CIS Center for Internet Security®

CIS Benchmarks™

CIS Cisco NX OS Switch NDM STIG Benchmark

v1.0.0 - 09-05-2025

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 NX OS Switch NDM Secure Technical Implementation Guide (STIG)

Version: 3 Release: 4 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 NX OS 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 NX OS Switch NDM

Recommendations

1 STIG RULES

Cisco NX-OS

Cisco NX OS Switch NDM Secure Technical Implementation Guide (STIG)

Version: 3 Release: 4 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-220474
RULE ID: SV-220474r960735
```

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 upon 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:

Review the switch configuration to determine if concurrent management sessions are limited as show in the example below:

```
line vty
 session-limit 2
```

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)# line vty
SW4(config)# session-limit 2
```

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-220475
RULE ID: SV-220475r960777
```

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.

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

```
aaa accounting default group RADIUS_SERVERS
```

Step 2: Verify that the referenced group name has defined AAA servers that are online.

```
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.12
```

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

If account creation is not automatically audited, this is a finding.

Remediation:

Configure the switch to log account creation using the following steps:

Step 1: Configure the AAA servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.48.10
SW1(config)# radius-server host 10.1.48.12
```

Step 2: Configure an AAA server group as shown in the example below:

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.12
SW1(config-radius)# exit
```

Step 3: Enable AAA accounting as shown in the example below:

```
SW1(config)# aaa accounting default group RADIUS_SERVERS
SW1(config)# 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-220476
RULE ID: SV-220476r960780
```

Rationale:

Since 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.

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

aaa accounting default group RADIUS_SERVERS

Step 2: Verify that the referenced group name has defined AAA servers that are online.

aaa group server radius RADIUS_SERVERS

server 10.1.48.10

server 10.1.48.12

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

If account modification is not automatically audited, this is a finding.

Remediation:

Configure the switch to log account modification using the following steps:

Step 1: Configure the AAA servers as shown in the example below:

SW1(config)# radius-server host 10.1.48.10

SW1(config)# radius-server host 10.1.48.12

Step 2: Configure an AAA server group as shown in the example below:

SW1(config)# aaa group server radius RADIUS_SERVERS

SW1(config-radius)# server 10.1.48.10

SW1(config-radius)# server 10.1.48.12

SW1(config-radius)# exit

Step 3: Enable AAA accounting as shown in the example below:

SW1(config)# aaa accounting default group RADIUS_SERVERS

SW1(config)# 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-220477
RULE ID: SV-220477r960783
```

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.

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

```
aaa accounting default group RADIUS_SERVERS
```

Step 2: Verify that the referenced group name has defined AAA servers that are online.

```
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.12
```

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

If account disabling is not automatically audited, this is a finding.

Remediation:

Configure the switch to log account disabling using the following steps:

Step 1: Configure the AAA servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.48.10
SW1(config)# radius-server host 10.1.48.12
```

Step 2: Configure an AAA server group as shown in the example below:

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.12
SW1(config-radius)# exit
```

Step 3: Enable AAA accounting as shown in the example below:

```
SW1(config)# aaa accounting default group RADIUS_SERVERS
SW1(config)# 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-220478
RULE ID: SV-220478r960786
```

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.

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

```
aaa accounting default group RADIUS_SERVERS
```

Step 2: Verify that the referenced group name has defined AAA servers that are online.

```
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.12
```

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

If account removal is not automatically audited, this is a finding.

Remediation:

Configure the switch to log account removal using the following steps:

Step 1: Configure the AAA servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.48.10
SW1(config)# radius-server host 10.1.48.12
```

Step 2: Configure an AAA server group as shown in the example below:

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.12
SW1(config-radius)# exit
```

Step 3: Enable AAA accounting as shown in the example below:

```
SW1(config)# aaa accounting default group RADIUS_SERVERS
SW1(config)# 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-220479
RULE ID: SV-220479r991956
```

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 it is compliant with this requirement.

