Release Notes for Cisco ESR 6300 Router, IOS XE 26.1.x

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cisco ESR6300 Routers, IOS XE 26.1.x 3
New software features 3
IOS XE 26.1.2 3
IOS XE 26.1.1 3
New hardware features 3
IOS XE 26.1.2 3
IOS XE 26.1.1 4
Change in behavior 4
IOS XE 26.1.2 4
IOS XE 26.1.1 4
Example: 4
Resolved issues 5
IOS XE 26.1.2 5
IOS XE 26.1.1 5
Open issues 5
IOS XE 26.1.2 5
IOS XE 26.1.1 5
Known issues 5
IOS XE 26.1.1 5
Compatibility 5
Supported software packages 6
IOS XE 26.1.2 6
IOS XE 26.1.1 7
Port Naming Conventions 7
Related resources 7
Legal information 9

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco ESR6300 Routers, IOS XE 26.1.x

This release note provides information about the new features, resolved and open issues, supported software packages and information on how to obtain support and documentation.

New software features

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

IOS XE 26.1.2

There are no new software features in this release.

IOS XE 26.1.1

Table 1. New software features for Cisco ESR6300 Routers, IOS XE 26.1.1

Product Impact	Feature	Description
Security	Resilient Infrastructure	As part of the ongoing commitment to network security, this release introduces secure alternatives to legacy commands. These updates are designed to mitigate potential risks and assist in establishing a more robust and secure operational baseline. The identified insecure commands are categorized as: • Line transport: Updates to secure remote access methods. • Device server configuration: Hardening of server-side settings. • File transfer protocols: Transitioning to encrypted transfer methods. • SNMP: Enhancements to secure management traffic. • Passwords: Strengthening authentication and credential management. • Miscellaneous: General security improvements for various system functions. The show system insecure configuration command introduced in Cisco IOS XE 17.18.2 release lists all insecure commands configured on the device. For all detected insecure configurations during device boot or upgrade, error messages are displayed. In Cisco IOS XE 26.1.1 release, all insecure CLI commands are blocked by default to strengthen your network infrastructure. If your environment requires the use of a legacy command, you must enable the system mode insecure command in global configuration mode. • Recommendation: Do not use insecure mode. This mode is temporary and will be removed in a future release. Identify and replace all insecure commands with their secure alternatives. • Upgrade behavior: If you upgrade to Cisco IOS XE 26.1.1 release with insecure commands already present in the running configuration, the system mode insecure command is automatically added to your configuration to prevent service disruption. For more details, see Resilient Infrastructure IOS XE Security Warnings Reference

New hardware features

IOS XE 26.1.2

There are no new hardware features in this release.

© 2026 Cisco and/or its affiliates. All rights reserved.

IOS XE 26.1.1

There are no hardware features in this release.

Change in behavior

IOS XE 26.1.2

There is no new change in behavior in this release.

IOS XE 26.1.1

Syslog Warning on Reload for SSH Hostkeys

After a device reload, you may see a syslog warning indicating insufficient SSH host key length, even if a strong RSA or EC key is configured.

Note:

- In the syslog warning message "**crypto key generate rsa modulus** *<modulus-size>* **label** *<label-name>",* the *<modulus-size>* and *<label-name>* represent the actual modulus size and label configured on the device.
- The SSH keypair association configuration is done using the command: **ip ssh ec|rsa** *<keypair-name>,* where *<keypair-name>* corresponds to the keypair name configured on the device.

Example:

RSA

Warning Observed: INSECURE DYNAMIC WARNING - Module: SSH.

Command: **crypto key generate rsa modulus** *<modulus-size>* **label** *<label-name>.*

Reason: An SSH host key has been provisioned on the device with insufficient key length.

Remediation: Please provision an SSH RSA host key with minimum modulus size of 3072 bits for enhanced security.

Sub mode: exec.

Parent CLI: Not Applicable.

EC

Warning Observed: INSECURE DYNAMIC WARNING - Module: SSH.

Command: **crypto key generate ec keysize** *<modulus-size>* **label** *<label-name>.*

Reason: An SSH host key has been provisioned on the device with insufficient key length.

Remediation: Please provision an SSH EC host key with minimum modulus size of 256 bits for enhanced security.

Sub mode: exec.

Parent CLI: Not Applicable.

If you have already configured a strong key, you can ignore the warnings that may appear during boot before the keypair association takes effect. The system applies the SSH keypair association (**ip ssh ec/rsa** *<keypair-name>*) after the boot process.

Once this configuration is active, SSH will use the correct key for secure connections.

© 2026 Cisco and/or its affiliates. All rights reserved.

Resolved issues

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

IOS XE 26.1.2

There are no resolved issues in this release.

IOS XE 26.1.1

There are no resolved issues in this release.

You can also access the resolved caveats for this release through the Cisco Bug Search Tool.

Open issues

IOS XE 26.1.2

There are no open issues in this release.

