CIS Cisco IOS XR Router NDM STIG Benchmark

v1.0.0 - 09-03-2025

Terms of Use

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

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

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

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

Table of Contents

Overview

Target Technology Details

Cisco IOS XR Router NDM Secure Technical Implementation Guide (STIG)

Version: 3 Release: 3 Benchmark

Date: 02 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Cisco IOS XR Router NDM and are looking to comply with the STIG guidance

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

The Rule Title from the STIG.

Rationale Statement

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

Audit Procedure

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

Remediation Procedure

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

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

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

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

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

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

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

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

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

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

  This profile is intended for servers and workstations.

Acknowledgements

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

Recommendations

1 STIG RULES

Cisco IOS XR router

Cisco IOS XR Router NDM Secure Technical Implementation Guide (STIG)

Version: 3 Release: 3 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 CISC-ND-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216522
RULE ID: SV-216522r960735
```

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:

Note: This requirement is not applicable to file transfer actions such as FTP, SCP and SFTP.

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

ssh server session-limit 2

If the router is not configured to limit the number of concurrent management sessions, this is a finding.

Remediation:

Configure the router to limit the number of concurrent management sessions to an organization-defined number as shown in the example below.

RP/0/0/CPU0:R3(config)#ssh server 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-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216523
RULE ID: SV-216523r991929
```

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 router 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 default

access-class ingress MANAGEMENT_NET

transport input ssh

!

vty-pool default 0 4

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

ipv4 access-list MANAGEMENT_NET

10 permit ipv4 10.1.1.0 255.255.255.0 any

20 deny ipv4 any any log-input

If the Cisco router 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 router to restrict management access to specific IP addresses via SSH as shown in the example below.

RP/0/0/CPU0:ios(config)#ipv4 access-list MANAGEMENT_NET

RP/0/0/CPU0:ios(config-ipv4-acl)#permit ipv4 10.1.1.0 255.255.255.0 any

RP/0/0/CPU0:ios(config-ipv4-acl)#deny ipv4 any any log-input

RP/0/0/CPU0:ios(config-ipv4-acl)#exit

RP/0/0/CPU0:R3(config)#vty default 0 4

RP/0/0/CPU0:R3(config)#line default

RP/0/0/CPU0:R3(config-line)#transport input ssh

RP/0/0/CPU0:R3(config-line)#access-class MANAGEMENT_NET in

RP/0/0/CPU0:R3(config-line)#end

Additional Information:

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

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

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

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

1.3 CISC-ND-000150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216524
RULE ID: SV-216524r960840
```

Rationale:

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

Audit:

The Cisco router is not compliant with this requirement. However, the risk associated with this requirement can be fully mitigated if the router is configured to utilize an authentication server to authenticate and authorize users for administrative access.

Review the router configuration to verify that the device is configured to use an authentication server as primary source for authentication as shown in the following example:

radius-server host 10.1.3.16 auth-port 1645 acct-port 1646

key xxxxxxxxxx

…

…

…

aaa authentication login LOGIN_AUTHENTICATION group radius local

line console

login authentication LOGIN_AUTHENTICATION

!

line default

login authentication LOGIN_AUTHENTICATION

transport input ssh

If the router is not configured to use an authentication server to authenticate and authorize users for administrative access, this is a finding.

Remediation:

Step 1: Configure the router to use an authentication server as shown in the following example:

RP/0/0/CPU0:R3(config)#radius-server host 10.1.3.16 key xxxxxxxx

Step 2: Configure the authentication order to use the authentication server as primary source for authentication as shown in the following example:

RP/0/0/CPU0:R3(config)#aaa authentication login LOGIN_AUTHENTICATION group radius local

Step 3: Configure all network connections associated with a device management to use an authentication server for the purpose of login authentication as shown in the following example:

RP/0/0/CPU0:R3(config)#line default

RP/0/0/CPU0:R3(config-line)#login authentication LOGIN_AUTHENTICATION

RP/0/0/CPU0:R3(config-line)#exit

RP/0/0/CPU0:R3(config)#line console

RP/0/0/CPU0:R3(config-line)#login authentication LOGIN_AUTHENTICATION

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

1.4 CISC-ND-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216525
RULE ID: SV-216525r960843
```

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

banner login ^C

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

^C

If the Cisco router 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 router to display the Standard Mandatory DoD Notice and Consent Banner before granting access as shown in the following example:

RP/0/0/CPU0:R3(config)#banner login #

Enter TEXT message. End with the character '#'.