Step 1: Verify that the line vty has an ACL inbound applied as shown in the example below:

```
line vty
 access-class MGMT_NET in
```

Step 2: Verify that the ACL permits only hosts from the management network to access the switch.

```
ip access-list MGMT_NET
 10 permit ip 10.1.48.0/24 any
 20 deny ip any any log
```

NX-OS v8 and later example:

Step 1: Verify that an ACL has been applied to the management interface inbound as shown in the example below:

```
interface mgmt0
ip access-group MGMT_NET in
```

Step 2: Verify that the ACL permits only hosts from the management network to access the switch.

```
ip access-list MGMT_NET
10 permit ip 10.1.48.0/24 any
20 deny ip any any log
```

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 as shown in the example below:

```
SW1(config)# ip access-list MGMT_NET
SW1(config-acl)# permit ip 10.1.48.0/24 any
SW1(config-acl)# deny ip any any log
SW1(config-acl)# exit
SW1(config)# line vty
SW1(config-line)# access-class MGMT_NET in
SW1(config-acl)# end
```

NX-OS v8 and later example:

```
SW1(config)# ip access-list MGMT_NET
SW1(config-acl)# permit ip 10.1.48.0/24 any
SW1(config-acl)# deny ip any any log
SW1(config-acl)# exit
SW1(config)# interface mgmt0
SW1(config-if)#  ip access-group MGMT_NET in
SW1(config-acl)# 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 disconnect the session.

```
GROUP ID: V-220480
RULE ID: SV-220480r960840
```

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:

```
ssh login-attempts 3
```

If the Cisco switch is not configured to enforce the limit of three consecutive invalid logon attempts, this is a finding.

NOTE: The NX-OS switch does not lock out the account, it disconnects the session. The AAA server will lock out the user account on three failed attempts.

Remediation:

Configure the Cisco switch to enforce the limit of three consecutive invalid logon attempts as shown in the example below:

```
SW2(config)# ssh login-attempts 3
```

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-220481
RULE ID: SV-220481r960843
```

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 is compliant with this requirement as shown in the example below:

```
banner motd #
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.
#
```

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 motd #
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 switch must be configured to protect against an individual falsely denying having performed organization-defined actions to be covered by non-repudiation.

```
GROUP ID: V-220482
RULE ID: SV-220482r960864
```

Rationale:

This requirement supports non-repudiation of actions taken by an administrator and is required in order 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 is compliant with this requirement as shown in steps below:

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

```
aaa accounting default group RADIUS_SERVERS
```

Step 2: Verify that the referenced group name has defined AAA servers that are online.

```
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.12
```

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

If logging of administrator activity is not configured, this is a finding.

Remediation:

Configure the switch to log administrator activity as shown in the steps below:

Step 1: Configure the AAA servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.48.10
SW1(config)# radius-server host 10.1.48.12
```

Step 2: Configure an AAA server group as shown in the example below:

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.12
SW1(config-radius)# exit
```

Step 3: Enable AAA accounting as shown in the example below:

```
SW1(config)# aaa accounting default group RADIUS_SERVERS
SW1(config)# 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

1.10 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-220484
RULE ID: SV-220484r1026067
```

Rationale:

In order 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:

Step 1: Review the deny statements in all ACLs to determine if the log parameter has been configured as shown in the example below:

```
ip access-list extended BLOCK_INBOUND
 deny icmp any any log
```

Step 2: Verify that the Optimized Access-list Logging (OAL) has been configured.

```
logging ip access-list cache entries nnnn
```

Note: Once OAL has been enabled, the logged ACL hits can be viewed via the show logging ip access-list cache command.

If the switch is not configured with the log parameter after any deny statements to note where packets have been dropped via an ACL, this is a finding.

Remediation:

Enable OAL as shown in the example below:

```
SW1(config)# logging ip access-list cache entries nnnn
```

Set the 'log' parameter after any 'deny' entries in the ACL as referenced in the check text above.

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

1.11 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-220485
RULE ID: SV-220485r960909
```

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 is compliant with this requirement.

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

```
aaa accounting default group RADIUS_SERVERS
```

Step 2: Verify that the referenced group name has defined AAA servers that are online.

