CIS Cisco IOS XR 7.x

v1.0.0 - 10-23-2023

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/

Table of Contents

Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document, Security Configuration Benchmark for Cisco IOS XR, provides prescriptive guidance for establishing a secure configuration posture for Cisco Routers running Cisco IOS XR. This guide was developed and tested against Cisco IOS XR version 7.3. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at benchmarkinfo@cisecurity.org.

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 on a Cisco routing and switching platforms.

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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 for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

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

Impact Statement

Any security, functionality, or operational consequences that can result from following 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.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) '4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

   Items in this profile intend to:

   - map to CIS Controls implementation group 1;
   - be practical and prudent;
   - provide a clear security benefit; and
   - not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

   This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

   - map to CIS Controls implementation group 2 or 3;
   - are intended for environments or use cases where security is paramount.
   - acts as defense in depth measure.
   - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Recommendations

1 Management Plane

1.1 Authentication, Authorization and Accounting (AAA) Rules

Rules in the authentication, authorization and accounting (AAA) configuration class enforce device access control, provide a mechanism for tracking configuration changes, and enforcing security policy.

1.1.1 AAA prerequisites

This sub-section contains prerequsites for effective AAA implementation.

1.1.1.1 TACACS+ (Automated)

Profile Applicability:

- Level 2

Description:

Cisco IOS XR devices can use the TACACS+ protocol to communicate with a central AAA server. Using a central authentication store ensures that all administrative actions are tied to named users, making the tracking of changes much easier. It also makes tracking compromised accounts and malicious activities much easier.

Rationale:

Central authentication is key as it minimizes the effort in managing named user accounts. Keeping local admin accounts opens the door to all the issues inherent in shared accounts, namely:

- Errors in implementation being done by generic admin accounts, which can then be denied by all.
- Shared credentials staying unchanged when administrative staff leave the organization or change roles.
- Giving malicious actors the ability to recover shared credentials from saved device backups

Impact:

Implementing TACACS+ (or any central authentication solution) ensures that only named users are allowed to gain an administrative session to the device. This allows:

- Tracking of all changes to named users
- Simplification of reconciling changes to a change management process
- Off-loading password change cycles and password complexity requirements to that central authentication store
- Simplification of removing admin access as administrators leave the organization or change their roles in the organization

Audit:

"show run aaa" shows all hierarchic configuration on a single line with the hierarchy prepended.
Two or more TACACS servers must be defined, and they must be referenced by a aaa group:

```
IOSXR#sh run aaa
!
tacacs-server host 1.1.1.1 port 49
 key 7 070C285F4D06
!
tacacs-server host 1.1.1.2 port 49
 key 7 00071A150754
!
aaa group server tacacs+ TAC
 server 1.1.1.1
 server 1.1.1.2
```

Remediation:

For complete instructions how to configure AAA please refer to the configuration guide.
Below you can find some minimum config snippets to implement a radius or tacacs+
server group.

```
IOSXR(config)#tacacs-server host {tacacs_ip_address} port 49
IOSXR(config-tacacs-host)#key {tacacs_key}

IOSXR(config)#aaa group server tacacs+ {tacacs_group_name}
IOSXR(config-sg-tacacs)#server {tacacs_ip_address}
```

Default Value:

By default no aaa groups are implemented.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-
   5/system-security/configuration/guide/b-system-security-cg-asr9000-
   75x/configuring-aaa-services.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.5 Centralize Network Authentication, Authorization, and Auditing (AAA) Centralize network AAA.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

1.1.1.2 RADIUS (Automated)

Profile Applicability:

- Level 2

Description:

Cisco IOS XR devices can use the RADIUS protocol to communicate with a central AAA server. Using a central authentication store ensures that all administrative actions are tied to named users, making the tracking of changes much easier. It also makes tracking compromised accounts and malicious activities much easier.

Rationale:

Central authentication is key as it minimizes the effort in managing named user accounts. Keeping local admin accounts opens the door to all the issues inherent in shared accounts, namely:

- Errors in implementation being done by generic admin accounts, which can then be denied by all.
- Shared credentials staying unchanged when administrative staff leave the organization or change roles.
- Giving malicious actors the ability to recover shared credentials from saved device backups

Impact:

Implementing RADIUS (or any central authentication solution) ensures that only named users are allowed to gain an administrative session to the device. This allows:

- Tracking of all changes to named users
- Simplification of reconciling changes to a change management process
- Off-loading password change cycles and password complexity requirements to that central authentication store
- Simplification of removing admin access as administrators leave the organization or change their roles in the organization

Audit:

"show run aaa" shows all hierarchic configuration on a single line with the hierarchy prepended.
Two or more RADIUS servers must be defined, and they must be referenced by a aaa group:

```
IOSXR#sh run aaa
!
radius-server host 2.2.2.2 auth-port 1645 acct-port 1646
 key 7 1511021F0725
!
radius-server host 2.2.2.3 auth-port 1645 acct-port 1646
 key 7 13061E010803
!
aaa group server radius RAD
 server 2.2.2.2 auth-port 1645 acct-port 1646
 server 2.2.2.3 auth-port 1645 acct-port 1646
```

Remediation:

For complete instructions how to configure AAA please refer to the configuration guide.
Below you can find some minimum config snippets to implement a radius or tacacs+
server group.

```
radius-server host {radius_ip_address}
 key {radius_key}

aaa group server radius {radius_group_name}
 server radius_ip_address}
```

Default Value:

By default no aaa groups are implemented.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-
   5/system-security/configuration/guide/b-system-security-cg-asr9000-
   75x/configuring-aaa-services.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.5 Centralize Network Authentication, Authorization, and Auditing (AAA) Centralize network AAA.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

1.1.2 Authentication

Authentication is the most important security process by which a principal (a user or an application) obtains access to the system. The principal is identified by a username (or user ID) that is unique across an administrative domain. The applications serving the user (such as EXEC or Management Agent) procure the username and the credentials from the user. AAA performs the authentication based on the username and credentials passed to it by the applications. The role of an authenticated user is determined by the group (or groups) to which the user belongs. (A user can be a member of one or more user groups.)

1.1.2.1 console authentication (Automated)

Profile Applicability:

- Level 1

Description:

Authenticate management access to the network devices. Typically a central authentication store combined with a fallback mechanism should be implemented to allow emergency access, in case the central authentication servers are not available.

Rationale:

Management access to network devices must be authenticated. The default under AAA (local or network) is to require users to log in using a valid user name and password. This rule applies for both local and network AAA. Fallback mode should also be enabled to allow emergency access to the router or switch in the event that the AAA server was unreachable.

Impact:

If no authentication is implemented, any user with network reachability to the management interface can access network devices and change their configuration.

Audit:

The console doesn't have any line pool. The console is configured directly:

```
IOSXR#show run formal | i "login authentication"
line console login authentication default
```

Verify an authentication list is defined and optionally references the aaa group that was created in the prerequisites:

```
IOSXR#show run formal | i "aaa authentication login"
aaa authentication login default group {tacacs_group|radius_group} local
```

If a group is referenced above in the authentication list, verify that group is defined:

```
IOSXR#r#show run formal | i "aaa group server"
aaa group server tacacs+ {tacacs_group|radius_group}
```

Remediation:

Configure an authentication list that references the AAA group that was created in the prerequisites. AAA lists are prioritized list of databases. If the system is unable to use a database, it automatically rolls over to the next database on the list. If the authentication, authorization, or accounting request is rejected by any database, the rollover does not occur and the request is rejected.
It is common to include "local" as the last entry in the list, to allow access to manage the device even if all servers from the AAA group are unavailable. Note that it also means that if an attacker can DoS the AAA Servers, they can start to try authenticate locally as well. Hence, always ensure to use strong passwords for local users.

```
IOSXR(config)#aaa authentication login default group
{tacacs_group|radius_group} local
```

Above configuration authenticates first against a central aaa group and uses local user accounts as fallback.
Ensure the above list is referenced under the line templates:

```
IOSXR(config)#line console login authentication default
```

Ensure the vty pool references the above line template:

```
IOSXR(config)#vty-pool default 0 4 line-template default
```

Default Value:

By default IOS XR authenticates against the local user database. However, there is no way to show the default configuration. We follow the principle "explicit is better than implicit" and recommend to configure the authentication explicitly.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/system-security/configuration/guide/b-system-security-cg-asr9000-75x/configuring-aaa-services.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	**12.5 <u>Centralize Network Authentication, Authorization, and Auditing (AAA)</u>** Centralize network AAA.		🟠	🔵
v7	**16.2 <u>Configure Centralized Point of Authentication</u>** Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		🟠	🔵

1.1.2.2 vty line authentication (Automated)

Profile Applicability:

- Level 1

Description:

Authenticate management access to the network devices. Typically a central authentication store combined with a fallback mechanism should be implemented to allow emergency access, in case the central authentication servers are not available.

Rationale:

Management access to network devices must be authenticated. The default under AAA (local or network) is to require users to log in using a valid user name and password. This rule applies for both local and network AAA. Fallback mode should also be enabled to allow emergency access to the router or switch in the event that the AAA server was unreachable.

Impact:

If no authentication is implemented, any user with network reachability to the management interface can access network devices and change their configuration.

Audit:

Check which line templates are referenced by the vty pool:

```
IOSXR#show run formal | i "vty-pool"
vty-pool default 0 4 line-template default
```

Ensure the above list is referenced under the line templates:

```
IOSXR#show run formal | i "login authentication"
line console login authentication default
line default login authentication default
```

Verify an authentication list is defined and optionally references the aaa group that was created in the prerequisites:

```
IOSXR#show run formal | i "aaa authentication login"
aaa authentication login default group {tacacs_group|radius_group} local
```

Remediation:

Configure an authentication list that references the AAA group that was created in the prerequisites. AAA lists are prioritized list of databases. If the system is unable to use a database, it automatically rolls over to the next database on the list. If the authentication, authorization, or accounting request is rejected by any database, the rollover does not occur and the request is rejected.
It is common to include "local" as the last entry in the list, to allow access to manage the device even if all servers from the AAA group are unavailable. Note that it also means that if an attacker can DoS the AAA Servers, they can start to try authenticate locally as well. Hence, always ensure to use strong passwords for local users.

```
IOSXR(config)#aaa authentication login default group
{tacacs_group|radius_group} local
```

Above configuration authenticates first against a central aaa group and uses local user accounts as fallback.
Ensure the above list is referenced under the line templates:

```
IOSXR(config)#line console login authentication default
IOSXR(config)#line default login authentication default
```

Ensure the vty pool references the above line template:

```
IOSXR(config)#vty-pool default 0 4 line-template default
```

Default Value:

By default IOS XR authenticates against the local user database. However, there is no way to show the default configuration. We follow the principle "explicit is better than implicit" and recommend to configure the authentication explicitly.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/system-security/configuration/guide/b-system-security-cg-asr9000-75x/configuring-aaa-services.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.5 <u>Centralize Network Authentication, Authorization, and Auditing (AAA)</u> Centralize network AAA.		●	●
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

1.1.3 Authorization

Authentication is the most important security process by which a principal (a user or an application) obtains access to the system. The principal is identified by a username (or user ID) that is unique across an administrative domain. The applications serving the user (such as EXEC or Management Agent) procure the username and the credentials from the user. AAA performs the authentication based on the username and credentials passed to it by the applications. The role of an authenticated user is determined by the group (or groups) to which the user belongs. (A user can be a member of one or more user groups.)

1.1.3.1 Configure Authorization (Manual)

Profile Applicability:

- Level 2

Description:

Command authorization allows restricting specific users to specific command sets that they can use on the device. Command authorization is a complex endeavor and is very rarely implemented. Usually, the TACACS+ protocol is used with a central AAA server.

Rationale:

Command authorization allows the implementation of fine-grained role-based access control concepts.

Impact:

Prevent users from issuing certain commands.

Audit:

Check which line template is referenced by the vty-pools

```
IOSXR#show run formal | i "vty-pool"
vty-pool default 0 4 line-template default
```

Check the relationship between line template in use and the aaa list:

```
IOSXR##show run formal | i "authorization"
line console authorization commands default
line default authorization commands default
```

Verify an authentication list is defined and optionally references the aaa group that was created in the prerequisites:

```
IOSXR#show run formal | i "aaa authorization"
aaa authorization commands default group {tacacs_group} none
```

Remediation:

Currently CIS makes no recommendations how to implement command authorization. Roles and access-privileges should be defined in collaboration with your operations and security teams.

Default Value:

By default command authorization is not enabled.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/system-security/configuration/guide/b-system-security-cg-asr9000-75x/configuring-aaa-services.html

Additional Information:

Commands authorization—Applies to the EXEC mode mode commands a user issues. Command authorization attempts authorization for all EXEC mode mode commands. Note

"Command" authorization is distinct from "task-based" authorization, which is based on the task profile established during authentication.

EXEC mode authorization—Applies authorization for starting EXEC mode session. So either a user is allowed to start an "exec" session (usually this is equivalent to opening a vty line) or not.