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. #

RP/0/0/CPU0:R3(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

1.5 CISC-ND-000250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco router must be configured to generate audit records when successful/unsuccessful attempts to logon with access privileges occur.

```
GROUP ID: V-216526
RULE ID: SV-216526r960885
```

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 information system (e.g., module or policy filter).

Audit:

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

logging buffered informational

logging 10.1.22.2 vrf default severity info

If the Cisco router is not configured to generate audit records when successful/unsuccessful attempts to logon, this is a finding.

Remediation:

Configure the Cisco router to log all logon attempts as shown in the example below.

RP/0/0/CPU0:R3(config)#logging buffered informational

RP/0/0/CPU0:R3(config)#logging 10.1.22.2 severity info

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

1.6 CISC-ND-000280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216527
RULE ID: SV-216527r960894
```

Rationale:

It is essential for security personnel to know what is being done, what was attempted, where it was done, when it was done, and by whom it was done in order to compile an accurate risk assessment. Logging the date and time of each detected event provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured network device. In order to establish and correlate the series of events leading up to an outage or attack, it is imperative the date and time are recorded in all log records.

Audit:

Verify that the router is configured to include the date and time on all log records as shown in the configuration example below.

service timestamps log datetime localtime

If time stamps are not configured, this is a finding.

Remediation:

Configure the router to include the date and time on all log records as shown in the example below.

RP/0/0/CPU0:R3(config)#service timestamps log datetime localtime

Additional Information:

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

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

1.7 CISC-ND-000290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216528
RULE ID: SV-216528r960897
```

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:

Review the deny statements in all interface ACLs to determine if the log-input parameter has been configured as shown in the example below.

Note: log-input can only apply to interface bound ACLs.

ipv4 access-list BLOCK_INBOUND

10 deny icmp any any log-input

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

Remediation:

Configure the log-input parameter after any deny statements to provide the location as to where packets have been dropped via an ACL.

RP/0/0/CPU0:R3(config)#ipv4 access-list BLOCK_INBOUND

RP/0/0/CPU0:R3(config-ipv4-acl)#deny icmp any any log-input

Additional Information:

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

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

1.8 CISC-ND-000470 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-216529
RULE ID: SV-216529r1043177
```

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 router does not have any unnecessary or nonsecure ports, protocols, and services enabled. For example, the following commands should not be in the configuration:

service ipv4 tcp-small-servers max-servers 10

service ipv4 udp-small-servers max-servers 10

http client vrf xxxxx

telnet vrf default ipv4 server max-servers 1

service call-home

Note: Certain legacy devices may require 'service call-home' be enabled to support Smart Licensing as they do not support the newer smart transport configuration. Those devices do not incur a finding for having call-home enabled for Smart Licensing.

If any unnecessary or nonsecure ports, protocols, or services are enabled, this is a finding.

Remediation:

Disable the following services if enabled as shown in the example below.

RP/0/0/CPU0:R3(config)#no service ipv4 tcp-small-servers

RP/0/0/CPU0:R3(config)#no service ipv4 udp-small-servers

RP/0/0/CPU0:R3(config)#no http client vrf xxxxx

RP/0/0/CPU0:R3(config)#no telnet ipv4 server

RP/0/0/CPU0:R3(config)#no service call-home

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

1.9 CISC-ND-000490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco router 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-216530
RULE ID: SV-216530r1051115
```

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 router configuration to verify that a local account for last resort has been configured.

username xxxxxxxxxxxx

group netadmin

secret 5 xxxxxxxxxxxxxxxxxxxx

Note: The following groups should not be assigned to this local account: root-system and root-lr. A custom group that provides appropriate tasks can be used.