```
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.12
```

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

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:

Step 1: Configure the AAA servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.48.10
SW1(config)# radius-server host 10.1.48.12
```

Step 2: Configure an AAA server group as shown in the example below:

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.12
SW1(config-radius)# exit
```

Step 3: Enable AAA accounting as shown in the example below:

```
SW1(config)# aaa accounting default group RADIUS_SERVERS
SW1(config)# 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)

1.12 CISC-ND-000470 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-220486
RULE ID: SV-220486r1043177
```

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, then it must be documented and approved.

Audit:

Verify that the switch does not have any unnecessary or non-secure ports, protocols and services enabled. For example, the following features such as telnet should never be enabled, while other features should only be enabled if required for operations.

```
feature telnet

feature dhcp

feature wccp

feature nxapi

feature imp
```

If any unnecessary or non-secure ports, protocols, or services are enabled, this is a finding.

Remediation:

Disable features that should not be enabled unless required for operations.

```
SW2(config)# no feature telnet
SW2(config)# no feature dhcp
SW2(config)# no feature wccp
SW2(config)# no feature nxapi
SW2(config)# no feature imp
```

Note: Telnet must always be disabled.

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

1.13 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-220487
RULE ID: SV-220487r1051115
```

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 xxxxxxxxxxxx password 5
$5$88SPgpAn$Q6/17o5U/5lz4dNL1iQZuj/1a0wcKdrk29ZH1HJsnF. role priv-9
```

Step 2: Verify that the fallback to use local account has not been disabled as shown in the example below:

```
no aaa authentication login default fallback error local
```

Note: The fallback is enabled by default; hence the above command should not be seen in the configuration.

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)# switch(config)# username xxxxxxx password xxxxxx role priv-9
```

Step 2: Configure the authentication to use an AAA server with the fallback 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 RADIUS_SERVERS
SW2(config)# aaa authentication login default fallback error local
SW2(config)# end
```

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

1.14 CISC-ND-000530 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to implement replay-resistant authentication mechanisms for network access to privileged accounts.

```
GROUP ID: V-220488
RULE ID: SV-220488r1026069
```

Rationale:

A replay attack may enable an unauthorized user to gain access to the application. Authentication sessions between the authenticator and the application validating the user credentials must not be vulnerable to a replay attack.

An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message.

Audit:

Review the Cisco router configuration to verify it is compliant with this requirement as shown in the example below.

SSH Example

```
ssh macs hmac-sha2-256 hmac-sha2-512
```

NOTE: Using "fips mode enable" to enable all FIPS protocols disables TACACS+ and RADIUS, which is required for authentication server requirements. It is recommended to enable FIPS-validated protocols manually and keep FIPS mode disabled.

If the Cisco router 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

```
R1(config)#ssh macs hmac-sha2-256 hmac-sha2-512
```

Additional Information:

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

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

1.15 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-220489
RULE ID: SV-220489r1026157
```

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:

Password complexity is enabled by default. Review the Cisco switch configuration to verify that it is compliant with this requirement. The following command should not be found in the configuration:

```
no password strength-check
```

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)# password strength-check
```

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)

1.16 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 lower-case character be used.

```
GROUP ID: V-220490
RULE ID: SV-220490r1026158
```

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:

Password complexity is enabled by default. Review the Cisco switch configuration to verify that it is compliant with this requirement. The following command should not be found in the configuration:

```
no password strength-check
```

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)# password strength-check
```

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)

1.17 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-220491
RULE ID: SV-220491r1026159
```

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:

Password complexity is enabled by default. Review the Cisco switch configuration to verify that it is compliant with this requirement. The following command should not be found in the configuration:

```
no password strength-check
```

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)# password strength-check
```

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)

1.18 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-220492
RULE ID: SV-220492r1026160
```

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:

Password complexity is enabled by default. Review the Cisco switch configuration to verify that it is compliant with this requirement. The following command should not be found in the configuration:

```
no password strength-check
```

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)# password strength-check
```

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)

1.19 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-220493
RULE ID: SV-220493r961068
```

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 also 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 following example:

```
line console
 exec-timeout 5
line vty
 exec-timeout 5
```

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 console
SW1(config-console)# exec-timeout 5
SW1(config-console)# exit
SW1(config)# line vty
SW1(config-line)# exec-timeout 5
```

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

1.20 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-220494
RULE ID: SV-220494r961290
```

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 simply 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 which documents the creation of application user accounts and notifies administrators and Information System Security Officers (ISSO). 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:

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

aaa accounting default group RADIUS_SERVERS

Step 2: Verify that the referenced group name has defined AAA servers that are online.

