



Release Notes for Cisco IOS XRd, IOS XR Release 26.3.1

Contents

Cisco IOS XRd, IOS XR Release 26.3.1 2

New software features 2

Changes in behavior 3

Open issues 3

Known issues 3

Compatibility 4

Related resource 4

Legal information 5

Cisco IOS XRd, IOS XR Release 26.3.1

Cisco IOS XRd Release 26.3.1 introduces targeted advancements in system security and software reliability, reinforcing the platform’s commitment to robust operational integrity. This release integrates Gated shell access, which mandates cryptographic Consent Token authorization for direct root shell access, thereby ensuring secure, auditable control and persistent enforcement of security policies across reloads and high-availability events. Complementing this, SSH client strict host key check strengthens outbound SSH connection security by enforcing rigorous host key validation, with system-wide trusted key storage that persists through system events. Collectively, these features fortify the security posture of Cisco IOS XRd, mitigate risks associated with unauthorized access, and provide consistent, policy-driven operational safeguards, aligning with the evolving requirements of secure, reliable network infrastructure deployments.

New software features

This section provides a brief description of the new software features introduced in this release.

Table 1. New software features for IOS XRd, Release 26.3.1

Product impact	Feature	Description
System Security		
Software Reliability	Gated shell access	Gated shell access requires consent token authorization for direct root shell access initiated through supported shell commands. You gain secure, auditable control over root shell access by requiring cryptographic Consent Token authorization before granting access. This feature persists your security settings across reloads and high-availability events, helping prevent unauthorized or accidental changes while retaining familiar shell workflows after authorization.
Software Reliability	SSH client strict host key check	You enhance SSH security by enforcing strict host key checking, allowing you to control how the SSH client handles new or changed server keys – accept, reject, or prompt for approval. Trusted host keys are stored system-wide and persist across

Product impact	Feature	Description
		reloads, ensuring consistent validation for your outbound SSH connections.

Changes in behavior

Deprecation and phasing out features with insecure capabilities and its secure alternatives

In Release 26.3.1, Cisco IOS XR software displays warning messages when you configure features or protocols that lack sufficient security, such as those that transmit sensitive data without encryption or use outdated encryption mechanisms. The software also shows warnings when you do not follow security best practices, and it provides suggestions for secure alternatives.

This list may change, but Cisco plans to generate warnings for the following features and protocols from Release 25.3.1. Each Release Notes will describe the exact changes for that version.

These documents list all features planned for removal, including insecure commands, and provide recommended secure alternatives to help you maintain network security and compliance.

- o [Feature deprecation phasing out insecure capabilities](#)
- o [Feature deprecation and removal details](#)
- o [Feature removal and suggested alternatives](#)

Table 2. Deprecation and phasing out features with insecure capabilities and its secure alternatives

If you are using the following insecure features...	Then follow these secure alternatives...
TLS 1.0 TLS 1.1	Use TLS 1.2 or TLS 1.3.
SSH key-exchange algorithm diffie-hellman-group1-sha1	Use stronger SSH key-exchange algorithms. Do not configure diffie-hellman-group1-sha1.
SSH ciphers 3des-cbc	Use stronger SSH ciphers.
SSH host-key DSA algorithm	Use ECDSA, ED25519, or RSA host keys. Note: The SSH host-key DSA algorithm is not recommended. However, it has not been removed. If required, you can still generate and use DSA host keys. Cisco recommends using ECDSA, ED25519, or RSA host keys.
SSHv1	Use SSHv2.

Open issues

There are no open issues in this release.

Known issues

There are no known issues in this release.

Compatibility

Supported deployments

This section details the supported XRd deployments in this release.

Table 3. Supported deployments for Cisco IOS XRd, Release 26.3.1

Deployment	Reference
Amazon Elastic Kubernetes Service (AWS EKS)	XRd vRouter or XRd Control Plane on AWS EKS
XRd lab deployments	XR docs virtual routing

Related resource

Table 4. Related resource

Resource	Description
Smart licensing	Provides information about Smart Licensing Using Policy solutions and their deployment on IOS XR routers.
Cisco XRd documentation	Provides CDC documentation for Cisco XRd.
XRd tools	Provides utilities to: - Apply bugfixes to XRd images - Verify the host is setup correctly to run XRd - Assist in launching XRd instances in a lab environment
XR docs virtual routing	Provides instructions for deploying XRd in lab settings, along with information on other deployment environments that are not yet officially supported.
Cisco IOS XR Error messages	Allows searching by release number, error strings, or comparing release numbers to view a detailed repository of error messages and descriptions.
Cisco IOS XR MIBs	Allows selecting the MIB of your choice from a drop-down to explore an extensive repository of MIB information.
Feature deprecation and removal details	Outlines the features currently supported by each operating system.
Feature deprecation phasing out insecure capabilities	Provides a list of insecure features and protocols that are scheduled for systematic deprecation and eventual removal from specified Cisco products.
Feature removal and suggested alternatives	Details the reasons why certain features or protocols are deemed insecure and offers secure alternatives when available.
Yang data models in GitHub	Provides yang data models introduced and enhanced in every IOS XR release.
Recommended release	Provides a general guide in case of upgrading IOS XR routers or new deployments that involve IOS XR routers.

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.