audit:

Review the Cisco switch configuration to verify that it authenticates NTP sources using cryptographically based authentication as shown in the configuration example below:
ntp authentication-key 1 hmac-sha2-256 xxxxxx
ntp authenticate
ntp trusted-key 1
ntp server x.x.x.x key 1
ntp server y.y.y.y key 1
If the Cisco switch is not configured to authenticate NTP sources using authentication that is cryptographically based, this is a finding.

Remediation:

Configure the Cisco switch to authenticate NTP sources using authentication that is cryptographically based as shown in the example below:
SW2(config)#ntp authenticate
SW2(config)#ntp authentication-key 1 hmac-sha2-256 xxxxxx
SW2(config)#ntp trusted-key 1
SW2(config)#ntp server x.x.x.x key 1
SW2(config)#ntp server y.y.y.y key 1

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)

1.33 CISC-ND-001200 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must be configured to use FIPS-validated Keyed-Hash Message Authentication Code (HMAC) to protect the integrity of remote maintenance sessions.

```
GROUP ID: V-220607
RULE ID: SV-220607r1056197
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied on to provide confidentiality or integrity, and DOD data may be compromised.

Nonlocal maintenance and diagnostic activities are conducted by individuals communicating through either an external network (e.g., the internet) or an internal network.

Currently, HMAC is the only FIPS-approved algorithm for generating and verifying message/data authentication codes in accordance with FIPS 198-1. Products that are FIPS 140-2/140-3 validated will have an HMAC that meets specification; however, the option must be configured for use as the only message authentication code used for authentication to cryptographic modules.

Separate requirements for configuring applications and protocols used by each application (e.g., SNMPv3, SSHv2, NTP, HTTPS, and other protocols and applications that require server/client authentication) are required to implement this requirement. Where SSH is used, the SSHv2 protocol suite is required because it includes Layer 7 protocols such as SCP and SFTP, which can be used for secure file transfers.

Audit:

Review the Cisco switch configuration to verify that it uses FIPS-validated HMAC to protect the integrity of remote maintenance sessions as shown in the example below:
NOTE: Although allowed by NIST SP 800-131A Rev. 2 for some applications, SHA-1 is considered a compromised hashing standard and is being phased out of use by industry and government standards. Unless required for legacy use, DOD systems should not be configured to use SHA-1 for integrity of remote access sessions.
SSH Example
ip ssh version 2
iip ssh server algorithm mac hmac-sha2-512 hmac-sha2-256
If the Cisco switch is not configured to use FIPS-validated HMAC to protect the integrity of remote maintenance sessions, this is a finding.

Remediation:

Configure SSH to use FIPS-validated HMAC for remote maintenance sessions as shown in the following example:
SSH Example
SW1(config)#ip ssh version 2
SW1(config)#iip ssh server algorithm mac hmac-sha2-512 hmac-sha2-256

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-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)

1.34 CISC-ND-001210 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must be configured to implement cryptographic mechanisms to protect the confidentiality of remote maintenance sessions.

```
GROUP ID: V-220608
RULE ID: SV-220608r961557
```

Rationale:

This requires the use of secure protocols instead of their unsecured counterparts, such as SSH instead of telnet, SCP instead of FTP, and HTTPS instead of HTTP. If unsecured protocols (lacking cryptographic mechanisms) are used for sessions, the contents of those sessions will be susceptible to eavesdropping, potentially putting sensitive data (including administrator passwords) at risk of compromise and allowing hijacking of maintenance sessions.

Audit:

Review the Cisco switch configuration to verify that it implements cryptographic mechanisms to protect the confidentiality of remote maintenance sessions using a FIPS 140-2 approved algorithm as shown in the example below:
ip ssh version 2
ip ssh server algorithm encryption aes256-ctr aes192-ctr aes128-ctr
If the switch is not configured to implement cryptographic mechanisms to protect the confidentiality of remote maintenance sessions using a FIPS 140-2 approved algorithm, this is a finding.

Remediation:

Configure the Cisco switch to implement cryptographic mechanisms to protect the confidentiality of remote maintenance sessions using a FIPS 140-2 approved algorithm as shown in the example below:
SW1(config)#ip ssh server algorithm encryption aes256-ctr aes192-ctr aes128-ctr

Additional Information:

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)

1.35 CISC-ND-001220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to protect against known types of denial-of-service (DoS) attacks by employing organization-defined security safeguards.