```
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.12
```

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

If account enabling is not automatically audited, this is a finding.

Remediation:

Configure the switch to log account enabling using the following steps:

Step 1: Configure the AAA servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.48.10
SW1(config)# radius-server host 10.1.48.12
```

Step 2: Configure an AAA server group as shown in the example below:

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.12
SW1(config-radius)# exit
```

Step 3: Enable AAA accounting as shown in the example below:

```
SW1(config)# aaa accounting default group RADIUS_SERVERS
SW1(config)# 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)

1.21 CISC-ND-000940 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to audit the execution of privileged functions.

```
GROUP ID: V-220495
RULE ID: SV-220495r961362
```

Rationale:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Audit:

Review the Cisco switch configuration to verify that it is compliant with this requirement. The configuration example below will log all configuration changes.

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

```
aaa accounting default group RADIUS_SERVERS
```

Step 2: Verify that the referenced group name has defined AAA servers that are online.

```
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.12
```

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

If the Cisco switch is not configured to log all configuration changes, this is a finding.

Remediation:

Configure the Cisco switch to log all configuration changes as shown in the following example:

Step 1: Configure the AAA servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.48.10
SW1(config)# radius-server host 10.1.48.12
```

Step 2: Configure an AAA server group as shown in the example below:

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.12
SW1(config-radius)# exit
```

Step 3: Enable AAA accounting as shown in the example below:

```
SW1(config)# aaa accounting default group RADIUS_SERVERS
SW1(config)# end
```

Additional Information:

CCI-002234 Log the execution of privileged functions.

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

1.22 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-220496
RULE ID: SV-220496r961392
```

Rationale:

In order to ensure 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 logfile size. The configuration should look like the example below:

```
logging logfile LOGFILE1 6 size nnnnn
```

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 logfile LOGFILE1 6 size nnnnn
```

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

1.23 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-220497
RULE ID: SV-220497r991965
```

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 is compliant with this requirement as shown in the example below:

```
logging server 10.1.48.10 2
```

Note: The parameter 2 (critical) can replaced with a lesser severity level 3 through 6 (i.e. error, warning, notice, informational). Informational is the default severity level; hence, if the severity level is configured to informational, the parameter 7 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 server 10.1.48.10 2
```

Note: The parameter 2 (critical) can replaced with a lesser severity level 3 through 6 (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

1.24 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-220498
RULE ID: SV-220498r1026071
```

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 utilize 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 it is compliant with this requirement as shown in the configuration example below:

```
ntp server 10.1.12.10
ntp server 10.1.22.13
```

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:

```
SW1(config)# feature ntp
SW1(config)# ntp server 10.1.12.10
SW1(config)# ntp server 10.1.22.13
SW1(config)# end
```

Additional Information:

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)

1.25 CISC-ND-001050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to record time stamps for log records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

```
GROUP ID: V-220499
RULE ID: SV-220499r961443
```

Rationale:

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the application include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

Audit:

Review the Cisco switch configuration to verify that it is compliant with this requirement as shown in the example below:

```
clock timezone EST -5 0
```

Note: UTC is the default; hence, the command set time-zone may not be seen in the configuration. This can be verified using the show system uptime command.

If the switch is not configured to record time stamps for log records that can be mapped to UTC or GMT, this is a finding.

Remediation:

Configure the Cisco switch to record time stamps for audit records that can be mapped to UTC or GMT as shown in the example below:

```
SW1(config)# clock timezone EST -5 0
```

Additional Information:

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

1.26 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-220500
RULE ID: SV-220500r961506
```