The Cisco IOS XR software supports the following methods for authorization:

- none : The router does not request authorization information; authorization is not performed over this line or interface.
- local : Uses local database for authorization; Authorizes any command if user is authenticated locally.
- group [radius|tacacs+] : use all configured radius or tacacs servers

1.1.4 Accounting

The AAA accounting feature allows the services that users are accessing and the amount of network resources that users are consuming to be tracked. When AAA accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method is implemented) in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, and auditing.

1.1.4.1 exec accounting (Automated)

Profile Applicability:

- Level 1

Description:

The router reports user activity to the TACACS+ or RADIUS security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Rationale:

Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control, the services that may be accessed once authenticated and accountability by tracking services accessed. Additionally, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices. AAA Accounting provides a management and audit trail for user and administrative sessions through TACACS+.

Impact:

Enabling 'aaa accounting exec' records each new exec session on the router and sends it to the accounting servers and enables organizations to monitor and analyze the activity.

Command accounting is not supported for commands that are executed using Netconf, XML or GRPC.

Audit:

Make sure an accounting list is defined and that same list (called 'default' in the example below) is referenced by the line templates.

```
IOSXR#show run aaa
aaa accounting exec default start-stop group {tacacs_group|radius_group}
line console accounting exec default
line default accounting exec default
```

If not the 'line default' template is used, make sure the correct line template is associated with the vty-pool.

Remediation:

Configure an accounting list which for example includes the tacacs+ or radius server group, which was defined in the prerequisites or local or both:

```
IOSXR(config)#aaa accounting exec default start-stop group
{tacacs_group|radius_group}
IOSXR(config)#line console accounting exec default
IOSXR(config)#line default accounting exec default
```

Note: exec accounting doesn't support the "local" / syslog target.

Default Value:

No accounting is configured.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/system-security/configuration/guide/b-system-security-cg-asr9000-75x/configuring-aaa-services.html

Additional Information:

For minimal accounting, include the stop-only keyword to send a "stop accounting" notice at the end of the requested user process. For more accounting, you can include the start-stop keyword, so that the external AAA server sends a "start accounting" notice at the beginning of the requested process and a "stop accounting" notice at the end of the process.

Command accounting with a method as local, enables the logging of commands executed by all users as syslog messages. This feature can be enabled or disabled only by users who have AAA write permissions. Once enabled, all the commands that are executed by all users can be viewed from the output of the show logging command.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	12.5 Centralize Network Authentication, Authorization, and Auditing (AAA) Centralize network AAA.		●	●

1.1.4.2 command accounting (Automated)

Profile Applicability:

- Level 1

Description:

The router reports user activity to the TACACS+ or RADIUS security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Rationale:

Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control, the services that may be accessed once authenticated and accountability by tracking services accessed. Additionally, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices. AAA Accounting provides a management and audit trail for user and administrative sessions through TACACS+.

Impact:

Enabling 'aaa accounting commands' records and sends any user entered command to the accounting servers and enables organizations to monitor and analyze the activity.

Command accounting is not supported for commands that are executed using Netconf, XML or GRPC.

Audit:

Make sure an accounting list is defined and that same list (called 'default' in the example below) is referenced by the line templates.

```
IOSXR#show run aaa
aaa accounting commands default start-stop local none
line console accounting commands default
line default accounting commands default
```

If not the 'line default' template is used, make sure the correct line template is associated with the vty-pool.

Remediation:

Configure an accounting list which for example includes the tacacs+ or radius server group, which was defined in the prerequisites or local or both:

```
IOSXR(config)#aaa accounting commands default start-stop group
{tacacs_group|radius_group} local
IOSXR(config)#line console accounting commands default
IOSXR(config)#line default accounting commands default
```

Default Value:

No accounting is configured.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/system-security/configuration/guide/b-system-security-cg-asr9000-75x/configuring-aaa-services.html

Additional Information:

For minimal accounting, include the stop-only keyword to send a "stop accounting" notice at the end of the requested user process. For more accounting, you can include the start-stop keyword, so that the external AAA server sends a "start accounting" notice at the beginning of the requested process and a "stop accounting" notice at the end of the process.

Command accounting with a method as local, enables the logging of commands executed by all users as syslog messages. This feature can be enabled or disabled only by users who have AAA write permissions. Once enabled, all the commands that are executed by all users can be viewed from the output of the show logging command.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	12.5 Centralize Network Authentication, Authorization, and Auditing (AAA) Centralize network AAA.		●	●

1.1.4.3 network accounting (Automated)

Profile Applicability:

- Level 1

Description:

The router reports user activity to the TACACS+ or RADIUS security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Rationale:

Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control, the services that may be accessed once authenticated and accountability by tracking services accessed. Additionally, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices. AAA Accounting provides a management and audit trail for user and administrative sessions through TACACS+.

Impact:

Enabling 'aaa accounting network' records all network-related service requests, such as Internet Key Exchange (IKE) and Point-to-Point Protocol (PPP) to the accounting servers and enables organizations to monitor and analyze the activity.

Audit:

Verify the network accounting

```
IOSXR#show run aaa
aaa accounting network default start-stop group {tacacs_group|radius_group}
```

Remediation:

Configure an accounting list which includes the tacacs+ or radius server group, that was defined in the prerequisites or local or both:

```
aaa accounting network default start-stop group {tacacs_group|radius_group}
```

Default Value:

No accounting is configured.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/system-security/configuration/guide/b-system-security-cg-asr9000-75x/configuring-aaa-services.html
2. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/security/command/reference/b-system-security-cr-asr9k/b-system-security-cr-71x-asr9k_chapter_01.html#wp1912054943

Additional Information:

For minimal accounting, include the stop-only keyword to send a "stop accounting" notice at the end of the requested user process. For more accounting, you can include the start-stop keyword, so that the external AAA server sends a "start accounting" notice at the beginning of the requested process and a "stop accounting" notice at the end of the process.

Command accounting with a method as local, enables the logging of commands executed by all users as syslog messages. This feature can be enabled or disabled only by users who have AAA write permissions. Once enabled, all the commands that are executed by all users can be viewed from the output of the show logging command.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	12.5 Centralize Network Authentication, Authorization, and Auditing (AAA) Centralize network AAA.		●	●

1.1.4.4 system accounting (Automated)

Profile Applicability:

- Level 1

Description:

The router reports user activity to the TACACS+ or RADIUS security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Rationale:

Authentication, authorization and accounting (AAA) systems provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control, the services that may be accessed once authenticated and accountability by tracking services accessed. Additionally, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices. AAA Accounting provides a management and audit trail for user and administrative sessions through TACACS+.

Impact:

Enabling 'aaa accounting system' records all system-related events to the accounting servers and enables organizations to monitor and analyze the activity.

Audit:

Verify the system accounting:

```
IOSXR#show run aaa
aaa accounting system default start-stop group {tacacs_group|radius_group}
```

Remediation:

Configure an accounting list which includes the tacacs+ or radius server group, that was defined in the prerequisites or local or both:

```
aaa accounting system default start-stop group {tacacs_group|radius_group}
```

Default Value:

No accounting is configured.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/system-security/configuration/guide/b-system-security-cg-asr9000-75x/configuring-aaa-services.html

2.

Additional Information:

For minimal accounting, include the stop-only keyword to send a "stop accounting" notice at the end of the requested user process. For more accounting, you can include the start-stop keyword, so that the external AAA server sends a "start accounting" notice at the beginning of the requested process and a "stop accounting" notice at the end of the process.

Command accounting with a method as local, enables the logging of commands executed by all users as syslog messages. This feature can be enabled or disabled only by users who have AAA write permissions. Once enabled, all the commands that are executed by all users can be viewed from the output of the show logging command.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	12.5 Centralize Network Authentication, Authorization, and Auditing (AAA) Centralize network AAA.		●	●

1.1.5 Local users, groups and tasks (Automated)

Profile Applicability:

- Level 2

Description:

To provide controlled access to the XR and System Admin configurations on the router, user profiles are created with assigned privileges. The privileges are specified using command rules and data rules. The authentication, authorization, and accounting (aaa) commands are used for the creation of users, groups, command rules, and data rules. The aaa commands are also used for changing the disaster-recovery password.

Rationale:

IOS-XR has a very strong embedded mechanism to do user authentication and authorization. While XR does not have the concept of privilege-levels as what IOS had, the embedded user task group management is extremely strong allow for the creation of different task groups.

Impact:

Default task-groups

The following task-groups are predefined in IOS-XR

root-system: Root system users

root-lr: Root logical router users

netadmin: Network administrators

sysadmin: System administrators

operator: Operators performing day-to-day activities

cisco-support: highest level of privilege allowing lowest level access

Audit:

"show run aaa" shows all hierarchic configuration on a single line with the hierarchy prepended.

```
IOSXR#sh run aaa

taskgroup TASKGROUP
 task read bgp
!
usergroup XRGROUP
 taskgroup TASKGROUP
!
username cisco
 group root-lr
 group cisco-support
 secret 10
$6$O51Wr/lUsR6S5r/.$.qUOapiguyRPwNwix3FVwc9APW3WvrhZv84z0F7cM0zxcyCiXwQ45YuX/
p/jDXb4cS7bTxemvGK73giBtJHoj.
!
username USER1
 group XRGROUP
 secret 10
$6$cTTjN1rrPqxaBN1.$jq8GqQ.hSwZXb72YxgTCPgm3kZ2MT51FAlXcJDN54l/vY9TNa8Nob6cyY
tT4vT4Y9wjtH9R7aK3KmUgwjR5pz0
!
```

Remediation:

The commands below will enable authorizarion for a user.

```
IOSXR(config)#taskgroup {task_group} task read {task}
IOSXR(config)#usergroup {user_group} taskgroup {task_group}
IOSXR(config)#username {username}
IOSXR(config-un)#secret {password}
IOSXR(config-un)#group {user_group}
```

Default Value:

By default no aaa groups are implemented.

References:

1. https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5000/system-setup/62x/b-system-setup-cg-ncs5000-62x/b-system-setup-cg-ncs5000-62x_chapter_0101.html#id_134674
2. https://community.cisco.com/t5/service-providers-knowledge-base/asr9000-xr-using-task-groups-and-understanding-priv-levels-and/ta-p/3109596

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.5 Centralize Network Authentication, Authorization, and Auditing (AAA) Centralize network AAA.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	**16.2** <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

1.2 SSH

Secure Shell (SSH) is an application and a protocol that provides a secure replacement to the Berkeley r-tools. The protocol secures sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools.

Two versions of the SSH server are available: SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2). SSHv1 uses Rivest, Shamir, and Adelman (RSA) keys and SSHv2 uses either Digital Signature Algorithm (DSA) keys or Rivest, Shamir, and Adelman (RSA) keys. Cisco IOS XR software supports both SSHv1 and SSHv2.

1.2.1 Set the 'hostname' (Automated)

Profile Applicability:

- Level 1

Description:

The hostname is used in prompts and default configuration filenames.

Rationale:

The domain name is prerequisite for setting up SSH.

Impact:

Organizations should plan the enterprise network and identify an appropriate host name for each router.

Audit:

Perform the following to determine if the local time zone is configured:
Verify the result shows the summer-time recurrence is configured properly.

```
IOSXR#sh run | incl hostname
```

Remediation:

Configure an appropriate host name for the router.

```
IOSXR(config)#hostname {hostname}
```

Default Value:

The default hostname is Router.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r6-1/security/configuration/guide/b-syssec-cg-crs-61x.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.5 <u>Use Multifactor Authentication For All Administrative Access</u> Use multi-factor authentication and encrypted channels for all administrative account access.		🟠	🔵

1.2.2 Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa' (Automated)

Profile Applicability:

- Level 1

Description:

Use this command to generate RSA key pairs for your Cisco device.

RSA keys are generated in pairs--one public RSA key and one private RSA key.

Rationale:

An RSA key pair is a prerequisite for setting up SSH and should be at least 2048 bits.

NOTE: IOS does NOT display the modulus bit value in the Audit Procedure.

Impact:

Organizations should plan and implement enterprise network cryptography and generate an appropriate RSA key pairs, such as 'modulus', greater than or equal to 2048.

Audit:

Perform the following to determine if the RSA key pair is configured:

```
IOSXR#sh crypto key mypubkey rsa
Wed Jul 19 18:09:46.009 UTC
Key label: the_default
Type     : RSA General purpose
Size     : 2048
Created  : 16:25:09 UTC Wed Jul 19 2023
```

Remediation:

Generate an RSA key pair for the router.

```
IOSXR#crypto key generate rsa general-keys
Wed Jul 19 18:10:51.633 UTC
The name for the keys will be: the_default
% You already have keys defined for the_default
Do you really want to replace them? [yes/no]: yes

Choose the size of the key modulus in the range of 512 to 4096 for your
General Purpose Keypair. Choosing a key modulus greater than 512 may take a
few minutes.

How many bits in the modulus [2048]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]
```

Default Value:

RSA key pairs do not exist.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r6-1/security/configuration/guide/b-syssec-cg-crs-61x.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

1.2.3 Set 'seconds' for 'ssh timeout' for 60 seconds or less (Automated)

Profile Applicability:

- Level 1

Description:

The time interval that the router waits for the SSH client to respond before disconnecting an uncompleted login attempt.

