Product bulletin
Cisco public

Cisco IOS-XR – Resilient Infrastructure

Contents

Introduction 3

Product-specific resources 5

Introduction

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 defences, reduce attack surfaces, and safeguard sensitive data. Cisco's commitment to resilient infrastructure supports global regulations that require products to be secure by default and secure by design.

To facilitate a seamless transition, Cisco will enhance default settings for greater protection, introduce advanced security features, and retire outdated functionalities that no longer meet current security standards. Customers are encouraged to adopt these modern capabilities and align with current best practices. This phased approach begins with informational alerts, progresses to enabling stronger configurations by default, and culminates in the removal of older features.

Beginning with Cisco IOS XR 25.4.1 and all future releases, Cisco IOS XR software will display warning messages when features or protocols are configured without sufficient security. This includes scenarios involving the transmission of sensitive data without encryption or via outdated encryption mechanisms. Furthermore, warnings will be issued when security best practices are not adhered to, along with suggestions for secure alternatives.

In upcoming releases, certain protocols listed below will transition to optional packages, enabling a more restricted deployment. To ensure existing configurations on the router continue to function, administrators must install the relevant optional packages. Ultimately, the features detailed in the list below will be removed, with the timing of their removal subject to user impact and adoption.

While this list is subject to change, the following features and protocols are currently planned to generate warnings in releases beginning with Cisco IOS XR 25.4.1. Specific changes for each release will be detailed in its respective Release Notes.

- **FTP** Recommendation: Use SFTP or SCP.
- **Install using FTP** Recommendation: SFTP or SCP
- **copy using FTP as source or destination** Recommendation: Use SFTP or SCP.
- **TFTP** Recommendation: Use SFTP or SCP
- **Install using TFTP** Recommendation: SFTP or SCP
- **copy using FTP as source or destination** Recommendation: Use SFTP or SCP.
- **Telnet** Recommendation: Use SSH
- **IPV4 SOURCE ROUTE** Recommendation: Discontinue its use
- **TCP UDP small servers** Recommendation: Discontinue its use.
- **Weak DSA SSH host key** Recommendation: Remove crypto key zeroize dsa.

- **Weak DSA and RSA SSH host keys** Recommendation: Remove crypto key zeroize dsa, and upgrade crypto key generate rsa to at least 3072 bits.
- **Weak RSA SSH host key** Recommendation: Upgrade crypto key generate rsa to minimum length of 3072 bits.
- **SSHv1** Recommendation: Use ssh server v2.
- **SSH host-key DSA algorithm** Recommendation: Use other algorithms.
- **Weak SSH ciphers: 3des-cbc** Recommendation: Use aes128gcm.
- **Weak SSH key-exchange: diffie-hellman-group1-sha1**. Recommendation: Use diffie-hellman-group16-sha512.
- **Syslog TLS Version 1.1 (server1)** Recommendation: Configure TLS version 1.2 or higher.
- **TLS 1.0/1.1 Usage** Recommendation: Use TLS version 1.2 or 1.3 for better security.
- **NTP version number**. Recommendation: **Use version 4.’**
- **RADIUS over UDP with shared secret (Type7 encoding)** Recommendation: **Use Type-6 encryption instead of Type-7**.
- **Radius over UDP with shared secret - Default mode** Recommendation: Use RADIUS over TLS (RadSec) or DTLS.
- **TACACS+ shared secret (Type 7 encoding) Recommendation: Use Type 6 (AES-based) encryption**.
- **TACACS+ over TCP with shared secret - Default mode.** Recommendation: **Use TACACS+ over TLS (Secure TACACS+).**

In addition to the protocols listed above that will begin generating warnings in the 25.4.1 release, **SNMPv1, SNMPv2, SNMPv2c**, and **SNMPv3 without AuthPriv** will be restricted and ultimately removed in a future release and the recommendation is to migrate to **SNMPv3 with AuthPriv**. SNMP updates are being shared at this stage for informational purposes. Cisco will communicate the exact modifications once the release and related restrictions are confirmed.

A comprehensive list of protocol deprecations, including reasons for removal and associated release timelines, is available in the Feature Deprecation section of the Cisco Trust Center. Note that timelines for restrictions and removals are subject to change; therefore, customers are advised to consult the XR Release Notes for the most current guidance.

Full details on Cisco’s commitment to resilient infrastructure are available at cisco.com/go/ri with updates and details on future changes.

Product-specific resources

For links to the configuration guides for implementing the recommendation listed above on Cisco IOS-XR devices, please refer to the following table.

Product Name	Impact	Solution and guidelines
Cisco IOS XR series Devices	System will generate warnings if any of the features listed in this bulletin are configured	Users are recommended to migrate to more secure features using the steps provided in Cisco IOS XR documentation.

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 C25-5825003-00 03/26