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 is compliant with this requirement as shown in the example below:

```
snmp-server user NETOPS auth sha 5Er23@#as178 priv aes-128
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

snmp-server host 10.1.48.10 traps version 3 priv NETOPS
```

Authentication used by the SNMP users can be viewed via the show snmp user command as shown in the example below:

```
SW1# show snmp user

_____________________________________________________________
 SNMP USERS

_____________________________________________________________

User Auth Priv(enforce) Groups acl_filter

____ ____ ____________ ______ __________
NETOPS sha aes-128 network-operator
```

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:

```
SW1(config)# snmp-server user NETOPS auth sha xxxxxxxxxxxxx priv aes-128
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

SW1(config)# snmp-server host 10.1.48.10 traps version 3 priv NETOPS
```

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)

1.27 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-220501
RULE ID: SV-220501r961506
```

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 is compliant with this requirement as shown in the example below:

```
snmp-server user NETOPS auth sha 5Er23@#as178 priv aes-128
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

snmp-server host 10.1.48.10 traps version 3 priv NETOPS
```

Encryption used by the SNMP users can be viewed via the show snmp user command as shown in the example below:

```
SW1# show snmp user
_____________________________________________________________
 SNMP USERS
_____________________________________________________________

User Auth Priv(enforce) Groups acl_filter
____ ____ ____________ ______ __________
NETOPS sha aes-128 network-operator
```

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:

```
SW1(config)# snmp-server user NETOPS auth sha xxxxxxxxxxxx priv aes-128
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

SW1(config)# snmp-server host 10.1.48.10 traps version 3 priv NETOPS
```

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)

1.28 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-220502
RULE ID: SV-220502r1107166
```

Rationale:

If Network Time Protocol 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 is compliant with this requirement as shown in the configuration example below:

```
ntp distribute
ntp server 10.1.12.10 key 1
ntp server 10.1.22.13 key 1
ntp authenticate
ntp authentication-key 1 hmac-sha2-256 xxxxxx
ntp trusted-key 1
ntp commit
```

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:

```
SW1(config)# ntp authenticate
SW1(config)# ntp authentication-key 1 hmac-sha2-256 xxxxxx
SW1(config)# ntp trusted-key 1
SW1(config)# ntp server 10.1.12.10 key 1
SW1(config)# ntp server 10.1.22.13 key 1
SW1(config)# ntp commit
SW1(config)# end
```

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)

1.29 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-220503
RULE ID: SV-220503r1026073
```

Rationale:

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

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, 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 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 router configuration to verify it is compliant with this requirement as shown in the example below.

SSH Example

```
ssh macs hmac-sha2-256 hmac-sha2-512
```

NOTE: Using "fips mode enable" to enable all FIPS protocols disables TACACS+ and RADIUS, which is required for authentication server requirements. It is recommended to enable FIPS-validated protocols manually and keep FIPS mode disabled.

If the Cisco router 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

```
R1(config)#ssh macs hmac-sha2-256 hmac-sha2-512
```

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)

1.30 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-220504
RULE ID: SV-220504r1026075
```

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 potentially allowing hijacking of maintenance sessions.

Audit:

Review the Cisco router configuration to verify it is compliant with this requirement.

SSH Example

```
ssh ciphers aes128-ctr aes256-ctr
```

NOTE: Using "fips mode enable" to enable all FIPS protocols disables TACACS+ and RADIUS, which is required for authentication server requirements. It is recommended to enable FIPS-validated protocols manually and keep FIPS mode disabled.

If the router 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 router to implement cryptographic mechanisms to protect the confidentiality of remote maintenance sessions using a FIPS 140-2 approved algorithm as shown in the examples below.

SSH Example

```
R1(config)#ssh ciphers aes128-ctr aes256-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)

1.31 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-260464
RULE ID: SV-260464r1082186
```

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 it is compliant with this requirement.