Step 2: Verify that local is defined after radius or tacas+ in the authentication order as shown in the example below.

aaa authentication login default group tacacs+ local

If the Cisco router 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:

RP/0/0/CPU0:R3(config)#username xxxxxxxxx group netadmin

RP/0/0/CPU0:R3(config)#username xxxxxxxxx secret xxxxxx

Step 2: Configure the authentication order to use the local account if the authentication server is not reachable as shown in the following example:

RP/0/0/CPU0:R3(config)#aaa authentication login default group tacacs+ local

Additional Information:

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

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

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

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

1.10 CISC-ND-000530 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216531
RULE ID: SV-216531r960993
```

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.

Techniques used to address this include protocols using nonces (e.g., numbers generated for a specific one-time use) or challenges (e.g., TLS, WS_Security). Additional techniques include time-synchronous or challenge-response one-time authenticators.

Audit:

Review the router configuration to verify that SSH version 2 is configured as shown in the example below.

ssh server v2

Note: IOS XR supports SSHv1 and SSHv2. SSHv1 uses Rivest, Shamir, and Adelman (RSA) keys while SSHv2 uses Digital Signature Algorithm (DSA) keys.

If the router is not configured to implement replay-resistant authentication mechanisms for network access to privileged accounts, this is a finding.

Remediation:

Configure the router to use SSH version 2 as shown in the example below.

RP/0/0/CPU0:R3(config)#ssh server v2

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)

1.11 CISC-ND-000720 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-216532
RULE ID: SV-216532r961068
```

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 router 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 0

!

line default

…

…

…

exec-timeout 5 0

transport input ssh

If the Cisco router 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.

RP/0/0/CPU0:R3(config)#line con

RP/0/0/CPU0:R3(config-line)#exec-timeout

RP/0/0/CPU0:R3(config)#line default

RP/0/0/CPU0:R3(config-line)#exec-timeout 5 0

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

1.12 CISC-ND-000980 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216533
RULE ID: SV-216533r961392
```

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 router is configured with a logging buffer size as well as on the hard drive. The configuration should look like the example below:

logging archive

device harddisk

severity notifications

file-size 10

archive-size 100

…

…

…

logging buffered 8888888

If a logging buffer size and the archive size is not configured, this is a finding.

If the Cisco router 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 logging buffer size as well as the active log file size and the amount of storage to be reserved for archive log files as shown in the example below.

RP/0/0/CPU0:R3(config)#logging buffered 8888888

RP/0/0/CPU0:R3(config)#logging archive

RP/0/0/CPU0:R3(config-logging-arch)#severity notifications

RP/0/0/CPU0:R3(config-logging-arch)#device harddisk

RP/0/0/CPU0:R3(config-logging-arch)#archive-size 100

RP/0/0/CPU0:R3(config-logging-arch)#file-size 10

RP/0/0/CPU0:R3(config-logging-arch)#end

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

1.13 CISC-ND-001000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216534
RULE ID: SV-216534r991930
```

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

logging 10.1.12.7 vrf default severity critical

Note: The parameter "critical" can be replaced with a lesser severity level (i.e., error, warning, notice, informational).

If the Cisco router is not configured to generate an alert for all audit failure events, this is a finding.

Remediation:

Configure the Cisco router to send critical to emergency log messages to the syslog server as shown in the example below.

RP/0/0/CPU0:R3(config)#logging 10.1.12.7 severity critical

Note: The parameter "critical" can replaced with a lesser severity level (i.e., error, warning, notice, informational).

Additional Information:

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

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

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

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

1.14 CISC-ND-001030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216535
RULE ID: SV-216535r1015296
```

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

ntp server x.x.x.x

ntp server y.y.y.y

If the Cisco router is not configured to synchronize its clock with redundant authoritative time sources, this is a finding.

Remediation:

Configure the Cisco router to synchronize its clock with redundant authoritative time sources as shown in the example below.

RP/0/0/CPU0:R3 (config)#ntp server x.x.x.x

RP/0/0/CPU0:R3 (config)#ntp server y.y.y.y

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)

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

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

1.15 CISC-ND-001050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco router 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-216537
RULE ID: SV-216537r961443
```

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 UTC, a modern continuation of GMT, or local time with an offset from UTC.