```
GROUP ID: V-220609
RULE ID: SV-220609r1056195
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of network devices to mitigate the impact of DoS attacks that have occurred or are ongoing on device availability. For each network device, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or restricting the number of sessions the device opens at one time). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

The security safeguards cannot be defined at the DoD level because they vary according to the capabilities of the individual network devices and the security controls applied on the adjacent networks (e.g., firewalls performing packet filtering to block DoS attacks).

Audit:

Review the Cisco switch configuration to verify that it protects against known types of DoS attacks by employing organization-defined security safeguards.
Note: Cisco IOS Version 15 and newer could use the command "mls qos copp protocol" to meet the intent of this requirement. This can be checked using command "show mls qos copp protocols".
Step 1: Verify traffic types have been classified based on importance levels. The following is an example configuration:

```
class-map match-all CoPP_CRITICAL
match access-group name CoPP_CRITICAL
class-map match-any CoPP_IMPORTANT
match access-group name CoPP_IMPORTANT
match protocol arp
class-map match-all CoPP_NORMAL
match access-group name CoPP_NORMAL
class-map match-any CoPP_UNDESIRABLE
match access-group name CoPP_UNDESIRABLE
class-map match-all CoPP_DEFAULT
match access-group name CoPP_DEFAULT
```

Step 2: Review the access control lists (ACLs) referenced by the class-maps to determine if the traffic is being classified appropriately. The following is an example configuration:

```
ip access-list extended CoPP_CRITICAL
remark our control plane adjacencies are critical
permit ospf host [OSPF neighbor A] any
permit ospf host [OSPF neighbor B] any
permit pim host [PIM neighbor A] any
permit pim host [PIM neighbor B] any
permit pim host [RP addr] any
permit igmp any 224.0.0.0 15.255.255.255
permit tcp host [BGP neighbor] eq bgp host [local BGP addr]
permit tcp host [BGP neighbor] host [local BGP addr] eq bgp
deny ip any any
```

ip access-list extended CoPP_IMPORTANT
permit tcp host [TACACS server] eq tacacs any
permit tcp [management subnet] 0.0.0.255 any eq 22
permit udp host [SNMP manager] any eq snmp
permit udp host [NTP server] eq ntp any
deny ip any any
ip access-list extended CoPP_NORMAL
remark we will want to rate limit ICMP traffic
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any time-exceeded
permit icmp any any unreachable
deny ip any any
ip access-list extended CoPP_UNDESIRABLE
remark other management plane traffic that should not be received
permit udp any any eq ntp
permit udp any any eq snmp
permit tcp any any eq 22
permit tcp any any eq 23
remark other control plane traffic not configured on switch
permit eigrp any any
permit udp any any eq rip
deny ip any any
ip access-list extended CoPP_DEFAULT
permit ip any any
Note: Explicitly defining undesirable traffic with ACL entries enables the network operator to collect statistics. Excessive Address Resolution Protocol (ARP) packets can potentially monopolize Route Processor resources, starving other important processes. Currently, ARP is the only Layer 2 protocol that can be specifically classified using the match protocol command.
Step 3: Review the policy-map to determine if the traffic is being policed appropriately for each classification. The following is an example configuration:
policy-map CONTROL_PLANE_POLICY
class CoPP_CRITICAL
police 512000 8000 conform-action transmit exceed-action transmit
class CoPP_IMPORTANT
police 256000 4000 conform-action transmit exceed-action drop
class CoPP_NORMAL
police 128000 2000 conform-action transmit exceed-action drop
class CoPP_UNDESIRABLE
police 8000 1000 conform-action drop exceed-action drop
class CoPP_DEFAULT
police 64000 1000 conform-action transmit exceed-action drop
Step 4: Verify that the Control Plane Policing (CoPP) policy is enabled. The following is an example configuration:
control-plane

service-policy input CONTROL_PLANE_POLICY
Note: Control Plane Protection (CPPr) can be used to filter as well as police control plane traffic destined to the RP. CPPr is very similar to CoPP and has the ability to filter and police traffic using finer granularity by dividing the aggregate control plane into three separate categories: 1) host, 2) transit, and 3) CEF-exception. Hence, a separate policy-map could be configured for each traffic category.
If the Cisco switch is not configured to protect against known types of DoS attacks by employing organization-defined security safeguards, this is a finding.