Step 1: Verify traffic types have been classified based on importance levels. The following is an example configuration:

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

Step 2: Review the 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 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 type control-plane to determine if the traffic is being policed appropriately for each classification. The following is an example configuration:

policy-map type control-plane 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 the CoPP policy is enabled. The following is an example configuration:

control-plane

service-policy input CONTROL_PLANE_POLICY

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 ACLs' specific traffic types.

```
SW1(config)# ip access-list CoPP_CRITICAL
SW1(config-acl)# remark our control plane adjacencies are critical
SW1(config-acl)# permit ospf host 10.1.12.1 any
SW1(config-acl)# permit ospf host 10.1.22.1 any
SW1(config-acl)# permit pim host 10.1.12.1 any
SW1(config-acl)# permit pim host 10.1.22.1 any
SW1(config-acl)# permit pim host 10.1.33.4 any
SW1(config-acl)# permit igmp any 224.0.0.0 15.255.255.255
SW1(config-acl)# permit tcp host 10.2.33.3 eq bgp host 10.2.33.4
SW1(config-acl)# permit tcp host 10.2.33.3 host 10.2.33.4 eq bgp
SW1(config-acl)# deny ip any any
SW1(config-acl)# exit

SW1(config)# ip access-list CoPP_IMPORTANT
SW1(config-acl)# permit tcp host 10.1.33.5 eq tacacs any
SW1(config-acl)# permit tcp 10.1.33.0 0.0.0.255 any eq 22
SW1(config-acl)# permit udp host 10.1.33.7 any eq snmp
SW1(config-acl)# permit udp host 10.1.33.9 eq ntp any
SW1(config-acl)# deny ip any any
SW1(config-acl)# exit

SW1(config)# ip access-list CoPP_NORMAL
SW1(config-acl)# remark we will want to rate limit ICMP traffic
SW1(config-acl)# permit icmp any any echo
SW1(config-acl)# permit icmp any any echo-reply
SW1(config-acl)# permit icmp any any time-exceeded
SW1(config-acl)# permit icmp any any unreachable
SW1(config-acl)# deny ip any any
SW1(config-acl)# exit

SW1(config)# ip access-list CoPP_UNDESIRABLE
SW1(config-acl)# remark other management plane traffic that should not be
received
SW1(config-acl)# permit udp any any eq ntp
SW1(config-acl)# permit udp any any eq snmp
SW1(config-acl)# permit tcp any any eq 22
SW1(config-acl)# permit tcp any any eq 23
SW1(config-acl)# remark other control plane traffic not configured on switch
SW1(config-acl)# permit eigrp any any
SW1(config-acl)# permit udp any any eq rip
SW1(config-acl)# deny ip any any
SW1(config-acl)# exit

SW1(config)# ip access-list CoPP_DEFAULT
SW1(config-acl)# permit ip any any
SW1(config-acl)# exit
```

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

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

1.32 CISC-ND-001240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-220506
RULE ID: SV-220506r961800
```

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:

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

```
aaa accounting default group RADIUS_SERVERS
```

Step 2: Verify that the referenced group name has defined AAA servers that are online.

```
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.12
```

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

If the Cisco switch is not configured to generate log records when administrator privileges are modified, this is a finding.

Remediation:

Configure the Cisco switch to generate log records when account privileges are modified as shown in the example below:

Step 1: Configure the AAA servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.48.10
SW1(config)# radius-server host 10.1.48.12
```

Step 2: Configure an AAA server group as shown in the example below:

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.12
SW1(config-radius)# exit
```

Step 3: Enable AAA accounting as shown in the example below:

```
SW1(config)# aaa accounting default group RADIUS_SERVERS
SW1(config)# 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

1.33 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-220507
RULE ID: SV-220507r961812
```

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 is compliant with this requirement as shown in the example below:

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

```
aaa accounting default group RADIUS_SERVERS
```

Step 2: Verify that the referenced group name has defined AAA servers that are online.