Rationale:

This reduces the risk of an administrator leaving an authenticated session logged in for an extended period of time.

Impact:

Organizations should implement a security policy requiring minimum timeout settings for all network administrators and enforce the policy through the 'ip ssh timeout' command.

Audit:

Perform the following to determine if the SSH timeout is configured:
Verify the timeout is configured properly.

```
IOSXR#sh running-config ssh timeout
Wed Jul 19 18:13:59.732 UTC
ssh timeout 53
```

Remediation:

Configure the SSH timeout

```
IOSXR(config)#ssh timeout {ssh_timeout}
```

Default Value:

SSH in not enabled by default. When SSH is enabled and no value is configured, the default value of 30 seconds is used. The range is from 5 to 120.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r6-1/security/configuration/guide/b-syssec-cg-crs-61x.html

Additional Information:

This cannot exceed 120 seconds.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**6.5 Require MFA for Administrative Access** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	**4.5 Use Multifactor Authentication For All Administrative Access** Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

1.3 Global Service Rules

Rules in the global service class enforce server and service controls that protect against attacks or expose the device to exploitation.

1.3.1 Disable CDP (Automated)

Profile Applicability:

- Level 1

Description:

Disable Cisco Discovery Protocol (CDP) service at device level.

Rationale:

The Cisco Discovery Protocol is a proprietary protocol that Cisco devices use to identify each other on a LAN segment. It is useful only in network monitoring and troubleshooting situations but is considered a security risk because of the amount of information provided from queries. In addition, there have been published denial-of-service (DoS) attacks that use CDP. CDP should be completely disabled unless necessary.

Impact:

To reduce the risk of unauthorized access, organizations should implement a security policy restricting network protocols and explicitly require disabling all insecure or unnecessary protocols.

Audit:

Perform the following to determine if CDP is enabled:
Verify the result shows "CDP is not enabled"

```
IOSXR#show cdp
```

Remediation:

Disable Cisco Discovery Protocol (CDP) service globally.

```
IOSXR(config)#no cdp
```

Default Value:

Enabled on all platforms except the Cisco 10000 Series Edge Services Router

References:

1. https://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/system_management/command/reference/yr37cdp.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.3.2 Disable TCP and UDP small servers (Automated)

Profile Applicability:

- Level 1

Description:

TCP and UDP small servers are servers (daemons, in Unix parlance) that run in the router which are useful for diagnostics.

Rationale:

TCP Small Servers The TCP small servers are:

Echo: Echoes back whatever you type through the telnet x.x.x.x echo command.

Chargen: Generates a stream of ASCII data. Use the telnet x.x.x.x chargen command.

Discard: Throws away whatever you type. Use the telnet x.x.x.x discard command.

Daytime: Returns system date and time, if it is correct. It is correct if you run Network Time Protocol (NTP), or have set the date and time manually from the exec level. Use the telnet x.x.x.x daytime command.

Replace x.x.x.x with the IP address of your router. Most routers inside Cisco run the small servers.

UDP Small Servers The UDP small servers are:

Echo: Echoes the payload of the datagram you send.

Discard: Silently pitches the datagram you send.

Chargen: Pitches the datagram you send, and responds with a 72-character string of ASCII characters terminated with a CR+LF.

Notes:

Almost all Unix boxes support the small servers listed above.

The router also offers finger service and async line bootp service, which you can independently turn off with the configuration global commands no service finger and no ip bootp server, respectively.

Impact:

TBC

Audit:

Perform the following to determine if the feature is enabled:
Verify a command string result returns

```
IOSXR#show run | incl small

service ipv4 tcp-small-servers max-servers 10
service ipv4 udp-small-servers max-servers 10
```

Remediation:

Disable TCp and UDP small services

```
IOSXR(config)#no service ipv4 tcp-small-servers max-servers 10
IOSXR(config)#no service ipv4 udp-small-servers max-servers 10
IOSXR(config)#commit
```

Default Value:

Disabled by default.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r4-3/addr_serv/command/reference/b_ipaddr_cr43xr12k/b_ipaddr_cr42xr12k_chapter_01010.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.4 Implement and Manage a Firewall on Servers** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	**4.5 Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.4 Logging Rules

Rules in the logging class enforce controls that provide a record of system activity and events.

1.4.1 Enable logging (Automated)

Profile Applicability:

- Level 1

Description:

Enable logging of system messages.

Rationale:

Logging provides a chronological record of activities on the Cisco device and allows monitoring of both operational and security related events.

Impact:

TBC

Audit:

Perform the following to determine if the feature is enabled:
Verify no result returns

```
IOSXR#sh logging
Wed Jul 19 18:27:39.571 UTC
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level warnings, 121 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level alert, 0 messages logged
    Logging to 1.1.1.1, 0 message lines logged
    Buffer logging: level debugging, 909 messages logged
```

Remediation:

Enable system logging.

```
IOSXR(config)#logging trap {severity_level}
```

Default Value:

Logging is not enabled/

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-4/system-monitoring/configuration/guide/b-system-monitoring-cg-asr9000-64x/b-system-monitoring-cg-asr9000-64x_chapter_0101.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 <u>Collect Detailed Audit Logs</u>** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	**6.3 <u>Enable Detailed Logging</u>** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

1.4.2 Set 'buffer size' (Automated)

Profile Applicability:

- Level 1

Description:

Enable system message logging to a local buffer.

Rationale:

The device can copy and store log messages to an internal memory buffer. The buffered data is available only from a router exec or enabled exec session. This form of logging is useful for debugging and monitoring when logged in to a router.

Impact:

Data forensics is effective for managing technology risks and an organization can enforce such policies by enabling the 'logging buffered' command.

Audit:

Perform the following to determine if the feature is enabled:
Verify a command string result returns

```
IOSXR#sh logging
Wed Jul 19 18:30:49.736 UTC
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level warnings, 123 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level alert, 0 messages logged
    Logging to 1.1.1.1, 0 message lines logged
    Buffer logging: level debugging, 916 messages logged

IOSXR#sh run logging
Wed Jul 19 18:32:35.155 UTC
logging trap alerts
logging buffered 123123123
logging 1.1.1.1 vrf default severity alerts
```

Remediation:

Configure buffered logging (with minimum size). Recommended size is 64000.

```
IOSXR(config)#logging buffered {logging_buffer_size}
```

Default Value:

No logging buffer is set by default

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-4/system-monitoring/configuration/guide/b-system-monitoring-cg-asr9000-64x/b-system-monitoring-cg-asr9000-64x_chapter_0101.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	**6.3 Enable Detailed Logging** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

1.4.3 Set 'logging console critical' (Automated)

Profile Applicability:

- Level 1

Description:

Verify logging to device console is enabled and limited to a rational severity level to avoid impacting system performance and management.

Rationale:

This configuration determines the severity of messages that will generate console messages. Logging to console should be limited only to those messages required for immediate troubleshooting while logged into the device. This form of logging is not persistent; messages printed to the console are not stored by the router. Console logging is handy for operators when they use the console.

Impact:

Logging critical messages at the console is important for an organization managing technology risk. The 'logging console' command should capture appropriate severity messages to be effective.

Audit:

Perform the following to determine if the feature is enabled:
Verify a command string result returns

```
IOSXR#sh run logging
Wed Jul 19 18:32:35.155 UTC
logging trap alerts
logging buffered 123123123
logging 1.1.1.1 vrf default severity alerts
```

Remediation:

Configure console logging level.

```
IOSXR(config)#logging console critical
```

Default Value:

The default is to log all messages

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-4/system-monitoring/configuration/guide/b-system-monitoring-cg-asr9000-64x/b-system-monitoring-cg-asr9000-64x_chapter_0101.html

Additional Information:

The console is a slow display device. In message storms some logging messages may be silently dropped when the console queue becomes full. Set severity levels accordingly.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	**6.3 Enable Detailed Logging** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

1.4.4 Set IP address for 'logging host' (Automated)

Profile Applicability:

- Level 1

Description:

Log system messages and debug output to a remote host.

Rationale:

Cisco routers can send their log messages to a Unix-style Syslog service. A syslog service simply accepts messages and stores them in files or prints them according to a simple configuration file. This form of logging is best because it can provide protected long-term storage for logs (the devices internal logging buffer has limited capacity to store events.) In addition, logging to an external system is highly recommended or required by most security standards. If desired or required by policy, law and/or regulation, enable a second syslog server for redundancy.

Impact:

Logging is an important process for an organization managing technology risk. The 'logging host' command sets the IP address of the logging host and enforces the logging process.

Audit:

Perform the following to determine if a syslog server is enabled:
Verify one or more IP address(es) returns

```
RP/0/RP0/CPU0:IOSXR#sh logging
Wed Jul 19 18:35:21.188 UTC
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level critical, 127 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level alert, 0 messages logged
    Logging to 1.1.1.1, 0 message lines logged
    Buffer logging: level debugging, 950 messages logged


IOSXR#sh run logging
Wed Jul 19 18:35:46.794 UTC
logging trap alerts
logging console critical
logging buffered 123123123
logging 1.1.1.1 vrf default severity alerts
```

Remediation:

Designate one or more syslog servers by IP address.

```
hostname(config)#logging host {syslog_server}
```

Default Value:

System logging messages are not sent to any remote host.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-4/system-monitoring/configuration/guide/b-system-monitoring-cg-asr9000-64x/b-system-monitoring-cg-asr9000-64x_chapter_0101.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.1 Centralize Security Event Alerting Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		●	●
v8	13.11 Tune Security Event Alerting Thresholds Tune security event alerting thresholds monthly, or more frequently.			●

Controls Version	Control	IG 1	IG 2	IG 3
v7	**6.6 Deploy SIEM or Log Analytic tool** Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.		●	●
v7	**6.8 Regularly Tune SIEM** On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.			●

1.4.5 Set 'logging trap informational' (Automated)

Profile Applicability:

- Level 1

Description:

Limit messages logged to the syslog servers based on severity level informational.

Rationale:

This determines the severity of messages that will generate simple network management protocol (SNMP) trap and or syslog messages. This setting should be set to either "debugging" (7) or "informational" (6), but no lower.

Impact:

Logging is an important process for an organization managing technology risk. The 'logging trap' command sets the severity of messages and enforces the logging process.

Audit:

Perform the following to determine if a syslog server for SNMP traps is enabled: Verify "level informational" returns

```
IOSXR#sh run logging
Wed Jul 19 18:36:42.079 UTC
logging trap alerts
logging console critical
logging buffered 123123123
logging 1.1.1.1 vrf default severity alerts

IOSXR#sh logging
Wed Jul 19 18:37:03.574 UTC
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level critical, 127 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level alert, 0 messages logged
    Logging to 1.1.1.1, 0 message lines logged
    Buffer logging: level debugging, 961 messages logged
```

Remediation:

Configure SNMP trap and syslog logging level.

```
IOSXR(config)#logging trap informational
```

Default Value:

Disabled

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-4/system-monitoring/configuration/guide/b-system-monitoring-cg-asr9000-64x/b-system-monitoring-cg-asr9000-64x_chapter_0101.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	**6.3 Enable Detailed Logging** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

1.4.6 Set logging timestamps (Automated)

Profile Applicability:

- Level 1

Description:

Configure the system to apply a time stamp to debugging messages or system logging messages

Rationale:

Including timestamps in log messages allows correlating events and tracing network attacks across multiple devices. Enabling service timestamp to mark the time log messages were generated simplifies obtaining a holistic view of events enabling faster troubleshooting of issues or attacks.

Impact:

Logging is an important process for an organization managing technology risk and establishing a timeline of events is critical. The 'service timestamps' command sets the date and time on entries sent to the logging host and enforces the logging process.

Audit:

Perform the following to determine if the additional detail is enabled:
Verify a command string result returns

```
IOSXR#sh run | inc timestamp
Wed Jul 19 18:40:59.975 UTC
Building configuration...
service timestamps log datetime msec
```

Remediation:

Configure debug messages to include timestamps.

```
IOSXR(config)#service timestamps log datetime msec
```

Default Value:

Time stamps are applied to debug and logging messages.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-4/system-monitoring/configuration/guide/b-system-monitoring-cg-asr9000-64x/b-system-monitoring-cg-asr9000-64x_chapter_0101.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

1.4.7 Set 'logging source interface' (Automated)

Profile Applicability:

- Level 1

Description:

Specify the source IPv4 or IPv6 address of system logging packets

Rationale:

This is required so that the router sends log messages to the logging server from a consistent IP address.

Impact:

Logging is an important process for an organization managing technology risk and establishing a consistent source of messages for the logging host is critical. The 'logging source interface loopback' command sets a consistent IP address to send messages to the logging host and enforces the logging process.

