Cisco IOS XE Resilient Infrastructure

Contents

Overview

Cisco is committed to protecting its products and customer networks from increasingly sophisticated cyber threats. As computing power and the security landscape evolve, the industry must transition from older technologies to modern, more robust capabilities that strengthen network defenses, reduce attack surfaces, and safeguard sensitive data. The drive to resilient infrastructure aligns with global regulations that require products to be secure by default and secure by design.

To support a smooth transition, Cisco will enhance default settings for greater protection, introduce advanced security features, and retire outdated functionalities that no longer meet today's standards. Customers are encouraged to adopt these modern capabilities and align with current best practices. The phased approach begins with informational alerts, followed by enabling stronger configurations by default, and ultimately removing older features.

Transition plan and functionality impact by release

Beginning with Cisco IOS XE 17.18.2, Cisco will implement a phased plan to retire insecure capabilities. The table below describes the transition phases and the associated functionality impact across key release milestones.

Note: Cisco IOS XE 26.1 is the next major release train after 17.18; no intervening major releases are omitted. The new numbering reflects the year-based convention introduced in 2026. For details, see the Cisco IOS XE Software Lifecycle Support Statement.

Release milestone	Transition phase and functionality impact
IOS XE 17.18.2 and onwards	**Insecure Feature Warnings** Cisco IOS XE software will display warning messages when configuring features or protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings will also appear when security best practices are not followed, along with suggestions for secure alternatives.
IOS XE 26.1.1 and onwards	**Secure By Default** On Cisco IOS XE 26.1.1 and subsequent releases, key insecure features will be disabled by default. To configure these features, administrators must explicitly opt in to "**system mode insecure**." Existing deployments will continue to function. Upon upgrades to IOS XE 26.1.1 or later, "system mode insecure" will be enabled automatically on devices already configured with insecure protocols to prevent service disruption. Devices that have undergone a factory-reset, and new installations will require administrators to enable "system mode insecure" explicitly. Some features on specific platforms may not have a restriction phase, with only warnings continuing for several releases before removal. Continuing the functionality introduced in IOS XE 17.18.2, devices will generate warnings for insecure features in use.

Release milestone	Transition phase and functionality impact
Future Releases	**Removal of Insecure Features** Insecure features will be removed in phases, with the timing of removal based on user impact and feature adoption. For example, widely deployed features will be removed over a longer period compared to less-used ones.

For details about the changes introduced in a specific release, refer to the applicable release notes.

Information on the features and protocols impacted by this bulletin, and Cisco's recommended secure alternatives can be found at Resilient Infrastructure - Feature Removal and Suggested Alternatives.

To learn more about resilient infrastructure, please visit www.cisco.com/go/ri

Product-specific resources

The following product-specific documents provide guidance on how to identify if a device is using insecure features or protocols, along with the steps for adopting or implementing their secure alternatives or for enabling "system mode insecure," if necessary.

- Cisco 9000 Series Switches
- Cisco Catalyst SD-WAN & Cisco 8000 Series Routers
- Cisco Catalyst 9800 Series Wireless Controllers & Wireless Access Points
- Cisco Industrial IoT

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C51-5716501-00 08/26