```
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.12
```

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

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:

Step 1: Configure the AAA servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.48.10
SW1(config)# radius-server host 10.1.48.12
```

Step 2: Configure an AAA server group as shown in the example below:

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.12
SW1(config-radius)# exit
```

Step 3: Enable AAA accounting as shown in the example below:

```
SW1(config)# aaa accounting default group RADIUS_SERVERS
SW1(config)# 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

1.34 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-220508
RULE ID: SV-220508r961824
```

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 is compliant with this requirement as shown in the examples below:

```
logging logfile LOG_FILE 6
logging level authpri 6
```

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:

Step 1: Lower the authpriv level to 6.

```
SW1(config)# logging level authpriv 6
```

Step 2: Configure a logfile to record log messages at level 6.

```
SW1(config)# logging logfile LOG_FILE 6
```

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

1.35 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-220509
RULE ID: SV-220509r961827
```

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:

Step 1: Verify that account records will be sent to an AAA server as shown in the example below:

```
aaa accounting default group RADIUS_SERVERS
```

Step 2: Verify that the referenced group name has defined AAA servers that are online.

```
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.12
```

Note: Cisco NX-OS devices report configuration activity to TACACS+ or RADIUS servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

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:

Step 1: Configure the AAA servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.48.10
SW1(config)# radius-server host 10.1.48.12
```

Step 2: Configure an AAA server group as shown in the example below:

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.12
SW1(config-radius)# exit
```

Step 3: Enable AAA accounting as shown in the example below:

```
SW1(config)# aaa accounting default group RADIUS_SERVERS
SW1(config)# 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

1.36 CISC-ND-001280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must generate audit records showing starting and ending time for administrator access to the system.

```
GROUP ID: V-220510
RULE ID: SV-220510r961830
```

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:

Verify that the switch is configured to generate log records showing starting and ending time for administrator access as shown in the example below:

```
logging level authpri 6
```

If the switch is not configured to generate log records showing starting and ending time for administrator access, this is a finding.

Remediation:

Configure the switch to log session start and ending per admin session as shown in the example below:

```
SW1(config)# logging level authpriv 6
```

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-001310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured to off-load log records onto a different system than the system being audited.

```
GROUP ID: V-220512
RULE ID: SV-220512r961860
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Audit:

Review the Cisco switch configuration to verify that it is compliant with this requirement as shown in the example below:

```
logging server 10.1.48.10 6
```

If the Cisco switch is not configured to off-load log records onto a different system than the system being audited, this is a finding.

Remediation:

Configure the Cisco switch to send log records to a syslog server as shown in the example below:

```
SW4(config)# logging server 10.1.48.10 6
```

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)

1.38 CISC-ND-001370 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must be configured to use at least two authentication servers for the purpose of authenticating users prior to granting administrative access.

```
GROUP ID: V-220513
RULE ID: SV-220513r961863
```

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 primary source for authentication.

Step 1: Verify that an AAA server group is configured for login authentication for both in-band and console access methods.

```
aaa authentication login default group RADIUS_SERVERS
aaa authentication login console group RADIUS_SERVERS
```

Step 2: Verify that at least two AAA servers have been defined for the server group as shown in the example below:

```
radius-server host 10.1.48.10 key 7 "xxxxxx"
radius-server host 10.1.48.11 key 7 "xxxxxx"
authentication accounting
aaa group server radius RADIUS_SERVERS
 server 10.1.48.10
 server 10.1.48.11
```

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

Remediation:

Configure the Cisco switch to use at least two authentication servers as shown in the following example:

Step 1: Define the authentication servers.

```
SW1(config)# radius-server host 10.1.48.10 key xxxxxx
SW1(config)# radius-server host 10.1.48.11 key xxxxxx
```

Step 2: Configure the AAA group.

```
SW1(config)# aaa group server radius RADIUS_SERVERS
SW1(config-radius)# server 10.1.48.10
SW1(config-radius)# server 10.1.48.11
```

Step 3: Use the AAA servers for login authentication for both in-band and console access methods.

```
SW1(config)# aaa authentication login default group RADIUS_SERVERS
SW1(config)# aaa authentication login console group RADIUS_SERVERS
```

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)

1.39 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-220514
RULE ID: SV-220514r1069522
```

Rationale:

System-level information includes default and customized settings and security attributes, including 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 utilize this critical network component.

This control requires the network device to 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 is compliant with this requirement. 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 "SYSLOG_CONFIG_I"
 action 1 cli command "copy startup-config scp://user@10.1.48.10/nx-
config.bak"
 action 2 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 an 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 "SYSLOG_CONFIG_I"
SW4(config-applet)# action 1 cli command "copy startup-config
scp://user@10.1.48.10/nx-config.bak”
SW4(config-applet)# action 2 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)

1.40 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-220515
RULE ID: SV-220515r991969
```

Rationale:

For user certificates, each organization obtains 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:

If PKI certificates are not implemented on the switch, this requirement is not applicable.