Audit:

Perform the following to determine if logging services are bound to a source interface: Verify a command string result returns

```
IOSXR(config)#sh run logging
Wed Jul 19 18:41:55.797 UTC
logging trap informational
logging console critical
logging buffered 123123123
logging 1.1.1.1 vrf default severity alerts
logging source-interface MgmtEth0/RP0/CPU0/0
```

Remediation:

Bind logging to the loopback interface.

```
IOSXR(config)#logging source-interface {logging_source_interface}
```

Default Value:

The wildcard interface address is used.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-4/system-monitoring/configuration/guide/b-system-monitoring-cg-asr9000-64x/b-system-monitoring-cg-asr9000-64x_chapter_0101.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	**6.3 Enable Detailed Logging** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

1.5 SNMP Rules

Simple Network Management Protocol (SNMP) provides a standards-based interface to manage and monitor network devices. This section provides guidance on the secure configuration of SNMP parameters.

The recommendations in this Section apply to Organizations using SNMP. Organizations using SNMP should review and implement the recommendations in this section.

1.5.1 Unset 'private' for 'snmp-server community' (Automated)

Profile Applicability:

- Level 1

Description:

An SNMP community string permits read-only access to all objects.

Rationale:

The default community string "private" is well known. Using easy to guess, well known community string poses a threat that an attacker can effortlessly gain unauthorized access to the device.

Impact:

To reduce the risk of unauthorized access, Organizations should disable default, easy to guess, settings such as the 'private' setting for snmp-server community.

Audit:

Perform the following to determine if the public community string is enabled:
Ensure `private` does not show as a result

```
IOSXR# show run snmp-server | inc snmp-server community
```

Remediation:

Disable the default SNMP community string `private`

```
IOSXR(config)#no snmp-server community {community_string}
```

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r3-9/system_management/configuration/guide/yc39xr12k_chapter10.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.5** Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	**9.2** Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.5.2 Unset 'public' for 'snmp-server community' (Automated)

Profile Applicability:

- Level 1

Description:

An SNMP community string permits read-only access to all objects.

Rationale:

The default community string "public" is well known. Using easy to guess, well known community string poses a threat that an attacker can effortlessly gain unauthorized access to the device.

Impact:

To reduce the risk of unauthorized access, Organizations should disable default, easy to guess, settings such as the 'public' setting for snmp-server community.

Audit:

Perform the following to determine if the public community string is enabled: Ensure `public` does not show as a result

```
IOSXR#show run | inc snmp-server community
```

Remediation:

Disable the default SNMP community string "public"

```
IOSXR(config)#no snmp-server community {community_string}
```

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r3-9/system_management/configuration/guide/yc39xr12k_chapter10.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.5 Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.5.3 Do not set 'RW' for any 'snmp-server community' (Automated)

Profile Applicability:

- Level 1

Description:

Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.

Rationale:

Enabling SNMP read-write enables remote management of the device. Unless absolutely necessary, do not allow simple network management protocol (SNMP) write access.

Impact:

To reduce the risk of unauthorized access, Organizations should disable the SNMP 'write' access for snmp-server community.

Audit:

Perform the following to determine if a read/write community string is enabled:
Verify the result does not show a community string with a "RW"

```
IOSXR#show run | incl snmp-server community
```

Remediation:

Disable SNMP write access.

```
IOSXR(config)#no snmp-server community {community_string}
```

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s2.html#GUID-2F3F13E4-EE81-4590-871D-6AE1043473DE

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.5 <u>Implement and Manage a Firewall on End-User Devices</u>** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	**9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u>** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.5.4 Set the ACL for each 'snmp-server community' (Automated)

Profile Applicability:

- Level 1

Description:

This feature specifies a list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.

Rationale:

If ACLs are not applied, then anyone with a valid SNMP community string can potentially monitor and manage the router. An ACL should be defined and applied for all SNMP access to limit access to a small number of authorized management stations segmented in a trusted management zone. If possible, use SNMPv3 which uses authentication, authorization, and data privatization (encryption).

Impact:

To reduce the risk of unauthorized access, Organizations should enable access control lists for all snmp-server communities and restrict the access to appropriate trusted management zones. If possible, implement SNMPv3 to apply authentication, authorization, and data privatization (encryption) for additional benefits to the organization.

Audit:

Perform the following to determine if an ACL is enabled:
Verify the result shows a number after the community string

```
IOSXR#show run | incl snmp-server community
```

Remediation:

Configure authorized SNMP community string and restrict access to authorized management systems.

```
IOSXR(config)#snmp-server community {community_string} RO IPv4 {snmp_access-list}
```

Default Value:

No ACL is set for SNMP

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s2.html#GUID-2F3F13E4-EE81-4590-871D-6AE1043473DE

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.8 <u>Establish and Maintain Dedicated Computing Resources for All Administrative Work</u> Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			●
v7	11.7 <u>Manage Network Infrastructure Through a Dedicated Network</u> Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		●	●

1.5.5 Set 'snmp-server host' when using SNMP (Automated)

Profile Applicability:

- Level 1

Description:

SNMP notifications can be sent as traps to authorized management systems.

Rationale:

If SNMP is enabled for device management and device alerts are required, then ensure the device is configured to submit traps only to authorize management systems.

Impact:

Organizations using SNMP should restrict sending SNMP messages only to explicitly named systems to reduce unauthorized access.

Audit:

Perform the following to determine if SNMP traps are enabled:
If the command returns configuration values, then SNMP is enabled.

```
IOSXR#show run | incl snmp-server host
```

Remediation:

Configure authorized SNMP trap community string and restrict sending messages to authorized management systems.

```
IOSXR(config)#snmp-server host {ip_address} version {snmp_version}
{encryption-type} {trap_community_string}
```

Default Value:

A recipient is not specified to receive notifications.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s5.html#GUID-D84B2AB5-6485-4A23-8C26-73E50F73EE61

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.8 <u>Establish and Maintain Dedicated Computing Resources for All Administrative Work</u> Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			●
v7	11.7 <u>Manage Network Infrastructure Through a Dedicated Network</u> Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		●	●

1.5.6 Set 'snmp-server enable traps snmp' (Automated)

Profile Applicability:

- Level 1

Description:

SNMP notifications can be sent as traps to authorized management systems.

Rationale:

SNMP has the ability to submit traps .

Impact:

Organizations using SNMP should restrict trap types only to explicitly named traps to reduce unintended traffic. Enabling SNMP traps without specifying trap type will enable all SNMP trap types.

Audit:

Perform the following to determine if SNMP traps are enabled:
If the command returns configuration values, then SNMP is enabled.

```
IOSXR#show run | incl snmp-server
```

Remediation:

Enable SNMP traps.

```
IOSXR(config)#snmp-server traps snmp authentication
```

Default Value:

SNMP notifications are disabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s3.html#GUID-EB3EB677-A355-42C6-A139-85BA30810C54

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.8 <u>Establish and Maintain Dedicated Computing Resources for All Administrative Work</u> Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			●
v7	11.7 <u>Manage Network Infrastructure Through a Dedicated Network</u> Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		●	●

1.5.7 Set 'priv' for each 'snmp-server group' using SNMPv3 (Automated)

Profile Applicability:

- Level 2

Description:

Specifies authentication of a packet with encryption when using SNMPv3

Rationale:

SNMPv3 provides much improved security over previous versions by offering options for Authentication and Encryption of messages. When configuring a user for SNMPv3 you have the option of using a range of encryption schemes, or no encryption at all, to protect messages in transit. AES128 is the minimum strength encryption method that should be deployed.

Impact:

Organizations using SNMP can significantly reduce the risks of unauthorized access by using the 'snmp-server group v3 priv' setting to encrypt messages in transit.

Audit:

Verify the result show the appropriate group name and security model

```
IOSXR#show run | inc snmp-server group
```

Remediation:

For each SNMPv3 group created on your router add privacy options by issuing the following command...

```
IOSXR(config)#snmp-server group {snmp_group_name} v3 priv IPv4 {snmp_access-list}
```

Default Value:

No SNMP server groups are configured.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s5.html#GUID-56E87D02-C56F-4E2D-A5C8-617E31740C3F

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 <u>Use Multifactor Authentication For All Administrative Access</u> Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

1.5.8 Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3 (Automated)

Profile Applicability:

- Level 2

Description:

Specify the use of a minimum of 128-bit AES algorithm for encryption when using SNMPv3.

Rationale:

SNMPv3 provides much improved security over previous versions by offering options for Authentication and Encryption of messages. When configuring a user for SNMPv3 you have the option of using a range of encryption schemes, or no encryption at all, to protect messages in transit. AES128 is the minimum strength encryption method that should be deployed.

Impact:

Organizations using SNMP can significantly reduce the risks of unauthorized access by using the 'snmp-server user' setting with appropriate authentication and privacy protocols to encrypt messages in transit.

Audit:

Verify the result show the appropriate user name and security settings

```
IOSXR#show snmp user
```

Remediation:

For each SNMPv3 user created on your router add privacy options by issuing the following command.

```
hostname(config)#snmp-server user {snmp_user_name} {snmp_group_name} v3 auth
sha {snmp_auth_password} priv aes 128 {snmp_priv_password} ipv4 {snmp_access-
list}
```

Default Value:

SNMP username as not set by default.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-s5.html#GUID-4EED4031-E723-4B84-9BBF-610C3CF60E31

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**6.5 <u>Require MFA for Administrative Access</u>** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	**4.5 <u>Use Multifactor Authentication For All Administrative Access</u>** Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

1.6 Access Rules

Rules in the access class enforce controls for device administrative connections.

1.6.1 Disable Telnet Access (Automated)

Profile Applicability:

- Level 1

Description:

Telnet is a clear-text administrative protocol. As such, both the credentials used to establish the session and all commands and data within the session are readable in clear-text, so can be intercepted or modified by an attacker

Rationale:

Telnet doesn't natively support encryption or message integrity checks. Hence, any transmitted information (including credentials) is exposed to an attacker that gains access to the communication. Furthermore communication could be intercepted and modified by a man-in-the-middle attacker.

Impact:

Ensure you have already configured an alternative management access to the device before disabling telnet access. Otherwise you might be locked out of the device with no management access.

Audit:

Check the vty pools in use:

```
show run formal | i vty-pool
vty-pool default 0 4 line-template default
```

line-template is "default", multiple vty-pools might exist, check each.
check the corresponding line template:

```
show run formal | i "line default"
line default exec-timeout ...
...
line default transport input ssh
```

Check if `line default transport input ssh` or `line default transport input none` is present.

Remediation:

It's recommended to restrict VTYs to SSH for management access and not allow this device to SSH to other devices:

```
vty-pool default 0 4 line-template default
line default
 transport input ssh
 transport output none
```

Default Value:

By default both telnet and ssh access are enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.6 Securely Manage Enterprise Assets and Software** Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●

1.6.2 Restrict VTY Access (Automated)

Profile Applicability:

- Level 1

Description:

VTY access can be restricted via access-lists to limit from which the source addresses a management session to the device can be established.

Rationale:

VTY ACLs control what addresses may attempt to log in to the router. Configuring VTY lines to use an ACL, restricts the sources where a user can manage the device. You should limit the specific host(s) and or network(s) authorized to connect to and configure the device, via an approved protocol, to those individuals or systems authorized to administer the device. For example, you could limit access to specific hosts, so that only network managers can configure the devices only by using specific network management workstations. Make sure you configure all VTY lines to use the same ACL.

Impact:

You can potentially lock yourself out, we recommend using `commit confirmed` when implementing the changes.

Using VTY lines without access-lists opens up the attack surface because any source IP can establish a connection to the device. This could be exploited by an attacker to create DoS condition.

Audit:

Check the vty pools in use:

```
show run formal | i vty-pool
vty-pool default 0 4 line-template default
```

line-template is "default", multiple vty-pools might exist, check each.
check the corresponding line template:

```
show run formal | i "line default access"
line default access-class ingress {ssh_access-list}
```

Check if ACLs are applied to SSH server:

```
show run formal | i "ssh.*access"
ssh server vrf default ipv4 access-list {ssh_access-list}
```

Audit fails if `access-` is not in any of the outputs.

Remediation:

Define ACLs which match the allowed sources. To restrict access of incoming or outgoing connections over IPv4 and IPv6, the IPv4 access list and IPv6 access list must share the same name:

```
ipv4 access-list ACL-VTY-IN
 10 permit ipv4 192.168.1.0/24 any
 1000 deny ipv4 any any log icmp-off
ipv6 access-list ACL-VTY-IN
 10 permit ipv6 2001:db8::/64 any
 1000 deny any any log icmp-off
```

Apply the ACL on the line template:

```
vty-pool default 0 4 line-template default
line default
 access-class ingress ACL-VTY-IN
```

Alternatively you can implement restrictions on the SSH Server which allows both IPv4 and IPv6. Note that SSH could be also used for Netconf, so the ACL might need to include additional sources which do not apply for VTY access only.

```
ssh server ipv4 access-list ACL-VTY-IN ipv6 access-list ACL-VTY-IN
```

Default Value:

No access restrictions are in place by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.8 <u>Establish and Maintain Dedicated Computing Resources for All Administrative Work</u> Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			●
v7	11.7 <u>Manage Network Infrastructure Through a Dedicated Network</u> Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		●	●

1.6.3 Ensure Exec Timeout for Console Sessions is set (Automated)

Profile Applicability:

- Level 1

Description:

Verify device is configured to automatically disconnect console sessions after a defined maximum session time, set in minutes.