Remediation:

Configure the Cisco switch to protect against known types of DoS attacks on the route processor. Implementing a CoPP policy as shown in the example below is a best practice method.
Step 1: Configure ACL specific traffic types:

```
SW1(config)#ip access-list extended CoPP_CRITICAL
SW1(config-ext-nacl)#remark our control plane adjacencies are critical
SW1(config-ext-nacl)#permit ospf host x.x.x.x any
SW1(config-ext-nacl)#permit ospf host x.x.x.x any
SW1(config-ext-nacl)#permit pim host x.x.x.x any
SW1(config-ext-nacl)#permit pim host x.x.x.x any
SW1(config-ext-nacl)#permit igmp any 224.0.0.0 15.255.255.255
SW1(config-ext-nacl)#permit tcp host x.x.x.x eq bgp host x.x.x.x
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#ip access-list extended CoPP_IMPORTANT
SW1(config-ext-nacl)#permit tcp host x.x.x.x eq tacacs any
SW1(config-ext-nacl)#permit tcp x.x.x.x 0.0.0.255 any eq 22
SW1(config-ext-nacl)#permit udp host x.x.x.x any eq snmp
SW1(config-ext-nacl)#permit udp host x.x.x.x eq ntp any
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#ip access-list extended CoPP_NORMAL
SW1(config-ext-nacl)#remark we will want to rate limit ICMP traffic
SW1(config-ext-nacl)#permit icmp any any echo
SW1(config-ext-nacl)#permit icmp any any echo-reply
SW1(config-ext-nacl)#permit icmp any any time-exceeded
SW1(config-ext-nacl)#permit icmp any any unreachable
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#ip access-list extended CoPP_UNDESIRABLE
SW1(config-ext-nacl)#remark management plane traffic that should not be received
SW1(config-ext-nacl)#permit udp any any eq ntp
SW1(config-ext-nacl)#permit udp any any eq snmp
```

```
SW1(config-ext-nacl)#permit tcp any any eq 22
SW1(config-ext-nacl)#permit tcp any any eq 23
SW1(config-ext-nacl)#remark control plane traffic not configured on switch
SW1(config-ext-nacl)#permit eigrp any any
SW1(config-ext-nacl)#permit udp any any eq rip
SW1(config-ext-nacl)#deny ip any any
SW1(config-ext-nacl)#exit
SW1(config)#ip access-list extended CoPP_DEFAULT
SW1(config-ext-nacl)#permit ip any any
SW1(config-ext-nacl)#exit
```

Step 2: Configure class-maps referencing each of the ACLs:

```
SW1(config)#class-map match-all CoPP_CRITICAL
SW1(config-cmap)#match access-group name CoPP_CRITICAL
SW1(config-cmap)#class-map match-any CoPP_IMPORTANT
SW1(config-cmap)#match access-group name CoPP_IMPORTANT
SW1(config-cmap)#match protocol arp
SW1(config-cmap)#class-map match-all CoPP_NORMAL
SW1(config-cmap)#match access-group name CoPP_NORMAL
SW1(config-cmap)#class-map match-any CoPP_UNDESIRABLE
SW1(config-cmap)#match access-group name CoPP_UNDESIRABLE
SW1(config-cmap)#class-map match-all CoPP_DEFAULT
SW1(config-cmap)#match access-group name CoPP_DEFAULT
SW1(config-cmap)#exit
```

Step 3: Configure a policy-map referencing the configured class-maps and apply appropriate bandwidth allowance and policing attributes:

```
SW1(config)#policy-map CONTROL_PLANE_POLICY
SW1(config-pmap)#class CoPP_CRITICAL
SW1(config-pmap-c)#police 512000 8000 conform-action transmit exceed-action
transmit
SW1(config-pmap-c-police)#class CoPP_IMPORTANT
SW1(config-pmap-c)#police 256000 4000 conform-action transmit exceed-action drop
SW1(config-pmap-c-police)#class CoPP_NORMAL
SW1(config-pmap-c)#police 128000 2000 conform-action transmit exceed-action drop
SW1(config-pmap-c-police)#class CoPP_UNDESIRABLE
SW1(config-pmap-c)#police 8000 1000 conform-action drop exceed-action drop
SW1(config-pmap-c-police)#class CoPP_DEFAULT
SW1(config-pmap-c)#police 64000 1000 conform-action transmit exceed-action drop
SW1(config-pmap-c-police)#exit
SW1(config-pmap-c)#exit
SW1(config-pmap)#exit
```

Step 4: Apply the policy-map to the control plane:

```
SW1(config)#control-plane
SW1(config-cp)#service-policy input CONTROL_PLANE_POLICY
SW1(config-cp)#end
```