Audit:

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

hostname R3

clock timezone EST -5

service timestamps log datetime localtime

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 router is not configured to record time stamps for audit records that can be mapped to UTC or GMT, this is a finding.

Remediation:

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

RP/0/0/CPU0:R3(config)#clock timezone EST -5

RP/0/0/CPU0:R3(config)#service timestamps log datetime localtime

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

1.16 CISC-ND-001040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco router must record time stamps for audit records that meet a granularity of one second for a minimum degree of precision.

```
GROUP ID: V-216536
RULE ID: SV-216536r961446
```

Rationale:

Without sufficient granularity of time stamps, it is not possible to adequately determine the chronological order of records. Time stamps generated by the application include date and time. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks.

Audit:

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

hostname R3

service timestamps log datetime localtime

If the router is not configured to record time stamps that meet a granularity of one second, this is a finding.

Remediation:

Configure the Cisco router to record time stamps that meet a granularity of one second as shown in the example below.

RP/0/0/CPU0:R3(config)#service timestamps log datetime localtime

Additional Information:

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

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

1.17 CISC-ND-001130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216538
RULE ID: SV-216538r961506
```

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

snmp-server host x.x.x.x traps version 3 auth V3USER

snmp-server user V3USER V3GROUP v3 auth sha

snmp-server view V3READ iso included

snmp-server view V3WRITE iso included

snmp-server group V3GROUP v3 auth read V3READ write V3WRITE

If the Cisco router is not configured to authenticate SNMP messages using a FIPS-validated HMAC, this is a finding.

Remediation:

Configure the Cisco router to authenticate SNMP messages as shown in the example below.

RP/0/0/CPU0:R3(config)#snmp-server group V3GROUP v3 auth read V3READ write V3WRITE

RP/0/0/CPU0:R3(config)#snmp-server user V3USER V3GROUP v3 auth sha xxxxxx

RP/0/0/CPU0:R3(config)#snmp-server view V3READ iso included

RP/0/0/CPU0:R3(config)#snmp-server view V3WRITE iso included

RP/0/0/CPU0:R3(config)#snmp-server host x.x.x.x version 3 auth V3USER

Additional Information:

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

1.18 CISC-ND-001140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216539
RULE ID: SV-216539r961506
```

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

snmp-server host x.x.x.x traps version 3 auth V3USER

snmp-server user V3USER V3GROUP v3 auth sha encrypted 110B1607150B

snmp-server view V3READ iso included

snmp-server view V3WRITE iso included

snmp-server group V3GROUP v3 auth read V3READ write V3WRITE

If the Cisco router is not configured to encrypt SNMP messages using a FIPS 140-2 approved algorithm, this is a finding.

Remediation:

Configure the Cisco router to encrypt SNMP messages using a FIPS 140-2 approved algorithm as shown in the example below.

RP/0/0/CPU0:R3(config)#snmp-server group V3GROUP v3 auth read V3READ write V3WRITE

RP/0/0/CPU0:R3(config)#snmp-server user V3USER V3GROUP v3 auth sha xxxxxx priv aes 256 xxxxxx

RP/0/0/CPU0:R3(config)#snmp-server view V3READ iso included

RP/0/0/CPU0:R3(config)#snmp-server view V3WRITE iso included

RP/0/0/CPU0:R3(config)#snmp-server host x.x.x.x version 3 auth V3USER

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)

1.19 CISC-ND-001150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco router must be configured to authenticate NTP sources using authentication that is cryptographically based.

```
GROUP ID: V-216540
RULE ID: SV-216540r961506
```

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

ntp

authentication-key 1 md5 encrypted 030654090416

trusted-key 1

server x.x.x.x key 1

server y.y.y.y key 1

If the Cisco router is not configured to authenticate NTP sources using authentication that is cryptographically based, this is a finding.

Remediation:

Configure the Cisco router to authenticate NTP sources using authentication that is cryptographically based as shown in the example below.