Note there are 3 different timeout values:

- absolute-timeout: terminate the connection after the specified time has elapsed, regardless of whether the connection is being used at the time of termination.
- exec-timeout: If no user input is detected during the interval, the EXEC facility returns the terminal to the idle state and disconnects the incoming session
- session-timeout: Traditionally the VTY can be used for other features than EXEC (CLI), e.g. terminal server, PAD, async lines etc. The session-timeout applies to any sessions running to/through the router on VTY. Use the session-timeout command to set the interval that the Cisco IOS XR software waits for traffic before closing the connection to a remote device and returning the terminal to an idle state.

For management access we need to configure the exec-timeout.

Rationale:

This prevents unauthorized users from misusing abandoned sessions. For example, if the network administrator disconnects leaving a console session open, that session will remain open (in the same state and privilege level) for the next person who connects a console cable to the device.

A shorter timeout is usually desired, but this can be extended for longer-running operations such as debug sessions or software upgrades.

Impact:

10 minutes is the default exec-timeout for many Cisco Network Operating systems. You should determine the best value for your organization and your work habits.

Audit:

Check if the exec timeout on the console is configured:

```
show run formal | i "console exec"
line console exec-timeout 10 0
```

Audit fails if value is not in accordance with your organization standards.
If not configured, the default value of 10 minutes applies.

Remediation:

```
vty-pool default 0 4 line-template default
line default
 exec-timeout 10 0
```

Default Value:

When nothing is configured, the default is 10 minutes.

References:

1. https://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/system_management/command/reference/yr37term.pdf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●

1.7 Banner Rules

Rules in the banner section communicate legal rights and other information to users.

1.7.1 Pre-authentication Banner (Automated)

Profile Applicability:

- Level 1

Description:

A pre-authentication banner is displayed when a terminal connects, before a login occurs. This banner is useful for sending messages that affect all users (such as impending system shutdowns). This banner can also be used to notify unauthorized users of any penalties to accessing the device, or any logging that may be configured.

Rationale:

Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have following primary functions.

- Banners may be used to generate consent to real-time monitoring under ECPA Title III.
- Banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA.
- in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v. Ortega, 480 U.S. 709 (1987).
- In the case of a non-government network, banners may establish a system administrator's "common authority" to consent to a law enforcement search pursuant to United States v. Matlock, 415 U.S. 164 (1974)." (US Department of Justice APPENDIX A: Sample Network Banner Language)

In your country different laws might apply. Please consult with your corporate legal team to assess the exact legal context and rules for banners.

Impact:

Organizations provide appropriate legal notice(s) and warning(s) to persons accessing their networks by using a 'banner-text'.

Audit:

Show the running configuration banners:

```
IOSXR#show run banner
```

If the command does not return a result, the banner is not enabled.

Remediation:

Configure a login banner as shown below. The delimiter character shown is a "^", but any character can serve as a delimiter.

```
IOSXR(config)# banner login ^ {login_banner} ^
```

Default Value:

No login or motd banner is set by default.

Additional Information:

On IOS XR the sequence of banners is as follows (for SSH login, might differ for telnet):

1. motd banner (shown before authentication)
2. login banner (shown after motd, before authentication)
3. exec banner (shown after successful authentication)

We recommend using the "login" banner (for consistency with IOS XE). But motd banner can also be used instead.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

1.7.2 Post-authentication Banner (Automated)

Profile Applicability:

- Level 1

Description:

A post-authentication banner is displayed to the user after a successful login. It can also serve as a legal notice to authorized users of the equipment to notify them of any logging that may be configured.

This banner is not appropriate to notify unauthorized users of any penalties to accessing the device, because after successful login corresponding laws might have already been violated.

A post-authentication banner can often also hold asset-specific information, such as:

- The primary technical contacts for the equipment
- Location or environment information - for instance the street address or rack number or production / test / lab environment
- The purchase date
- The asset tag information for the device
- Any upstream circuit numbers
- Carrier or ISP support phone numbers
- Any other asset-specific information that may be important to the organization

Rationale:

Post-authentication banners can be used to reduce the risk of human error. For example by highlighting the current environment (Production or Lab).

Impact:

Organizations provide appropriate notice(s) and warning(s) to persons accessing their networks by using a 'banner-text'.

Audit:

Show the running configuration with a "b" filter to "begin" the listing at the found string

```
IOSXR#show run banner
```

If the command does not return a result, the banner is not enabled.

Remediation:

Configure an exec banner as shown below. The delimiter character shown is a "^", but any character can serve as a delimiter.

```
IOSXR(config)# banner exec ^ {exec_banner} ^
```

Default Value:

No banner is set by default.

Additional Information:

On IOS XR the sequence of banners is as follows (for SSH login):

1. motd banner (shown before authentication)
2. login banner (shown after motd, before authentication)
3. exec banner (shown after successful authentication)

Only the exec banner can be used for this purpose.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	**11.1 Maintain Standard Security Configurations for Network Devices** Maintain standard, documented security configuration standards for all authorized network devices.		●	●

1.8 Password Rules

Rules in the password class enforce secure, local device authentication credentials.

1.8.1 Enable AES Password Encryption (Manual)

Profile Applicability:

- Level 2

Description:

You can enable strong, reversible 128-bit Advanced Encryption Standard (AES) password encryption, also known as type-6 encryption. To start using type-6 encryption, you must enable the AES password encryption feature and configure a master encryption key, which is used to encrypt and decrypt passwords. After you enable AES password encryption and configure a master key, all existing and newly created clear-text passwords for supported applications are stored in type-6 encrypted format

Rationale:

Encryption of passwords is used to protect it from being sent over the wire cleartext or being accidentally exposed when sharing device configurations with third parties. By applying encryption you are making it more difficult for an adversary to gain access to your device/network.

Impact:

Make sure to store your master in a secure place and test your emergency backup/restore procedures. Without the masterkey all passwords of supported type6 applications will need to be re-entered manually upon config restore from backup.

Audit:

Just verifying the running configuration might not be sufficient because it could be that no masterkey has been set.

```
IOSXR# show run formal | i password6
password6 encryption aes
```

Use the following show command to see if encryption is enabled and functional. Only when all three status are "Enabled" the feature is fully working.

```
IOSXR#show type6 server

Server detail information:
==========================================
AES config State       :       Enabled
Masterkey config State :       Enabled
Type6 feature State    :       Enabled
Master key Inprogress  :       No

Verify Type 6 trace server details.
```

Remediation:

Define a password encryption key

```
IOSXR#key config-key password-encryption

New password Requirements: Min-length 6, Max-length 64
Characters restricted to [A-Z][a-z][0-9]
Enter new key :
Enter confirm key :
Master key operation is started in background
```

Enable aes config password encryption

```
/* Enable Type 6 password encryption */
IOSXR# configure
IOSXR(config)#password6 encryption aes
IOSXR(config)#commit
```

Default Value:

type 6 aes password encryption is disabled.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-9/system-security/configuration/guide/b-system-security-cg-asr9000-79x/implementing-type-6-password-encryption.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4 <u>Secure Configuration of Enterprise Assets and Software</u> Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).			

1.8.2 Set username secret for all local users (Manual)

Profile Applicability:

- Level 1

Description:

A root-system user with a normal password will not be authenticated because the normal password is two-way encrypted and poses a security risk because the password information is stored in the flash disk, which can be easily decrypted. Secrets are one-way encrypted and cannot be easily reverted without brute-forcing.

If both secret and password are configured for a user, then secret takes precedence, and password security policy does not have any effect on authentication or change of password for such users.

Rationale:

Secrets use a one-way cryptographic hash.

Impact:

Typically the username and secret are defined during initial setup. Make sure to use strong passwords or update it later accordingly.

Audit:

The following command is used to show all local users:

```
IOSXR# show run username
username {local_username}
 group root-lr
 group cisco-support
 secret {local_password}
```

Remediation:

```
IOSXR# configure
IOSXR(config)#username {local_username}
IOSXR(config)#secret {local_password}

commit
```

Default Value:

At least one user must be defined during initial setup via console.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-5/system-security/configuration/guide/b-system-security-cg-asr9000-65x/b-system-security-cg-asr9000-71x_chapter_010.html#concept_js2_ll3_jmb

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●

1.8.3 Configure a Password Policy (Manual)

Profile Applicability:

- Level 2

Description:

Because passwords are stored only in revertible type 7 format, please consider not applying this recommendation and using secrets instead.

This only applies if you absolutely need to configure "password" instead of "secret" for local users.

Cisco IOS XR Software introduces advanced AAA password strengthening policy and security mechanism to store, retrieve and provide rules or policy to specify user passwords. This password policy is applicable only for local users, and not for remote users whose profile information are stored in a third party AAA server.

Rationale:

Strong passwords are important because they help prevent unauthorized access to devices and the network. Even if a central authentication source is used, if that service is not available the fall-back authentication is often to local credentials. At least one local administrator user must be present on the device.

Impact:

This policy is not applicable to secrets of the user. If both secret and password are configured for a user, then secret takes precedence, and password security policy does not have any effect on authentication or change of password for such users.

Audit:

```
IOSXR#sh run aaa

aaa password-policy {password_policy}
 lifetime months 3
 max-length 25
 min-length 18
 lockout-time days 1
 min-char-change 5
 authen-max-attempts 3
!
username {local_username}
 group root-lr
 group cisco-support
 secret {local_password}
```

The policy is only in effect when it is also applied under a "username" section.

Remediation:

Use the following configuration to enable a password policy. Choose values according to established guidelines of your organization.

```
IOSXR# configure
IOSXR(config)#aaa password-policy {password_policy}
IOSXR(config-aaa)#min-length 8
IOSXR(config-aaa)#max-length 25
IOSXR(config-aaa)#lifetime months 3
IOSXR(config-aaa)#min-char-change 5
IOSXR(config-aaa)#authen-max-attempts 3
IOSXR(config-aaa)#lockout-time days 1
IOSXR(config)#username {local_username} password-policy {password_policy}
password 0 {local_password}
IOSXR(config)#commit
```

Default Value:

By default no password policy is enabled.

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-5/system-security/configuration/guide/b-system-security-cg-asr9000-65x/b-system-security-cg-asr9000-71x_chapter_010.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●

1.9 Management plane protection (Automated)

Profile Applicability:

- Level 2

Description:

The Management Plane Protection (MPP) feature provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows a network operator to designate one or more router interfaces as management interfaces.

The MPP protection feature, as well as all the management protocols under MPP, are disabled by default. When you configure an interface as either out-of-band or inband, it automatically enables MPP. Consequently, this enablement extends to all the protocols under MPP. If MPP is disabled and a protocol is activated, all interfaces can pass traffic.

When MPP is enabled with an activated protocol, the only default management interfaces allowing management traffic are the route processor (RP) and standby route processor (SRP) Ethernet interfaces. You must manually configure any other interface for which you want to enable MPP as a management interface.

Rationale:

This is part of the MPP setup.

Impact:

The following restrictions are listed for implementing Management Plane Protection (MPP):

Currently, MPP does not keep track of the denied or dropped protocol requests.

MPP configuration does not enable the protocol services. MPP is responsible only for making the services available on different interfaces. The protocols are enabled explicitly.

Management requests that are received on inband interfaces are not necessarily acknowledged there.

Both Route Processor (RP) and distributed route processor (DRP) Ethernet interfaces are by default out-of-band interfaces and can be configured under MPP.

The changes made for the MPP configuration do not affect the active sessions that are established before the changes.

Currently, MPP controls only the incoming management requests for protocols, such as TFTP, Telnet, Simple Network Management Protocol (SNMP), Secure Shell (SSH), XML , HTTP and Netconf.

MPP does not support MIB.

Audit:

Verify the appropriate management plane protection configuration.

```
IOSXR#sh run control-plane
Wed Jul 19 23:25:11.297 UTC
control-plane
 management-plane
  inband
   interface Loopback1
    allow SSH peer
     address ipv4 1.1.1.1
     !
   !
  !
  out-of-band
   interface MgmtEth0/RP0/CPU0/0
    allow SSH peer
     address ipv4 1.1.1.1
```

Remediation:

Configure the management plane so that only certain protocols connectced to certain interfaces can access this IOS-XR device.

```
IOSXR(config)#control-plane
IOSXR(config-ctrl)#management-plane
IOSXR(config-mpp)#inband
IOSXR(config-mpp-inband)#interface {interface} allow {protocol} peer address
ipv4 {IP_address}
IOSXR(config-mpp)#out-of-band
IOSXR(config-mpp-outband)#interface {interface} allow {protocol} peer address
ipv4 {IP_address}
```

Default Value:

Not set

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r5-3/security/configuration/guide/b-syssec-cg53x-crs/b-syssec-cg53x-crs_chapter_0110.html

2 Control Plane

The control plane covers monitoring, route table updates, and generally the dynamic operation of the router. Services, settings, and data streams that support and document the operation, traffic handling, and dynamic status of the router. Examples of control plane services include: logging (e.g. Syslog), routing protocols, status protocols like CDP and HSRP, network topology protocols like STP, and traffic security control protocols like IKE. Network control protocols like ICMP, NTP, ARP, and IGMP directed to or sent by the router itself also fall into this area.