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

1.36 CISC-ND-001250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to generate log records when administrator privileges are deleted.

```
GROUP ID: V-220611
RULE ID: SV-220611r961812
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the network device (e.g., module or policy filter).

Audit:

Review the Cisco switch configuration to verify that it generates log records when administrator privileges are deleted as shown in the example below:
archive
log config
logging enable
If the Cisco switch is not configured to generate log records when administrator privileges are deleted, this is a finding.

Remediation:

Configure the Cisco switch to generate log records when administrator privileges are deleted as shown in the example below:
SW4(config)#archive
SW4(config-archive)#log config
SW4(config-archive-log-cfg)#logging enable
SW4(config-archive-log-cfg)#end

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

1.37 CISC-ND-001260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to generate audit records when successful/unsuccessful logon attempts occur.

```
GROUP ID: V-220612
RULE ID: SV-220612r961824
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the network device (e.g., module or policy filter).

Audit:

Review the Cisco switch configuration to verify that it generates audit records when successful/unsuccessful logon attempts occur as shown in the examples below:
login on-failure log
login on-success log
If the Cisco switch is not configured to generate audit records when successful/unsuccessful logon attempts occur, this is a finding.

Remediation:

Configure the Cisco switch to generate audit records when successful/unsuccessful logon attempts occur as shown in the example below:
R5(config)#login on-failure log
R5(config)#login on-success log

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

1.38 CISC-ND-001270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to generate log records for privileged activities.

```
GROUP ID: V-220613
RULE ID: SV-220613r961827
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the network device (e.g., module or policy filter).

Audit:

Review the Cisco switch configuration to verify that it generates log records for privileged activities as shown in the example configurations below:
archive
log config
logging enable
If the Cisco switch is not configured to generate log records for privileged activities, this is a finding.

Remediation:

Configure the Cisco switch to generate log records for privileged activities as shown in the example below:
SW4(config)#archive
SW4(config-archive)#log config
SW4(config-archive-log-cfg)#logging enable
SW4(config-archive-log-cfg)#end

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

1.39 CISC-ND-001370 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must be configured to use at least two authentication servers to authenticate users prior to granting administrative access.

```
GROUP ID: V-220617
RULE ID: SV-220617r961863
```

Rationale:

Centralized management of user accounts and authentication increases the administrative access to the switch. This control is particularly important protection against the insider threat.

With robust centralized management, audit records for administrator account access to the organization's network devices can be more readily analyzed for trends and anomalies. The alternative method of defining administrator accounts on each device exposes the device configuration to remote access authentication attacks and system administrators with multiple authenticators for each network device.

Audit:

Review the Cisco switch configuration to verify that the device is configured to use at least two authentication servers as the primary source for authentication as shown in the example below:

```
aaa new-model
!
aaa authentication CONSOLE local
aaa authentication login LOGIN_AUTHENTICATION group radius local
…
…
…
ip http authentication aaa login-authentication LOGIN_AUTHENTICATION
ip http secure-server
…
…
…
radius-server host x.x.x.x auth-port 1812 acct-port 1813 key xxxxxxx
radius-server host x.x.x.x auth-port 1812 acct-port 1813 key xxxxxxx
…
…
…
line con 0
exec-timeout 5 0
login authentication CONSOLE
line vty 0 1
exec-timeout 5 0
login authentication LOGIN_AUTHENTICATION
```

If the Cisco switch is not configured to use at least two authentication servers to authenticate users prior to granting administrative access, this is a finding.

Remediation:

Step 1: Configure the Cisco switch to use at least two authentication servers as shown in the example below:
SW4(config)#radius host 10.1.48.2 key xxxxxx
SW4(config)#radius host 10.1.48.3 key xxxxxx
Step 2: Configure the authentication order to use the authentication servers as the primary source for authentication as shown in the example below:
SW4(config)#aaa authentication CONSOLE local
SW4(config)#aaa authentication login LOGIN_AUTHENTICATION group radius local
Step 3: Configure all network connections associated with device management to use the authentication servers for login authentication:
SW4(config)#line vty 0 1
SW4(config-line)#login authentication LOGIN_AUTHENTICATION
SW4(config-line)#exit
SW4(config)#line con 0
SW4(config-line)#login authentication CONSOLE
SW4(config-line)#exit
SW4(config)#ip http authentication aaa login-authentication LOGIN_AUTHENTICATION

Additional Information:

CCI-000370 Manage configuration settings for organization-defined system components using organization-defined automated mechanisms.

- NIST SP 800-53::CM-6 (1)
- NIST SP 800-53A::CM-6 (1).1
- NIST SP 800-53 Revision 4::CM-6 (1)
- NIST SP 800-53 Revision 5::CM-6 (1)

1.40 CISC-ND-001410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to support organizational requirements to conduct backups of the configuration when changes occur.