RP/0/0/CPU0:R4#ntp authenticate

RP/0/0/CPU0:R4#ntp authentication-key 1 md5 xxxxxx

RP/0/0/CPU0:R4#ntp trusted-key

RP/0/0/CPU0:R4#ntp server x.x.x.x key 1

RP/0/0/CPU0:R4#ntp server y.y.y.y key 1

Additional Information:

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

1.20 CISC-ND-001200 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-216541
RULE ID: SV-216541r961554
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore 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 use d for authentication to cryptographic modules.

Audit:

Review the router configuration to verify that SSH version 2 is configured as shown in the example below.

ssh server v2

Note: IOS XR supports SSHv1 and SSHv2. SSHv1 uses Rivest, Shamir, and Adelman (RSA) keys while SSHv2 uses Digital Signature Algorithm (DSA) keys which is FIPS 186-4.

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 the router to use SSH version 2 as shown in the example below.

RP/0/0/CPU0:R3(config)#ssh server v2

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)

1.21 CISC-ND-001210 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-216542
RULE ID: SV-216542r961557
```

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 router configuration to verify that SSH version 2 is configured as shown in the example below.

ssh server v2

Note: IOS XR supports SSHv1 and SSHv2. The AES encryption algorithm is supported on the SSHv2 server and client, but not on the SSHv1 server and client. Any requests for an AES cipher sent by an SSHv2 client to an SSHv1 server are ignored, with the server using 3DES instead. The cipher preference for the SSH server follows the order AES128, AES192, AES256, and, finally, 3DES. The server rejects any requests by the client for an unsupported cipher, and the SSH session does not proceed.

If the router is configured to implement SSH version 1, this is a finding.

Remediation:

Configure the router to use SSH version 2 as shown in the example below.

RP/0/0/CPU0:R3(config)#ssh server v2

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)

1.22 CISC-ND-001310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216543
RULE ID: SV-216543r961860
```

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

logging 10.1.12.7 vrf default severity info

If the Cisco router 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 router to send log records to a syslog server as shown in the example below.

RP/0/0/CPU0:R3(config)#logging 10.1.12.7 severity info

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)

1.23 CISC-ND-001370 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-216544
RULE ID: SV-216544r961863
```

Rationale:

Centralized management of user accounts and authentication increases the administrative access to the router. 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 router configuration to verify that the device is configured to use at least two authentication servers as primary source for authentication as shown in the following example:

radius-server host 10.1.3.16 auth-port 1645 acct-port 1646

key xxxxxxxxxx

radius-server host 10.1.3.17 auth-port 1645 acct-port 1646

key xxxxxxxxxx…

…

…

aaa authentication login LOGIN_AUTHENTICATION group radius local

line console

login authentication LOGIN_AUTHENTICATION

!

line default

login authentication LOGIN_AUTHENTICATION

transport input ssh

If the Cisco router 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:

Step 1: Configure the router to use at least two authentication servers as shown in the following example:

RP/0/0/CPU0:R3(config)#radius-server host 10.1.3.16 key xxxxxxxx

RP/0/0/CPU0:R3(config)#radius-server host 10.1.3.17 key xxxxxxxx

Step 2: Configure the authentication order to use the authentication servers as primary source for authentication as shown in the following example:

RP/0/0/CPU0:R3(config)#aaa authentication login LOGIN_AUTHENTICATION group radius local

Step 3: Configure all network connections associated with a device management to use the authentication servers for the purpose of login authentication as shown in the following example:

RP/0/0/CPU0:R3(config)#line default

RP/0/0/CPU0:R3(config-line)#login authentication LOGIN_AUTHENTICATION

RP/0/0/CPU0:R3(config-line)#exit

RP/0/0/CPU0:R3(config)#line console

RP/0/0/CPU0:R3(config-line)#login authentication LOGIN_AUTHENTICATION

Additional Information:

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

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

1.24 CISC-ND-001410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco router must be configured to back up the configuration when changes occur.

