Insecure Feature Restrictions on IOS XE

Introduction

One component of Cisco Resilient Infrastructure is the deprecation and removal of insecure features from Cisco products. A key component of the feature deprecation and removal strategy is the “restriction” phase whereby customers’ administrators must intentionally acknowledge they wish to use features that have been designated as insecure.

This document explains the mechanism by which IOS XE implements these restrictions, and the operational considerations administrators should be aware of when deploying software versions that incorporate these changes. The first release of Cisco IOS XE to incorporate restrictions is 26.1.1. These restrictions are intended to evolve in future software releases, with additional features being added to the list of restricted, insecure features.

Beginning with the 17.18.2 release, many features are designed to generate warnings when configured, alerting customers that insecure configurations are present. The 26.1.1 release extends these warnings by restricting some of the features that trigger warnings, requiring the configuration of ‘insecure mode’ to enable them. Not all features that generate warnings will immediately be enforced with insecure mode but may be enforced in future releases.

Insecure Mode Overview

IOS XE 26.1.1 introduces the concept of ‘insecure mode’. The intention of this mode is to raise awareness of insecure configuration practices and encourage customers to move to more secure, modern alternatives. The general operation is as follows:

- When a device with no configuration is initialized (no startup-configuration), the device is designed to reject the configuration of any command designated as insecure. Customers who attempt to configure an insecure feature are expected to receive a warning message indicating the configuration is blocked and requires insecure mode to enable.
- If a customer enters ‘system mode insecure’, this enables insecure mode and permits the configuration that is featured on the insecure feature list. Warnings are still displayed even in insecure mode.
- To prevent network outages on upgrades, if a device is upgraded to a release that incorporates insecure feature restrictions and the existing configuration contains insecure commands, the device will automatically enable ‘system mode insecure’ and this command is configured to appear in the configuration file after the upgrade.
- To disable ‘insecure mode’, all insecure configurations must be removed from the device before the administrator can configure ‘no system mode insecure’ to return the device back to the hardened state.

Insecure Mode Command Reference

In addition to the configuration-level **system mode insecure** command used to enable and disable insecure mode, several exec-level commands are available to understand the posture of the device.

show system security mode

Indicates whether insecure mode is enabled or not

show system insecure configuration

Displays the configurations present that require **system mode insecure**. This command must indicate that no insecure configurations are present before insecure mode can be disabled. Note that the device scans for insecure configuration periodically, and configuration changes may not be immediately reflected in the output of this command. The command shows the last time the configuration was scanned and the timing for the next scan. Devices with very large configuration files may take several minutes to scan.

test system secure db

Triggers an insecure configuration scan immediately. If you have recently made a configuration change and **show system insecure configuration** still reflects the old configuration, this command will scan the configuration immediately so that the updated posture is reflected in **show system insecure configuration**.

show system insecure profile

Displays the list of all the commands that are designated as insecure with a description and reason why it is designated as insecure. This list may change in future releases to include additional commands as they are deemed insecure.

More Details

For more details and examples of command outputs, visit the TAC support bulletin.

Frequently Asked Questions (FAQ)

Q: What happens when a device with an insecure configuration is upgraded to a release in the Restriction phase for that feature?
A: When a device is upgraded to a restriction release for a given feature, the system is designed to detect the insecure configurations during the boot process and is designed to automatically transition the device to Insecure Mode.

Q: When will my insecure feature move into the Restriction or Removal phase?
A: The timing for when your insecure feature will move into the Restriction or Removal phase varies by feature and operating system. For detailed information, please refer to the Feature Deprecation and Removal Details documentation.

Q: What alternatives exist for my particular insecure feature?
A: Customers can refer to the Feature Removal and Suggested Alternatives documentation to identify recommended alternatives to various insecure features and protocols.

Q: How can I see which insecure configurations I currently have applied?
A: To see which Restriction phase insecure configurations you currently have applied, you can use the command **show system insecure configuration** on IOS XE 26.1.1 and later releases. Additionally, in Cisco SD-WAN Manager, you can navigate to **Monitor** > **Advisories** and select the **Insecure Configurations** tab to view insecure configurations across devices, configuration groups, and templates, with links to remediation steps. This view is refreshed approximately every 30 minutes to ensure up-to-date information.

Q: How can I see a list of all possible insecure configurations on a given software version?
A: You can use the command **show system insecure profile** to view a complete list of all Restriction-phase insecure CLI patterns that the system is designed to detect. Unlike **show system insecure configuration**, which shows only the insecure configurations currently applied, the profile output includes all known insecure configurations in the Restriction phase and will be updated over time as security best practices evolve.

Q: I corrected an insecure configuration. Why does it still show up in the **show system insecure configuration** output?
A: The scan for insecure configurations only runs periodically while in Insecure Mode. This means that after correcting an insecure configuration, the system may not immediately reflect the change until the next scheduled scan occurs, which

happens on a 30-minute interval. This scheduling ensures that the latest insecure configuration details are updated and displayed regularly while minimizing the overhead needed to perform the scan. You can use the **test system secure all** command to force an immediate rescan, so you don't have to wait for the scan timer to expire.

Q: How can I proactively check which insecure configurations I have applied before upgrading?
A: To proactively check which insecure configurations you have applied before upgrading, prior to IOS XE 17.18.2, customers can use the **Cisco AI Assistant for Support bot** available on the Cisco Resilient Infrastructure page, which allows uploading configurations to identify insecure features. A similar tool, the Cisco Config Resilient Infrastructure Tester is another option for customers. Starting with IOS XE 17.18.2 and later, customers can still use these tools, but you also have the option to directly run the command **show system insecure configuration** on your devices to view the insecure configurations currently applied. However, using the AI Assistant for Support bot and Resilient Infrastructure Tester provides additional AI-driven augmentation beyond the direct CLI command.