```
GROUP ID: V-220618
RULE ID: SV-220618r1069531
```

Rationale:

System-level information includes default and customized settings and security attributes, including access control lists (ACLs) that relate to the network device configuration, as well as software required for the execution and operation of the device. Information system backup is a critical step in ensuring system integrity and availability. If the system fails and there is no backup of the system-level information, a denial-of-service condition is possible for all who use this critical network component.

The network device must support the organizational central backup process for system-level information associated with the network device. This function may be provided by the network device itself; however, the preferred best practice is a centralized backup rather than each network device performing discrete backups.

Audit:

Review the Cisco switch configuration to verify that it backs up the configuration when changes occur. The example configuration below will send the configuration to a SCP server when a configuration change occurs:
event manager applet BACKUP_CONFIG
event syslog pattern "%SYS-5-CONFIG_I"
action 1 info type switchname
action 2 cli command "enable"
action 3 cli command "copy run scp" pattern "remote host"
action 4 cli command "x.x.x.x" pattern "filename"
action 5 cli command "$_info_switchname-config"
action 6 syslog priority informational msg "Configuration backup was executed"
If the Cisco switch is not configured to conduct backups of the configuration when changes occur, this is a finding.

Remediation:

Configure the Cisco switch to send the configuration to a SCP server when a configuration change occurs as shown in the example below:
SW4(config)#event manager applet BACKUP_CONFIG
SW4(config-applet)#event syslog pattern "%SYS-5-CONFIG_I"
SW4(config-applet)#action 1 cli command "enable"
SW4(config-applet)#action 2 info type switchname
SW4(config-applet)#action 3 cli command "copy run scp" pattern "remote host"
SW4(config-applet)#action 4 cli command "x.x.x.x" pattern "filename"
SW4(config-applet)#action 5 cli command "$_info_switchname-config"
SW4(config-applet)#action 6 syslog priority informational msg "Configuration backup was executed"
SW4(config-applet)#end

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

CCI-000537 Conduct backups of system-level information contained in the system per organization-defined frequency that is consistent with recovery time and recovery point objectives.

- NIST SP 800-53::CP-9 (b)
- NIST SP 800-53A::CP-9.1 (v)
- NIST SP 800-53 Revision 4::CP-9 (b)
- NIST SP 800-53 Revision 5::CP-9 (b)

1.41 CISC-ND-001440 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to obtain its public key certificates from an appropriate certificate policy through an approved service provider.

```
GROUP ID: V-220619
RULE ID: SV-220619r991871
```

Rationale:

Each organization obtains user certificates from an approved, shared service provider as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority (CA) at medium assurance or higher, this CA will suffice.

Audit:

Note: This requirement is not applicable if the router or switch does not have any public key certificates.
Review the switch configuration to determine if a CA trust point has been configured. The CA trust point will contain the URL of the CA in which the switch has enrolled. Verify this is a DOD or DOD-approved CA. This will ensure the switch has enrolled and received a certificate from a trusted CA. The CA trust point configuration would look similar to the example below:
crypto pki trustpoint CA_X
enrollment url http://trustpoint1.example.com
Note: A remote endpoint's certificate will always be validated by the switch by verifying the signature of the CA on the certificate using the CA's public key, which is contained in the switch's certificate that it received at enrollment.
If the Cisco switch is not configured to obtain its public key certificates from an appropriate certificate policy through an approved service provider, this is a finding.

Remediation:

Configure the switch to obtain its public key certificates from an appropriate certificate policy through an approved service provider as show in the example below:
SW2(ca-trustpoint)#enrollment url http://trustpoint1.example.com

Additional Information:

CCI-001159 Issue public key certificates under an organization-defined certificate policy or obtain public key certificates from an approved service provider.

- NIST SP 800-53::SC-17
- NIST SP 800-53A::SC-17.1
- NIST SP 800-53 Revision 4::SC-17
- NIST SP 800-53 Revision 5::SC-17 a

CCI-004909 Include only approved trust anchors in trust stores or certificate stores managed by the organization.

- NIST SP 800-53 Revision 5::SC-17 b

1.42 CISC-ND-001450 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must be configured to send log data to at least two central log servers for the purpose of forwarding alerts to the administrators and the information system security officer (ISSO).

