Release Notes for Cisco Catalyst IR1101, IR1800, IR8140, and IR8340 Routers, IOS-XE 26.1.x

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

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

Cisco Catalyst Rugged Series Routers, IOS-XE 26.1.x

Cisco IOS-XE 26.1.x introduces new features for the Cisco Catalyst Rugged Series Routers. Key features include UTD support, device sensors, timing support for 1588-2017 boundary clock, CoA support, segment routing over IPv6, power over Ethernet plus support, and send a UID to identify the unique source when sending GPS coordinates data.

New software features

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

IOS-XE 26.1.1

Table 1. New software features for Cisco Catalyst Rugged Series 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 information, see Resilient Infrastructure IOS XE Security Warnings Reference.
Operational efficiency	UTD Support on IR8140	You can now leverage Unified Threat Defense (UTD), Cisco's premier network security solution, to access a comprehensive suite of security features—including Enterprise Firewall, IPS/IDS, Advanced Malware Protection, URL Filtering, and DNS Security—for enhanced protection across your network. For more information, see Cisco Catalyst IR8140 Heavy Duty Series Router

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

Product Impact	Feature	Description
		Software Configuration Guide Supported device: IR8140
Better visibility	Device Sensor on IR8340	You can now use the device sensor network feature to gather raw endpoint data from network devices using protocols such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Dynamic Host Configuration Protocol (DHCP), DHCP version 6, and multicast DNS (mDNS). For more information, see Cisco Catalyst IR8340 Rugged Series Router Software Configuration Guide, Cisco IOS-XE Release 26.1.x Supported device: IR8340
Software Reliability	Segment Routing over IPv6	SRv6 is now officially supported on IR1101 router. For more information, see Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide Supported device: IR1101
Enhanced security and flexibility	CoA Support on IR1800	You can now leverage Change of Authorization (CoA), a network policy mechanism which is used for RADIUS authentication. It modifies session attributes for active authentication, authorization, and accounting sessions. For more information, see Cisco Catalyst IR1800 Rugged Series Router Software Configuration Guide Supported devices: IR1800
Greater Control	Send a UID to Identify the Unique Source When Sending GPS Coordinates Data	You can now configure Cisco routers to send a Unique Identifier (UID) when streaming NMEA GPS sentences over UDP. UID streaming is supported from both the Dead Reckoning (DR) module and cellular modems with GNSS capabilities, allowing each router to be uniquely identified in GPS data processing systems. For more information, see Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide and Cisco Catalyst IR1800 Rugged Series Router Software Configuration Guide Supported devices: IR1101 and IR1800
Upgrade	PoE+ Support on Cisco Catalyst IR8140 Router	You can use Cisco Catalyst IR8140 Heavy Duty Series Routers to provide up to 30 W of power per port to connected devices over Ethernet. For more information, see Cisco Catalyst IR8140 Heavy Duty Series Router Software Configuration Guide Supported device: IR8140
Ease of Use	Timing Support for 1588-2017 Boundary Clock on IR8340	Cisco Catalyst IR8340 Rugged Series Router now supports Power Profile-2017 in Boundary clock. For more information, see Cisco Catalyst IR8340 Rugged Series Router Software Configuration Guide, Cisco IOS-XE Release 26.1.x Supported device: IR8340
Greater Control	Support for 20K router instances	This release introduces updated computing resource recommendations for Cisco Catalyst SD-WAN Control components. These specifications are designed to support Industrial IOT deployments of up to 20,000 devices, ensuring stability, high availability, and optimal performance across the

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

Product Impact	Feature	Description
		control plane. For more information, see Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide.

New hardware features

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

IOS-XE 26.1.1

There are no new hardware features in this release.

Change in behavior

Syslog Warning on Reload for SSH Hostkeys: After a device reload, you may observe a syslog warning indicating insufficient key length for SSH hostkeys, even if a strong RSA or EC key is configured.