2.1 Routing protocols

A routing protocol specifies how routers communicate with each other to distribute information that enables them to select routes between nodes on a computer network.

Enable routing authentication so that they only accept updates from trusted systems.

2.1.1 EIGRP

The Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of IGRP developed by Cisco. EIGRP uses distance vector routing technology, which specifies that a router need not know all the router and link relationships for the entire network. Each router advertises destinations with a corresponding distance and upon receiving routes, adjusts the distance and propagates the information to neighboring routes.

2.1.1.1 Authentication (Automated)

Profile Applicability:

- Level 2

Description:

Configure the EIGRP address family.

Rationale:

Rationale: EIGRP is a true multi-protocol routing protocol and the 'address-family' feature enables restriction of exchanges with specific neighbors

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using 'address-family' for EIGRP enforces these policies by restricting the exchanges between predefined network devices.

Audit:

Verify that authentication is configured:

```
IOSXR#sh run key chain
Wed Jul 19 21:48:31.091 UTC
key chain CHAIN
 key 1
  key-string password 045802150C2E

IOSXR#sh run router eigrp
Wed Jul 19 21:48:03.792 UTC
router eigrp 100
 address-family ipv4
  interface Loopback1
   authentication keychain CHAIN
  !
  interface MgmtEth0/RP0/CPU0/0
   authentication keychain CHAIN
```

Remediation:

Configure the EIGRP address family.

```
IOSXR(config)#router eigrp {AS_number}
IOSXR(config-eigrp)# address-family ipv4
IOSXR(config-eigrp-af)#  interface {interface}
IOSXR(config-eigrp-af-if)#authentication keychain {key_chain_name}
```

Default Value:

Not set

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r3-9/routing/configuration/guide/xr12krc39_chapter2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** Secure Configuration for Network Devices, such as Firewalls, Routers and Switches			

2.1.2 OSPF

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) developed by the OSPF working group of the Internet Engineering Task Force (IETF). Designed expressly for IP networks, OSPF supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

OSPF Version 3 (OSPFv3) expands on OSPF Version 2, providing support for IPv6 routing prefixes.

2.1.2.1 Authentication (Automated)

Profile Applicability:

- Level 2

Description:

Enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication.

Rationale:

This is part of the OSPF authentication setup

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Configuring the proper interface(s) for 'ip ospf message-digest-key md5' enforces these policies by restricting exchanges between network devices.

Audit:

Verify the appropriate md5 key is defined on the appropriate interface(s)

```
IOSXR#sh run key chain
Wed Jul 19 21:54:01.554 UTC
key chain CHAIN
 key 1
  key-string password 045802150C2E

IOSXR#sh run router ospf
Wed Jul 19 21:54:20.095 UTC
router ospf 1
 address-family ipv4
 area 0
  authentication keychain CHAIN
```

Remediation:

Configure the appropriate interface(s) for Message Digest authentication

```
IOSXR(config)#router ospf {process_id}
IOSXR(config-ospf)# address-family ipv4
IOSXR(config-ospf)#area 0 authentication keychain {key_chain_name}
```

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/command/ospf-i1.html#GUID-939C79FF-8C09-4D5A-AEB5-DAF25038CA18

2.1.3 BGP

Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) that allows you to create loop-free interdomain routing between autonomous systems. An autonomous system is a set of routers under a single technical administration. Routers in an autonomous system can use multiple Interior Gateway Protocols (IGPs) to exchange routing information inside the autonomous system and an EGP to route packets outside the autonomous system.

2.1.3.1 Authentication (Automated)

Profile Applicability:

- Level 2

Description:

Enable message digest5 (MD5) authentication on a TCP connection between two BGP peers

Rationale:

Enforcing routing authentication reduces the likelihood of routing poisoning and unauthorized routers from joining BGP routing.

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols. Using the 'neighbor password' for BGP enforces these policies by restricting the type of authentication between network devices.

Audit:

Verify you see the appropriate neighbor password is defined:

```
IOSXR#sh run router bgp
Wed Jul 19 22:02:46.892 UTC
router bgp 100
 neighbor 10.10.10.10
  remote-as 200
  password encrypted 104D000A061811021F0725282D3B303A
```

Remediation:

Configure BGP neighbor authentication where feasible.

```
IOSXR(config)#router bgp {local_AS_number}
IOSXR(config-bgp)#neighbor {neighbor_IP_address} remote-as {remote_AS_number}
IOSXR(config-bgp)#neighbor {neighbor_IP_address} password clear
{BGP_password}
```

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/command/bgp-n1.html#GUID-A8900842-ECF3-42D3-B188-921BE0EC060B

2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/command/bgp-m1.html#GUID-159A8006-F0DF-4B82-BB71-C39D2C134205

Additional Information:

MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers.

2.1.4 ISIS

The IS-IS routing protocol supports the configuration of backbone Level 2 and Level 1 areas and the necessary support for moving routing information between the areas. Routers establish Level 1 adjacencies to perform routing within a local area (intra-area routing). Routers establish Level 2 adjacencies to perform routing between Level 1 areas (interarea routing).

For Cisco IOS XR software software, each IS-IS instance can support either a single Level 1 or Level 2 area, or one of each. By default, all IS-IS instances automatically support Level 1 and Level 2 routing. You can change the level of routing to be performed by a particular routing instance using the is-type command.

Key Features Supported in the Cisco IOS XR IS-IS Implementation The Cisco IOS XR implementation of IS-IS conforms to the IS-IS Version 2 specifications detailed in RFC 1195 and the IPv6 IS-IS functionality based on the Internet Engineering Task Force (IETF) IS-IS Working Group draft-ietf-isis-ipv6.txt document.

The following list outlines key features supported in the Cisco IOS XR implementation:

Single topology IPv6

Multitopology

Nonstop forwarding (NSF), both Cisco proprietary and IETF

Three-way handshake

Mesh groups

Multiple IS-IS instances

Configuration of a broadcast medium connecting two networking devices as a point-to-point link

Fast-flooding with different threads handling flooding and shortest path first (SPF)._

2.1.4.1 Authentication (Automated)

Profile Applicability:

- Level 2

Description:

Enable authentication for ISIS packets and to specify the set of keys that can be used on an interface.

Rationale:

This is part of the ISIS authentication setup

Impact:

TBC TBC

Audit:

Verify the appropriate key chain and mode are set on the appropriate interface(s)

```
RP/0/RP0/CPU0:IOSXR#sh run key chain
Wed Jul 19 22:22:46.974 UTC
key chain CHAIN
 key 1
  key-string password 045802150C2E


RP/0/RP0/CPU0:IOSXR#sh run router isis
Wed Jul 19 22:23:56.615 UTC
router isis 1
 lsp-password keychain CHAIN
 interface MgmtEth0/RP0/CPU0/0
  hello-password keychain CHAIN
```

Remediation:

Configure the Interface with the RIPv2 key chain.

```
IOSXR(config)#router isis {process_id}
IOSXR(config-isis)#lsp-password keychain {key_chain_name}
IOSXR(config-isis)#interface {interface}
IOSXR(config-isis-if)#hello-password keychain {key_chain_name}
```

Default Value:

Not set

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF
2. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_rip/command/irr-cr-rip.html#GUID-C1C84D0D-4BD0-4910-911A-ADAB458D0A84

2.1.5 RIP

The Routing Information Protocol (RIP) is a classic distance vector Interior Gateway Protocol (IGP) designed to exchange information within an autonomous system (AS) of a small network.

This module describes the concepts and tasks to implement basic RIP routing. Cisco IOS XR software supports a standard implementation of RIP Version 2 (RIPv2) that supports backward compatibility with RIP Version 1 (RIPv1) as specified by RFC 2453.

2.1.5.1 Authentication (Automated)

Profile Applicability:

- Level 2

Description:

Enable authentication for Routing Information Protocol (RIP) Version 2 packets and to specify the set of keys that can be used.

Rationale:

This is part of the RIPv2 authentication setup

Impact:

Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols, RIP v2 is no exception.

Audit:

Verify the appropriate key chain and mode are set on the appropriate interface(s)

```
IOSXR#sh run router rip
Wed Jul 19 21:19:21.400 UTC
router rip
 interface MgmtEth0/RP0/CPU0/0
  authentication keychain CHAIN mode md5

IOSXR#sh rip
Wed Jul 19 21:21:58.785 UTC

RIP config:
Active:                     Yes
Added to socket:            Yes
Out-of-memory state:         Normal
Version:                     2
Default metric:              Not set
Maximum paths:               4
Auto summarize:             No
Broadcast for V2:           No
Packet source validation:  Yes
NSF:                         Disabled
Timers: Update:              30 seconds (13 seconds until next update)
        Invalid:             180 seconds
        Holddown:            180 seconds
        Flush:               240 seconds
```

Remediation:

Configure the Interface with the RIPv2 key chain.

```
IOSXR(config)#router rip
IOSXR(config-rip)#interface {interface}
IOSXR(config-rip-if)#authentication keychain {key_chain_name} mode md5
```

Default Value:

Not set

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r4-0/routing/configuration/guide/rc40xr12k_chapter6.html

2.1.6 Key chains (Automated)

Profile Applicability:

- Level 2

Description:

Keychain management is a common method of authentication to configure shared secrets on all entities that exchange secrets such as keys, before establishing trust with each other. Routing protocols and network management applications on Cisco IOS XR software often use authentication to enhance security while communicating with peers.

Rationale:

The keychain by itself has no relevance; therefore, it must be used by an application that needs to communicate by using the keys (for authentication) with its peers. The keychain provides a secure mechanism to handle the keys and rollover based on the lifetime. Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS) use the keychain to implement a hitless key rollover for authentication. BGP uses TCP authentication, which enables the authentication option and sends the Message Authentication Code (MAC) based on the cryptographic algorithm configured for the keychain.

Impact:

This allows the configuration of routing protocol authentication to be made earier.

Audit:

```
IOSXR#sh run key chain
Wed Jul 19 21:02:23.744 UTC
key chain CHAIN
 key 1
  key-string password 1511021F0725
 !
```

Remediation:

```
IOSXR(config)#key chain {key_chain_name}
IOSXR(config-CHAIN)#key {key_id}
IOSXR(config-CHAIN-1)#key-string {key_string}
```

Default Value:

By default no key strings are configured

References:

1. https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r3-9/security/configuration/guide/sc39kcm.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.5 <u>Centralize Network Authentication, Authorization, and Auditing (AAA)</u> Centralize network AAA.		●	●
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

2.2 NTP

Network Time Protocol allows administrators to set the system time on all of their compatible systems from a single source, ensuring a consistent time stamp for logging and authentication protocols. NTP is an internet standard, defined in RFC1305.

2.2.1 Require Encryption Keys for NTP

NTP synchronizes timekeeping among a set of distributed time servers and clients. With this synchronization, you can correlate events to the time that system logs were created and the time that other time-specific events occur. An NTP server must be accessible by the client switch.

NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communication uses Coordinated Universal Time (UTC), which is the same as Greenwich Mean Time. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock that is attached to a time server. NTP distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another.

NTP uses a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server has a radio or atomic clock that is directly attached, a stratum 2 time server receives its time from a stratum 1 time server, and so on. A machine running NTP automatically chooses as its time source the machine with the lowest stratum number that it is configured to communicate with through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP has two ways to avoid synchronizing to a machine whose time might be ambiguous:

•NTP never synchronizes to a machine that is not synchronized itself.

•NTP compares the time that is reported by several machines and does not synchronize to a machine whose time is significantly different from the others, even if its stratum is lower.

The communications between machines running NTP, known as associations, are usually statically configured; each machine is given the IP addresses of all machines with which it should form associations. An associated pair of machines can keep accurate timekeeping by exchanging NTP messages between each other. However, in a LAN environment, you can configure NTP to use IP broadcast messages. With this alternative, you can configure the machine to send or receive broadcast messages, but the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

Cisco's implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that you obtain the time service for your network from the public NTP servers available on the IP Internet.

If the network is isolated from the Internet, Cisco's NTP implementation allows a machine to be configured so that it acts as though it is synchronized using NTP, when it actually has determined the time using other methods. Other machines synchronize to that machine using NTP.

2.2.1.1 Set 'ntp authenticate' (Automated)

Profile Applicability:

- Level 2

Description:

Enable NTP authentication.

Rationale:

Using authenticated NTP ensures the Cisco device only permits time updates from authorized NTP servers.

Impact:

Organizations should establish three Network Time Protocol (NTP) hosts to set consistent time across the enterprise. Enabling the 'ntp authenticate' command enforces authentication between NTP hosts.