```
GROUP ID: V-220620
RULE ID: SV-220620r961863
```

Rationale:

The aggregation of log data kept on a syslog server can be used to detect attacks and trigger an alert to the appropriate security personnel. The stored log data can used to detect weaknesses in security that enable the network Information Assurance (IA) team to find and address these weaknesses before breaches can occur.

Reviewing these logs, whether before or after a security breach, is important in showing whether someone is an internal employee or an outside threat.

Audit:

Verify that the switch is configured to send logs to at least two central log servers. The configuration should be similar to the example below:
logging x.x.x.x
logging x.x.x.x
If the switch is not configured to send log data to the syslog servers, this is a finding.

Remediation:

Configure the switch to send log messages to the syslog servers as shown in the example below:
SW4(config)#logging host x.x.x.x
SW4(config)#logging host x.x.x.x

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)

1.43 CISC-ND-001470 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must be running an IOS release that is currently supported by Cisco Systems.

```
GROUP ID: V-220621
RULE ID: SV-220621r961863
```

Rationale:

Network devices running an unsupported operating system lack current security fixes required to mitigate the risks associated with recent vulnerabilities. Running a supported release enables operations to maintain a stable and reliable network provided by improved quality of service and security features.

Audit:

Verify that the switch is in compliance with this requirement by having the switch administrator enter the following command:
show version
Verify that the release is still supported by Cisco. All releases supported by Cisco can be found at:
www.cisco.com/c/en/us/support/ios-nx-os-software
If the switch is not running a supported release, this is a finding.

Remediation:

Upgrade the switch to a supported release.

Additional Information:

CCI-002605 Install security-relevant software updates within an organization-defined time period of the release of the updates.

- NIST SP 800-53 Revision 4::SI-2 c
- NIST SP 800-53 Revision 5::SI-2 c

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	CISC-ND-000010 (Manual)	☐	☐
1.2	CISC-ND-000090 (Manual)	☐	☐
1.3	CISC-ND-000100 (Manual)	☐	☐
1.4	CISC-ND-000110 (Manual)	☐	☐
1.5	CISC-ND-000120 (Manual)	☐	☐
1.6	CISC-ND-000140 (Manual)	☐	☐
1.7	CISC-ND-000150 (Manual)	☐	☐
1.8	CISC-ND-000160 (Manual)	☐	☐
1.9	CISC-ND-000210 (Manual)	☐	☐
1.10	CISC-ND-000280 (Manual)	☐	☐
1.11	CISC-ND-000290 (Manual)	☐	☐
1.12	CISC-ND-000380 (Manual)	☐	☐
1.13	CISC-ND-000330 (Manual)	☐	☐
1.14	CISC-ND-000390 (Manual)	☐	☐
1.15	CISC-ND-000460 (Manual)	☐	☐
1.16	CISC-ND-000470 (Manual)	☐	☐
1.17	CISC-ND-000490 (Manual)	☐	☐
1.18	CISC-ND-000550 (Manual)	☐	☐
1.19	CISC-ND-000570 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	CISC-ND-000590 (Manual)	☐	☐
1.21	CISC-ND-000580 (Manual)	☐	☐
1.22	CISC-ND-000600 (Manual)	☐	☐
1.23	CISC-ND-000610 (Manual)	☐	☐
1.24	CISC-ND-000620 (Manual)	☐	☐
1.25	CISC-ND-000720 (Manual)	☐	☐
1.26	CISC-ND-000880 (Manual)	☐	☐
1.27	CISC-ND-000980 (Manual)	☐	☐
1.28	CISC-ND-001000 (Manual)	☐	☐
1.29	CISC-ND-001030 (Manual)	☐	☐
1.30	CISC-ND-001130 (Manual)	☐	☐
1.31	CISC-ND-001140 (Manual)	☐	☐
1.32	CISC-ND-001150 (Manual)	☐	☐
1.33	CISC-ND-001200 (Manual)	☐	☐
1.34	CISC-ND-001210 (Manual)	☐	☐
1.35	CISC-ND-001220 (Manual)	☐	☐
1.36	CISC-ND-001250 (Manual)	☐	☐
1.37	CISC-ND-001260 (Manual)	☐	☐
1.38	CISC-ND-001270 (Manual)	☐	☐
1.39	CISC-ND-001370 (Manual)	☐	☐
1.40	CISC-ND-001410 (Manual)	☐	☐
1.41	CISC-ND-001440 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	CISC-ND-001450 (Manual)	☐	☐
1.43	CISC-ND-001470 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 25, 2025	1.0.0	Initial CIS Release