Step 1: Review the switch configuration to determine if a CA trust point has been configured as shown in the example below:

```
crypto ca trustpoint CA_X
 enrollment terminal
```

Step 2: Verify the CA is a DOD or DOD-approved service provider by entering the following command: show crypto ca certificates

The output will list the following information for each certificate:

```
Trustpoint (will map to a configured trustpoint from step 1)
Common Name (CN) of the issuer
Organization (O) of the issuer
Organization Unit (OU) of the issuer
```

Note: Cisco NX-OS software supports only the manual cut-and-paste method for certificate enrollment.

If the switch is not configured to obtain its public key certificates from a DOD or DOD-approved service provider, this is a finding.

Remediation:

Ensure that certificate requests are only sent to DOD or DOD-approved service providers.

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

1.41 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-220516
RULE ID: SV-220516r961863
```

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 IA team to find and address these weaknesses before breaches can occur. Reviewing these logs, whether before or after a security breach, are 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 syslog servers. The configuration should look similar to the example below:

```
logging server 10.1.48.10 6
logging server 10.1.48.11 6
```

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 server 10.1.48.10 6
SW4(config)# logging server 10.1.48.11 6
```

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)

1.42 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-220517
RULE ID: SV-220517r961863
```

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 also 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 on the following URL:

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-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-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

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-000290 (Manual)	☐	☐
1.11	CISC-ND-000330 (Manual)	☐	☐
1.12	CISC-ND-000470 (Manual)	☐	☐
1.13	CISC-ND-000490 (Manual)	☐	☐
1.14	CISC-ND-000530 (Manual)	☐	☐
1.15	CISC-ND-000570 (Manual)	☐	☐
1.16	CISC-ND-000580 (Manual)	☐	☐
1.17	CISC-ND-000590 (Manual)	☐	☐
1.18	CISC-ND-000600 (Manual)	☐	☐
1.19	CISC-ND-000720 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	CISC-ND-000880 (Manual)	☐	☐
1.21	CISC-ND-000940 (Manual)	☐	☐
1.22	CISC-ND-000980 (Manual)	☐	☐
1.23	CISC-ND-001000 (Manual)	☐	☐
1.24	CISC-ND-001030 (Manual)	☐	☐
1.25	CISC-ND-001050 (Manual)	☐	☐
1.26	CISC-ND-001130 (Manual)	☐	☐
1.27	CISC-ND-001140 (Manual)	☐	☐
1.28	CISC-ND-001150 (Manual)	☐	☐
1.29	CISC-ND-001200 (Manual)	☐	☐
1.30	CISC-ND-001210 (Manual)	☐	☐
1.31	CISC-ND-001220 (Manual)	☐	☐
1.32	CISC-ND-001240 (Manual)	☐	☐
1.33	CISC-ND-001250 (Manual)	☐	☐
1.34	CISC-ND-001260 (Manual)	☐	☐
1.35	CISC-ND-001270 (Manual)	☐	☐
1.36	CISC-ND-001280 (Manual)	☐	☐
1.37	CISC-ND-001310 (Manual)	☐	☐
1.38	CISC-ND-001370 (Manual)	☐	☐
1.39	CISC-ND-001410 (Manual)	☐	☐
1.40	CISC-ND-001440 (Manual)	☐	☐
1.41	CISC-ND-001450 (Manual)	☐	☐

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

Appendix: Change History

Date	Version	Changes for this version
Sep 5, 2025	1.0.0	Initial CIS Release