```
GROUP ID: V-216545
RULE ID: SV-216545r1069525
```

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 router configuration to verify that it is compliant with this requirement. The example configuration below will send the configuration to an SCP server when a configuration change occurs.

configuration commit auto-save filename scp://user1@server1://test-folder/test_123

If the Cisco router is not configured to conduct backups of the configuration when changes occur, this is a finding.

Remediation:

Configure the Cisco router to send the configuration to an SCP server when a configuration change occurs as shown in the example below.

RP/0/0/CPU0:R3(config)#configuration commit auto-save filename scp://user1@server1://test-folder/test_123

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)

1.25 CISC-ND-001440 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-216546
RULE ID: SV-216546r961863
```

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 Certification Authority will suffice.

Audit:

Review the router configuration to determine if a CA trust point has been configured. The CA trust point will contain the URL of the CA in which the router has enrolled with. Verify this is a DoD or DoD-approved CA. This will ensure the router has enrolled and received a certificate from a trusted CA. The CA trust point configuration would look similar to the example below.

crypto pki trustpoint CA_X

enrollment url http://trustpoint1.example.com

Note: A remote end-point's certificate will always be validated by the router by verifying the signature of the CA on the certificate using the CA's public key, which is contained in the router's certificate it received at enrollment.

Note: This requirement is not applicable if the router does not have any public key certificates.

If the Cisco router is not configured to obtain its public key certificates from an appropriate certificate policy through an approved service provider, this is a finding.

Remediation:

Configure the router to obtain its public key certificates from an appropriate certificate policy through an approved service provider as show in the example below.

RP/0/0/CPU0:R3(config)#crypto ca trustpoint CA_X

RP/0/0/CPU0:R3(config-trustp)#enrollment url http://trustpoint1.example.com

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-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

1.26 CISC-ND-001450 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-216547
RULE ID: SV-216547r961863
```

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 router is configured to send logs to at least two syslog servers. The configuration should look similar to the example below:

logging 10.1.3.22 vrf default severity info

logging 10.1.3.23 vrf default severity info

If the router is not configured to send log data to the syslog server, this is a finding.

Remediation:

Configure the router to send log messages to the syslog servers as shown in the example below.

RP/0/0/CPU0:R3(config)#logging 10.1.3.22 severity info

RP/0/0/CPU0:R3(config)#logging 10.1.3.23 severity info

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)

1.27 CISC-ND-001470 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-216549
RULE ID: SV-216549r961863
```

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 router is in compliance with this requirement by having the router 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 router is not running a supported release, this is a finding.

Remediation:

Upgrade the router 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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	CISC-ND-000010 (Manual)	☐	☐
1.2	CISC-ND-000140 (Manual)	☐	☐
1.3	CISC-ND-000150 (Manual)	☐	☐
1.4	CISC-ND-000160 (Manual)	☐	☐
1.5	CISC-ND-000250 (Manual)	☐	☐
1.6	CISC-ND-000280 (Manual)	☐	☐
1.7	CISC-ND-000290 (Manual)	☐	☐
1.8	CISC-ND-000470 (Manual)	☐	☐
1.9	CISC-ND-000490 (Manual)	☐	☐
1.10	CISC-ND-000530 (Manual)	☐	☐
1.11	CISC-ND-000720 (Manual)	☐	☐
1.12	CISC-ND-000980 (Manual)	☐	☐
1.13	CISC-ND-001000 (Manual)	☐	☐
1.14	CISC-ND-001030 (Manual)	☐	☐
1.15	CISC-ND-001050 (Manual)	☐	☐
1.16	CISC-ND-001040 (Manual)	☐	☐
1.17	CISC-ND-001130 (Manual)	☐	☐
1.18	CISC-ND-001140 (Manual)	☐	☐
1.19	CISC-ND-001150 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	CISC-ND-001200 (Manual)	☐	☐
1.21	CISC-ND-001210 (Manual)	☐	☐
1.22	CISC-ND-001310 (Manual)	☐	☐
1.23	CISC-ND-001370 (Manual)	☐	☐
1.24	CISC-ND-001410 (Manual)	☐	☐
1.25	CISC-ND-001440 (Manual)	☐	☐
1.26	CISC-ND-001450 (Manual)	☐	☐
1.27	CISC-ND-001470 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 3, 2025	1.0.0	Initial CIS Release