IOS XE 26.1.1

There are no open issues in this release.

Known issues

IOS XE 26.1.1

There are no known issues in this release.

Compatibility

This section provides compatibility details for cellular module modem firmware and OEM/PRI versions used in Cisco IoT routers. It includes the latest modem firmware available for each supported modem. See the Cisco Firmware Upgrade Guide for 4G LTE and 5G Cellular Modems for upgrade instructions.

Cisco IOS XE updates do not automatically update modem firmware. You must manually check and update all modems to the latest firmware version, including any related PRI and/or OEMPRI components. Refer to the following table for the most up-to-date information.

Table 2. Cellular Module Modem Firmware for Cisco ESR6300 Router, IOS XE 26.1.x

Cellular Module	Modem and Firmware version	Software download link
P-LTE-MNA	WP7610 02.37.03.05	https://software.cisco.com/download/home/286324942/type
P-LTE-LA	EM7430 2.38.00.00	Generic: https://software.cisco.com/download/home/286308413/type
	EM7430 02.33.03.00	Australia Telstra: https://software.cisco.com/download/home/286311403/type

© 2026 Cisco and/or its affiliates. All rights reserved.

Cellular Module	Modem and Firmware version	Software download link
	EM7430 2.38.00.00	Japan: https://software.cisco.com/download/home/286311416/type
P-LTEA-EA	EM7455 02.37.0x.00	Generic: https://software.cisco.com/download/home/286308426/type
	EM7455 02.39.00.00	Europe: https://software.cisco.com/download/home/286308426/type
	EM7455 02.32.11.00	Canada: https://software.cisco.com/download/home/286319713/type
	EM7455 02.32.11.00	North America ATT: https://software.cisco.com/download/home/286311442/type
	EM7455 02.32.11.00	North American Sprint: https://software.cisco.com/download/home/286311455/type
	EM7455 02.33.03.00	North America Verizon: https://software.cisco.com/download/home/286311429/type
P-LTEAP18-GL	LM960 32.00.1x9	Generic: https://software.cisco.com/download/home/286324996/type
	LM960 32.00.1x9	North America: https://software.cisco.com/download/home/286324947/type
P-5GS6-GL	FN980 38.03.0202	https://software.cisco.com/download/home/286329300/type/
P-5GS6-R16SA-GL	EM9293 02.17.08.00	https://software.cisco.com/download/home/286334597/type

Supported software packages

This section provides information about the release packages associated with Cisco ESR6300 Router.

For latest software downloads, see the Software Download page.

IOS XE 26.1.2

Table 3. Software packages for Cisco ESR6300 Router, IOS XE 26.1.2

© 2026 Cisco and/or its affiliates. All rights reserved.

Image type	Filename
Universal	c6300-universalk9.26.01.02.SPA.bin

IOS XE 26.1.1

Table 4. Software packages for Cisco ESR6300 Router, IOS XE 26.1.1

Image type	Filename
Universal	c6300-universalk9.26.01.01.SPA.bin

Port Naming Conventions

This section shows the names of the ports on Cisco ESR6300 Series routers.

Table 5. Naming Conventions on Cisco ESR6300 Series Routers

Port	Naming Convention
Gigabit Ethernet combo port WAN Layer3	GigabitEthernet0/0/0 GigabitEthernet0/0/1
Gigabit Ethernet LAN Layer 2 ports	GigabitEthernet0/1/0 GigabitEthernet0/1/1 GigabitEthernet0/1/2 GigabitEthernet0/1/3
Cellular Interface	Cellular0/3/0 Cellular0/3/1
USB Port	usbflash0: (IOS and ROMMON)

Related resources

Table 6. Related resources

Document	Description
Cisco IOS XE	Provides information about products supported by Cisco IOS XE.
Cisco ESR6300 Embedded Series Router	Provides information about Cisco ESR6300 Embedded Series Router.
Cisco Industrial Routers and Industrial Wireless Access Points Antenna Guide	Provides information about Cisco Industrial Routers and Industrial Wireless Access Points.
Cisco IOS XE 26.x	Provides information about Cisco IOS XE 26 software.

© 2026 Cisco and/or its affiliates. All rights reserved.

Document	Description
Cisco SD-WAN	Provides information about Cisco SD-WAN routers.
Cisco IoT Field Network Director	Provides information about Cisco IoT Field Network Director.
Cisco Industrial Network Director	Provides information about Cisco Industrial Network Director.
Cisco Industrial IoT Licensing page	Provides information about Smart Licensing Using Policy solutions and their deployment on IOS XE routers.
Cisco Support	You can submit a service request here.
Cisco TAC	Provides the most up-to-date detailed troubleshooting information.
Cisco Feature Navigator	Use CFN to browse Cisco products and find relevant features and licenses. It allows you to compare platforms, determine common features between products, and identify unique product features. The CFN also has a tab that provides a MIB Locator.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

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: https://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.