Note:

- There is no change in behavior for greenfield deployments, as the feature is disabled by default. However, if insecure commands are executed, the system automatically enables insecure mode.
- 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 hostkey has been provisioned on the device with insufficient key length.

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

Submode: 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 hostkey has been provisioned on the device with insufficient key length.

Remediation: Please provision an SSH EC hostkey with minimum modulus size of 384 bits for enhanced security.

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

Submode: exec.

Parent CLI: Not Applicable.

Ignore these warnings if you have already configured a strong key. 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.

Resolved issues

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

This table lists the resolved issues in this specific software release.

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.
- To search for a documented Cisco product issue, type in the browser: <bug number> in Cisco.com

IOS-XE 26.1.1

Table 2. Resolved issues for Cisco Catalyst Rugged Series Routers, IOS-XE 26.1.1

Bug ID	Description
CSCwq60670	NVRAM Header Corruption on Power Cycle
CSCws66114	IR8340 is failing upgrade from 17.15.1a to 17.15.4 using install commands
CSCwn98622	Hardware removal & insertion SNMP traps received after soft reload-Misleading router actual activity
CSCwo91346	IR1101 WANMON failing to reach level 2 recovery
CSCwo73978	Disappearance of band selection configuration from cellular controller after a router reload
CSCwp90680	IR1101 not completing ARP for Emerson FB-3000.
CSCwm92704	IR8340 & IE9320 redbox forwarding multiple primary announce messages to SAN
CSCwp00808	IRM-NIM-RS232 module Serial interface stops transmitting TCP raw socket traffic
CSCwp15793	TOD not synced after hard power cycle
CSCwp13058	Unintended BBU fw upgrade when miscommunication occurs between IOS and BB fw
CSCwt01182	IR8340: PTP from UTC to TAI on an IR8340 is not working
CSCwo31561	“Error in showing license Information" when " show license rum id all" is executed

Open issues

You can also access

the open caveats for this release through the Cisco Bug Search Tool.

This table lists the open issues in this specific software release.

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.
- To search for a documented Cisco product issue, type in the browser: <bug number> in Cisco.com

IOS-XE 26.1.1

Table 3. Open issues for Cisco Catalyst Rugged Series Routers, IOS-XE 26.1.1

Bug ID	Description
CSCwr98904	WIFI6 module loses configuration with IR1821 reload.
CSCwt05807	Telemetry sends incorrect data when sensor's reading is negative
CSCwt42374	IOx app can exhaust router storage via core dumps & IOx app disk reservation not enforced

Known issues

IOS-XE 26.1.1

There are no known issues in this release.

Compatibility

This section lists compatibility information on Cellular Module Modem Firmware, OEM/PRI and it lists the latest modem firmware available for each of the modems used by the Cisco IoT routers. 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 should 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 4. Cellular Module Modem Firmware

Cellular Module	Modem and Firmware version	Software download link
P-5GS6-GL	FN980 38.03.0202	https://software.cisco.com/download/home/286329300/type/
P-LTEAP18-GL IRMH-LTEAP18-GL	LM960 32.00.1x9	Generic: https://software.cisco.com/download/home/286324996/type North America:

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

Cellular Module	Modem and Firmware version	Software download link
		https://software.cisco.com/download/home/286324947/type
P-LTEA-EA IRMH-LTEA-EA	Generic and Europe: EM7455 02.39.00.00 Canada, North America ATT, North American Sprint: EM7455 02.32.11.00 North America Verizon: EM7455 02.33.03.00	Generic: https://software.cisco.com/download/home/286308426/type Europe: https://software.cisco.com/download/home/286308426/type Canada: https://software.cisco.com/download/home/286319713/type North America ATT: https://software.cisco.com/download/home/286311442/type North American Sprint: https://software.cisco.com/download/home/286311455/type North America Verizon: https://software.cisco.com/download/home/286311429/type
P-LTEA-LA IRMH-LTEA-LA	Generic: EM7430 02.38.00.00 Australia Telstra EM7430 02.33.03.00 Japan: EM7430 02.38.00.00	Generic: https://software.cisco.com/download/home/286308413/type Australia Telstra: https://software.cisco.com/download/home/286311403/type Japan: https://software.cisco.com/download/home/286311416/type
P-LTE-VZW	WP7601 02.37.0x.00	https://software.cisco.com/download/home/286322139/type
P-LTE-US	WP7603 02.37.0x.00	https://software.cisco.com/download/home/286322143/type
P-LTE-JN	WP7605 02.28.03	https://software.cisco.com/download/home/286322156/type
P-LTE-GB	WP7607 02.37.03.05	https://software.cisco.com/download/home/286322147/type

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

Cellular Module	Modem and Firmware version	Software download link
P-LTE-IN	WP7608 02.28.03	https://software.cisco.com/download/home/286322152/type
P-LTE-AU	WP7609 02.28.03	https://software.cisco.com/download/home/286323720/type
P-LTE-MNA	WP7610 02.37.03.05	https://software.cisco.com/download/home/286324942/type
P-LTEA7-NA	EM7411 01.14.24.00	https://software.cisco.com/download/home/286333933/type
P-LTEA7-EAL	EM7421 01.14.22.00	https://software.cisco.com/download/home/286333937/type
P-LTEA7-JP	EM7431 01.14.22.00	https://software.cisco.com/download/home/286333939/type
P-5GS6-R16SA-GL	EM9293 02.17.08.00	https://software.cisco.com/download/home/286334597/type
P-LTE-450	Not applicable v1.3.0	Contact Intelliport for the software download link (info@intelliport.hu)

Supported software packages

This section provides information about the release packages associated with Cisco Catalyst Rugged Series Routers.

For latest software downloads, see the Software Download page.

Note: NPE stands for No Payload Encryption.

Table 5. Software packages for Cisco Catalyst Rugged Series Routers, IOS-XE 26.1.x

Router	Image type	Filename
IR1101	Universal	ir1101-universalk9.26.01.01.SPA.bin
IR1800	Universal	ir1800-universalk9.26.01.01.SPA.bin
	UTD Engine for Cisco IR1800	secapp-utd.17.13.01a.1.0.2_SV3.1.67.0_XE17.13.x86_64.tar

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

Router	Image type	Filename
IR8100	Universal	ir8100-universalk9.26.01.01.SPA.bin
	UTD Engine for Cisco IR8100	secapp-utd.26.01.01.1.0.1_SV3.3.5.0_XE26.1.aarch64.tar
IR8340	Universal	ir8340-universalk9.26.10.01.SPA.bin
	UTD Engine for Cisco IR8340	secapp-utd.26.01.01.1.0.1_SV3.3.5.0_XE26.1.x86_64.tar

Related resources

Table 6. Related resources

Document	Description
Cisco IOS-XE	Provides products supported by Cisco IOS-XE.
Cisco Catalyst IR1101 Rugged Series Router Cisco Catalyst IR1800 Rugged Series Router Cisco Catalyst IR8140 Heavy Duty Series Router Cisco Catalyst IR8340 Rugged Series Router	Provides data sheet for the specified routers.
Cisco Industrial Routers and Industrial Wireless Access Points Antenna Guide	Provides descriptions and installation instructions for wireless antennas supported on the Cisco Industrial Series Routers and Industrial Wireless Access Points.
Cisco SD-WAN	Provides information about SD-WAN releases and resources.
Cisco IoT Field Network Director	Provides information about Cisco IoT Field Network Director releases and resources.
Cisco Industrial Network Director	Provides information about Cisco Industrial Network Director releases and resources.
Smart Licensing Using Policy on the Cisco Catalyst IR1101, IR1800, IR8140, and IR8340 Routers or the Cisco Industrial IoT Licensing	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 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.

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.