Audit:

From the command prompt, execute the following commands:

```
IOSXR(config)#sh run ntp
!
ntp
 authentication-key 1 md5 encrypted 104D000A0618
 authenticate
 server 1.1.1.1 key 1
```

Remediation:

Configure NTP authentication:

```
IOSXR(config)#ntp authenticate
```

Default Value:

NTP authentication is not enabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-8BEBDAF4-6D03-4C3E-B8D6-6BCBC7D0F324

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.4** <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	**6.1** <u>Utilize Three Synchronized Time Sources</u> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.2.1.2 Set 'ntp authentication-key' (Automated)

Profile Applicability:

- Level 2

Description:

Define an authentication key for Network Time Protocol (NTP).

Rationale:

Using an authentication key provides a higher degree of security as only authenticated NTP servers will be able to update time for the Cisco device.

Impact:

Organizations should establish three Network Time Protocol (NTP) hosts to set consistent time across the enterprise. Enabling the 'ntp authentication-key' command enforces encrypted authentication between NTP hosts.

Audit:

From the command prompt, execute the following commands:

```
IOSXR#show run ntp
```

Remediation:

Configure at the NTP key ring and encryption key using the following command

```
IOSXR(config)#ntp authentication-key {ntp_key_id} md5 {ntp_key}
```

Default Value:

No authentication key is defined for NTP.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-0435BFD1-D7D7-41D4-97AC-7731C11226BC

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.4 Standardize Time Synchronization** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	**6.1 Utilize Three Synchronized Time Sources** Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.2.1.3 Set the 'ntp trusted-key' (Automated)

Profile Applicability:

- Level 2

Description:

Ensure you authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize

Rationale:

This authentication function provides protection against accidentally synchronizing the system to another system that is not trusted, because the other system must know the correct authentication key.

Impact:

Organizations should establish three Network Time Protocol (NTP) hosts to set consistent time across the enterprise. Enabling the 'ntp trusted-key' command enforces encrypted authentication between NTP hosts.

Audit:

From the command prompt, execute the following commands:

```
RP/0/RP0/CPU0:IOSXR#sh run ntp
Wed Jul 19 22:08:20.188 UTC
ntp
 authentication-key 1 md5 encrypted 130404160A1F
 authenticate
 trusted-key 1
 server 1.1.1.1 key 1
```

The above command should return any NTP server(s) configured with encryption keys. This value should be the same as the total number of servers configured as tested in.

Remediation:

Configure the NTP trusted key using the following command

```
IOSXR(config)#ntp trusted-key {ntp_key_id}
```

Default Value:

Authentication of the identity of the system is disabled.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-89CA798D-0F12-4AE8-B382-DE10CBD261DB

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.2.1.4 Set 'key' for each 'ntp server' (Automated)

Profile Applicability:

- Level 2

Description:

Specifies the authentication key for NTP.

Rationale:

This authentication feature provides protection against accidentally synchronizing the ntp system to another system that is not trusted, because the other system must know the correct authentication key.

Impact:

Organizations should establish three Network Time Protocol (NTP) hosts to set consistent time across the enterprise. Enabling the 'ntp server key' command enforces encrypted authentication between NTP hosts.

Audit:

From the command prompt, execute the following commands:

```
IOSXR#show run ntp
```

Remediation:

Configure each NTP Server to use a key ring using the following command.

```
IOSXR(config)#ntp server {ntp-server_ip_address} key {ntp_key_id}
```

Default Value:

No NTP key is set by default

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.2.2 Set 'ip address' for 'ntp server' (Automated)

Profile Applicability:

- Level 1

Description:

Use this command if you want to allow the system to synchronize the system software clock with the specified NTP server.

Rationale:

To ensure that the time on your Cisco router is consistent with other devices in your network, at least two (and preferably at least three) NTP Server/s external to the router should be configured.

Ensure you also configure consistent timezone and daylight savings time setting for all devices. For simplicity, the default of Coordinated Universal Time (UTC).

Impact:

Organizations should establish multiple Network Time Protocol (NTP) hosts to set consistent time across the enterprise. Enabling the 'ntp server ip address' enforces encrypted authentication between NTP hosts.

Audit:

From the command prompt, execute the following commands:

```
IOSXR#sh run ntp
```

Remediation:

Configure theexternal NTP Server using the following commands

```
IOSXR(config)#ntp server {ntp-server_ip_address} key {ntp_key_id}
```

Default Value:

No servers are configured by default.

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-255145EB-D656-43F0-B361-D9CBCC794112
2. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/command/bsm-cr-book/bsm-cr-n1.html#wp3294676008

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> 　　Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> 　　Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.3 VRRP

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network.

The Virtual Router Redundancy Protocol (VRRP) feature can solve the static configuration problem. VRRP is an IP routing redundancy protocol designed to allow for transparent failover at the first-hop IP router. VRRP enables a group of routers to form a single virtual router . The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

2.3.1 Authentication (Automated)

Profile Applicability:

- Level 2

Description:

You can ensure that VRRP messages received from VRRP routers that comprise a virtual router are authenticated by configuring a simple text password.

Rationale:

This is part of the VRRP authentication setup

Impact:

An important aspect of the VRRP redundancy scheme is VRRP router priority. Priority determines the role that each VRRP router plays and what happens if the master virtual router fails.

If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router functions as a master virtual router.

Priority also determines if a VRRP router functions as a backup virtual router and determines the order of ascendancy to becoming a master virtual router if the master virtual router fails. You can configure the priority of each backup virtual router with a value of 1 through 254, using the vrrp priority command.

For example, if Router A, the master virtual router in a LAN topology, fails, an election process takes place to determine if backup virtual Routers B or C should take over. If Routers B and C are configured with the priorities of 101 and 100, respectively, Router B is elected to become master virtual router because it has the higher priority. If Routers B and C are both configured with the priority of 100, the backup virtual router with the higher IP address is elected to become the master virtual router.

By default, a preemptive scheme is enabled whereby a higher-priority backup virtual router that becomes available takes over for the backup virtual router that was elected to become master virtual router. You can disable this preemptive scheme using the no vrrp preempt command. If preemption is disabled, the backup virtual router that is elected to become master virtual router remains the master until the original master virtual router recovers and becomes master again.

Audit:

Verify that VRRP is running and authentication is bsing used.

```
RP/0/RP0/CPU0:IOSXR#sh run router vrrp
Mon Jul 24 14:57:34.430 UTC
router vrrp
 interface MgmtEth0/RP0/CPU0/0
  address-family ipv4
   vrrp 1
    text-authentication cisco
```

Remediation:

Configure VRRP with the appropriate password.

```
IOSXR(config)#router vrrp
IOSXR(config-vrrp)#interface {interface}
IOSXR(config-vrrp-if)#address-family ipv4
IOSXR(config-vrrp-address-family)#vrrp {virtual_router_id}
IOSXR(config-vrrp-virtual-router)#text-authentication {password}
```

Default Value:

Not set

References:

1. https://community.cisco.com/t5/networking-knowledge-base/basic-hsrp-configuration-on-cisco-ios-xr/ta-p/3147683

2.4 HSRP

The Hot Standby Router Protocol (HSRP) is an IP routing redundancy protocol designed to allow for transparent failover at the first-hop IP router. HSRP provides high network availability, because it routes IP traffic from hosts on networks without relying on the availability of any single router. HSRP is used in a group of routers for selecting an active router and a standby router. (An active router is the router of choice for routing packets; a standby router is a router that takes over the routing duties when an active router fails, or when preset conditions are met.

2.4.1 Authentication (Automated)

Profile Applicability:

- Level 2

Description:

Enable authentication for HSRP packets and to specify the set of keys that can be used on an interface.

Rationale:

This is part of the HSRP authentication setup

Impact:

The Hot Standby Router Protocol (HSRP) is an IP routing redundancy protocol designed to allow for transparent failover at the first-hop IP router. HSRP provides high network availability, because it routes IP traffic from hosts on networks without relying on the availability of any single router. HSRP is used in a group of routers for selecting an active router and a standby router. (An active router is the router of choice for routing packets; a standby router is a router that takes over the routing duties when an active router fails, or when preset conditions are met.

Audit:

Verify that HSRP is running and authentication is bsing used.

```
IOSXR#sh run router hsrp
Wed Jul 19 22:29:07.903 UTC
router hsrp
 interface MgmtEth0/RP0/CPU0/0
  address-family ipv4
   hsrp 1
    authentication cisco
```

Remediation:

Configure HSRP with the appropriate password.

```
IOSXR(config)#router hsrp
IOSXR(config-hsrp)#interface {interface}
IOSXR(config-hsrp-if)#address-family ipv4 hsrp {hsrp_group_number}
authentication {hsrp_password}
```

Default Value:

Not set

References:

1. https://community.cisco.com/t5/networking-knowledge-base/basic-hsrp-configuration-on-cisco-ios-xr/ta-p/3147683

3 Data Plane

Services and settings related to the data passing through the router (as opposed to direct to it). The data plane is for everything not in control or management planes. Settings on a router concerned with the data plane include interface access lists, firewall functionality (e.g. CBAC), NAT, and IPSec. Settings for traffic-affecting services like unicast RPF verification and CAR/QoS also fall into this area.

3.1 URPF (Automated)

Profile Applicability:

- Level 2

Description:

Enable Unicast reverse path forwarding to prevent IP speeofing attacks.

Rationale:

Impact:

Unicast Reverse Path Forwarding (URPF) is a mechanism for validating the source IP address of packets received on a router. A router configured with URPF performs a reverse path lookup in the FIB table tovalidate the presence of the source IP address. If the source IP address is listed in the table, then it indicatesthat the source is reachable and valid. If source IP address cannot be located in the FIB table, the packet istreated as malicious by the router and discarded.

Audit:

Verify the appropriate key chain and mode are set on the appropriate interface(s)

```
IOSXR#sh run interface mgmtEth 0/RP0/CPU0/0
Wed Jul 19 22:37:55.238 UTC
interface MgmtEth0/RP0/CPU0/0
 cdp
 ipv4 address dhcp
 ipv4 verify unicast source reachable-via rx
```

Remediation:

Configure the Interface with the RIPv2 key chain.

```
IOSXR(config)#int {interface}
IOSXR(config-if)#ipv4 verify unicast source reachable-via rx
```

Default Value:

Not set

References:

1. https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/security/73x/b-system-security-cg-ncs5500-73x/implementing-urpf.pdf

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Management Plane**		
1.1	**Authentication, Authorization and Accounting (AAA) Rules**		
1.1.1	**AAA prerequisites**		
1.1.1.1	TACACS+ (Automated)	☐	☐
1.1.1.2	RADIUS (Automated)	☐	☐
1.1.2	**Authentication**		
1.1.2.1	console authentication (Automated)	☐	☐
1.1.2.2	vty line authentication (Automated)	☐	☐
1.1.3	**Authorization**		
1.1.3.1	Configure Authorization (Manual)	☐	☐
1.1.4	**Accounting**		
1.1.4.1	exec accounting (Automated)	☐	☐
1.1.4.2	command accounting (Automated)	☐	☐
1.1.4.3	network accounting (Automated)	☐	☐
1.1.4.4	system accounting (Automated)	☐	☐
1.1.5	Local users, groups and tasks (Automated)	☐	☐
1.2	**SSH**		
1.2.1	Set the 'hostname' (Automated)	☐	☐
1.2.2	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.2.3	Set 'seconds' for 'ssh timeout' for 60 seconds or less (Automated)	☐	☐
1.3	**Global Service Rules**		
1.3.1	Disable CDP (Automated)	☐	☐
1.3.2	Disable TCP and UDP small servers (Automated)	☐	☐
1.4	**Logging Rules**		
1.4.1	Enable logging (Automated)	☐	☐
1.4.2	Set 'buffer size' (Automated)	☐	☐
1.4.3	Set 'logging console critical' (Automated)	☐	☐
1.4.4	Set IP address for 'logging host' (Automated)	☐	☐
1.4.5	Set 'logging trap informational' (Automated)	☐	☐
1.4.6	Set logging timestamps (Automated)	☐	☐
1.4.7	Set 'logging source interface' (Automated)	☐	☐
1.5	**SNMP Rules**		
1.5.1	Unset 'private' for 'snmp-server community' (Automated)	☐	☐
1.5.2	Unset 'public' for 'snmp-server community' (Automated)	☐	☐
1.5.3	Do not set 'RW' for any 'snmp-server community' (Automated)	☐	☐
1.5.4	Set the ACL for each 'snmp-server community' (Automated)	☐	☐
1.5.5	Set 'snmp-server host' when using SNMP (Automated)	☐	☐
1.5.6	Set 'snmp-server enable traps snmp' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.5.7	Set 'priv' for each 'snmp-server group' using SNMPv3 (Automated)	☐	☐
1.5.8	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3 (Automated)	☐	☐
1.6	**Access Rules**		
1.6.1	Disable Telnet Access (Automated)	☐	☐
1.6.2	Restrict VTY Access (Automated)	☐	☐
1.6.3	Ensure Exec Timeout for Console Sessions is set (Automated)	☐	☐
1.7	**Banner Rules**		
1.7.1	Pre-authentication Banner (Automated)	☐	☐
1.7.2	Post-authentication Banner (Automated)	☐	☐
1.8	**Password Rules**		
1.8.1	Enable AES Password Encryption (Manual)	☐	☐
1.8.2	Set username secret for all local users (Manual)	☐	☐
1.8.3	Configure a Password Policy (Manual)	☐	☐
1.9	Management plane protection (Automated)	☐	☐
2	**Control Plane**		
2.1	**Routing protocols**		
2.1.1	**EIGRP**		
2.1.1.1	Authentication (Automated)	☐	☐
2.1.2	**OSPF**		
2.1.2.1	Authentication (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.3	**BGP**		
2.1.3.1	Authentication (Automated)	☐	☐
2.1.4	**ISIS**		
2.1.4.1	Authentication (Automated)	☐	☐
2.1.5	**RIP**		
2.1.5.1	Authentication (Automated)	☐	☐
2.1.6	Key chains (Automated)	☐	☐
2.2	**NTP**		
2.2.1	**Require Encryption Keys for NTP**		
2.2.1.1	Set 'ntp authenticate' (Automated)	☐	☐
2.2.1.2	Set 'ntp authentication-key' (Automated)	☐	☐
2.2.1.3	Set the 'ntp trusted-key' (Automated)	☐	☐
2.2.1.4	Set 'key' for each 'ntp server' (Automated)	☐	☐
2.2.2	Set 'ip address' for 'ntp server' (Automated)	☐	☐
2.3	**VRRP**		
2.3.1	Authentication (Automated)	☐	☐
2.4	**HSRP**		
2.4.1	Authentication (Automated)	☐	☐
3	**Data Plane**		
3.1	URPF (Automated)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.7.1	Pre-authentication Banner	☐	☐
1.7.2	Post-authentication Banner	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	TACACS+	☐	☐
1.1.1.2	RADIUS	☐	☐
1.1.2.1	console authentication	☐	☐
1.1.2.2	vty line authentication	☐	☐
1.1.5	Local users, groups and tasks	☐	☐
1.2.1	Set the 'hostname'	☐	☐
1.2.2	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa'	☐	☐
1.2.3	Set 'seconds' for 'ssh timeout' for 60 seconds or less	☐	☐
1.3.1	Disable CDP	☐	☐
1.3.2	Disable TCP and UDP small servers	☐	☐
1.4.1	Enable logging	☐	☐
1.4.2	Set 'buffer size'	☐	☐
1.4.3	Set 'logging console critical'	☐	☐
1.4.4	Set IP address for 'logging host'	☐	☐
1.4.5	Set 'logging trap informational'	☐	☐
1.4.6	Set logging timestamps	☐	☐
1.4.7	Set 'logging source interface'	☐	☐
1.5.1	Unset 'private' for 'snmp-server community'	☐	☐
1.5.2	Unset 'public' for 'snmp-server community'	☐	☐
1.5.3	Do not set 'RW' for any 'snmp-server community'	☐	☐
1.5.4	Set the ACL for each 'snmp-server community'	☐	☐
1.5.5	Set 'snmp-server host' when using SNMP	☐	☐
1.5.6	Set 'snmp-server enable traps snmp'	☐	☐
1.5.7	Set 'priv' for each 'snmp-server group' using SNMPv3	☐	☐
1.5.8	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.6.2	Restrict VTY Access	☐	☐
1.7.1	Pre-authentication Banner	☐	☐
1.7.2	Post-authentication Banner	☐	☐
2.1.6	Key chains	☐	☐
2.2.1.1	Set 'ntp authenticate'	☐	☐
2.2.1.2	Set 'ntp authentication-key'	☐	☐
2.2.1.3	Set the 'ntp trusted-key'	☐	☐
2.2.1.4	Set 'key' for each 'ntp server'	☐	☐
2.2.2	Set 'ip address' for 'ntp server'	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	TACACS+	☐	☐
1.1.1.2	RADIUS	☐	☐
1.1.2.1	console authentication	☐	☐
1.1.2.2	vty line authentication	☐	☐
1.1.5	Local users, groups and tasks	☐	☐
1.2.1	Set the 'hostname'	☐	☐
1.2.2	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa'	☐	☐
1.2.3	Set 'seconds' for 'ssh timeout' for 60 seconds or less	☐	☐
1.3.1	Disable CDP	☐	☐
1.3.2	Disable TCP and UDP small servers	☐	☐
1.4.1	Enable logging	☐	☐
1.4.2	Set 'buffer size'	☐	☐
1.4.3	Set 'logging console critical'	☐	☐
1.4.4	Set IP address for 'logging host'	☐	☐
1.4.5	Set 'logging trap informational'	☐	☐
1.4.6	Set logging timestamps	☐	☐
1.4.7	Set 'logging source interface'	☐	☐
1.5.1	Unset 'private' for 'snmp-server community'	☐	☐
1.5.2	Unset 'public' for 'snmp-server community'	☐	☐
1.5.3	Do not set 'RW' for any 'snmp-server community'	☐	☐
1.5.4	Set the ACL for each 'snmp-server community'	☐	☐
1.5.5	Set 'snmp-server host' when using SNMP	☐	☐
1.5.6	Set 'snmp-server enable traps snmp'	☐	☐
1.5.7	Set 'priv' for each 'snmp-server group' using SNMPv3	☐	☐
1.5.8	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
1.6.2	Restrict VTY Access	☐	☐
1.7.1	Pre-authentication Banner	☐	☐
1.7.2	Post-authentication Banner	☐	☐
2.1.6	Key chains	☐	☐
2.2.1.1	Set 'ntp authenticate'	☐	☐
2.2.1.2	Set 'ntp authentication-key'	☐	☐
2.2.1.3	Set the 'ntp trusted-key'	☐	☐
2.2.1.4	Set 'key' for each 'ntp server'	☐	☐
2.2.2	Set 'ip address' for 'ntp server'	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.3.1	Configure Authorization	☐	☐
1.1.4.1	exec accounting	☐	☐
1.1.4.2	command accounting	☐	☐
1.1.4.3	network accounting	☐	☐
1.1.4.4	system accounting	☐	☐
1.6.1	Disable Telnet Access	☐	☐
1.6.3	Ensure Exec Timeout for Console Sessions is set	☐	☐
1.8.1	Enable AES Password Encryption	☐	☐
1.8.2	Set username secret for all local users	☐	☐
1.8.3	Configure a Password Policy	☐	☐
1.9	Management plane protection	☐	☐
2.1.2.1	Authentication	☐	☐
2.1.3.1	Authentication	☐	☐
2.1.4.1	Authentication	☐	☐
2.1.5.1	Authentication	☐	☐
2.3.1	Authentication	☐	☐
2.4.1	Authentication	☐	☐
3.1	URPF	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.4.1	exec accounting	☐	☐
1.1.4.2	command accounting	☐	☐
1.1.4.3	network accounting	☐	☐
1.1.4.4	system accounting	☐	☐
1.2.1	Set the 'hostname'	☐	☐
1.2.2	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa'	☐	☐
1.2.3	Set 'seconds' for 'ssh timeout' for 60 seconds or less	☐	☐
1.3.1	Disable CDP	☐	☐
1.3.2	Disable TCP and UDP small servers	☐	☐
1.5.1	Unset 'private' for 'snmp-server community'	☐	☐
1.5.2	Unset 'public' for 'snmp-server community'	☐	☐
1.5.3	Do not set 'RW' for any 'snmp-server community'	☐	☐
1.5.7	Set 'priv' for each 'snmp-server group' using SNMPv3	☐	☐
1.5.8	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3	☐	☐
1.6.1	Disable Telnet Access	☐	☐
1.6.3	Ensure Exec Timeout for Console Sessions is set	☐	☐
1.7.1	Pre-authentication Banner	☐	☐
1.7.2	Post-authentication Banner	☐	☐
1.8.2	Set username secret for all local users	☐	☐
1.8.3	Configure a Password Policy	☐	☐
2.1.1.1	Authentication	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	TACACS+	☐	☐
1.1.1.2	RADIUS	☐	☐
1.1.2.1	console authentication	☐	☐
1.1.2.2	vty line authentication	☐	☐
1.1.4.1	exec accounting	☐	☐
1.1.4.2	command accounting	☐	☐
1.1.4.3	network accounting	☐	☐
1.1.4.4	system accounting	☐	☐
1.1.5	Local users, groups and tasks	☐	☐
1.2.1	Set the 'hostname'	☐	☐
1.2.2	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa'	☐	☐
1.2.3	Set 'seconds' for 'ssh timeout' for 60 seconds or less	☐	☐
1.3.1	Disable CDP	☐	☐
1.3.2	Disable TCP and UDP small servers	☐	☐
1.4.1	Enable logging	☐	☐
1.4.2	Set 'buffer size'	☐	☐
1.4.3	Set 'logging console critical'	☐	☐
1.4.4	Set IP address for 'logging host'	☐	☐
1.4.5	Set 'logging trap informational'	☐	☐
1.4.6	Set logging timestamps	☐	☐
1.4.7	Set 'logging source interface'	☐	☐
1.5.1	Unset 'private' for 'snmp-server community'	☐	☐
1.5.2	Unset 'public' for 'snmp-server community'	☐	☐
1.5.3	Do not set 'RW' for any 'snmp-server community'	☐	☐
1.5.7	Set 'priv' for each 'snmp-server group' using SNMPv3	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
1.5.8	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3	☐	☐
1.6.1	Disable Telnet Access	☐	☐
1.6.3	Ensure Exec Timeout for Console Sessions is set	☐	☐
1.7.1	Pre-authentication Banner	☐	☐
1.7.2	Post-authentication Banner	☐	☐
1.8.2	Set username secret for all local users	☐	☐
1.8.3	Configure a Password Policy	☐	☐
2.1.1.1	Authentication	☐	☐
2.1.6	Key chains	☐	☐
2.2.1.1	Set 'ntp authenticate'	☐	☐
2.2.1.2	Set 'ntp authentication-key'	☐	☐
2.2.1.3	Set the 'ntp trusted-key'	☐	☐
2.2.1.4	Set 'key' for each 'ntp server'	☐	☐
2.2.2	Set 'ip address' for 'ntp server'	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	TACACS+	☐	☐
1.1.1.2	RADIUS	☐	☐
1.1.2.1	console authentication	☐	☐
1.1.2.2	vty line authentication	☐	☐
1.1.4.1	exec accounting	☐	☐
1.1.4.2	command accounting	☐	☐
1.1.4.3	network accounting	☐	☐
1.1.4.4	system accounting	☐	☐
1.1.5	Local users, groups and tasks	☐	☐
1.2.1	Set the 'hostname'	☐	☐
1.2.2	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa'	☐	☐
1.2.3	Set 'seconds' for 'ssh timeout' for 60 seconds or less	☐	☐
1.3.1	Disable CDP	☐	☐
1.3.2	Disable TCP and UDP small servers	☐	☐
1.4.1	Enable logging	☐	☐
1.4.2	Set 'buffer size'	☐	☐
1.4.3	Set 'logging console critical'	☐	☐
1.4.4	Set IP address for 'logging host'	☐	☐
1.4.5	Set 'logging trap informational'	☐	☐
1.4.6	Set logging timestamps	☐	☐
1.4.7	Set 'logging source interface'	☐	☐
1.5.1	Unset 'private' for 'snmp-server community'	☐	☐
1.5.2	Unset 'public' for 'snmp-server community'	☐	☐
1.5.3	Do not set 'RW' for any 'snmp-server community'	☐	☐
1.5.4	Set the ACL for each 'snmp-server community'	☐	☐
1.5.5	Set 'snmp-server host' when using SNMP	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.5.6	Set 'snmp-server enable traps snmp'	☐	☐
1.5.7	Set 'priv' for each 'snmp-server group' using SNMPv3	☐	☐
1.5.8	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3	☐	☐
1.6.1	Disable Telnet Access	☐	☐
1.6.2	Restrict VTY Access	☐	☐
1.6.3	Ensure Exec Timeout for Console Sessions is set	☐	☐
1.7.1	Pre-authentication Banner	☐	☐
1.7.2	Post-authentication Banner	☐	☐
1.8.2	Set username secret for all local users	☐	☐
1.8.3	Configure a Password Policy	☐	☐
2.1.1.1	Authentication	☐	☐
2.1.6	Key chains	☐	☐
2.2.1.1	Set 'ntp authenticate'	☐	☐
2.2.1.2	Set 'ntp authentication-key'	☐	☐
2.2.1.3	Set the 'ntp trusted-key'	☐	☐
2.2.1.4	Set 'key' for each 'ntp server'	☐	☐
2.2.2	Set 'ip address' for 'ntp server'	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.3.1	Configure Authorization	☐	☐
1.9	Management plane protection	☐	☐
2.1.2.1	Authentication	☐	☐
2.1.3.1	Authentication	☐	☐
2.1.4.1	Authentication	☐	☐
2.1.5.1	Authentication	☐	☐
2.3.1	Authentication	☐	☐
2.4.1	Authentication	☐	☐
3.1	URPF	☐	☐

Appendix: Change History

Date	Version	Changes for this version