Release Notes for Cisco 8300 Series Secure Routers, Release 17.15.x

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

Cisco 8300 Series Secure Routers, Release 17.15.x 3
New hardware features 3
Resolved issues 3
Open issues 6
Compatibility 6
Related resources 7
Legal information 7

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco 8300 Series Secure Routers, Release 17.15.x

Cisco IOS XE 17.15.3a is the first release for the Cisco 8300 Series Secure Routers in the Cisco IOS XE 17.15.x release series.

Cisco 8300 Series Secure Routers deliver secure networking simplified. Powered by the all-new secure networking processor and the unified Cisco secure networking platform, the Cisco 8300 Series Secure Routers deliver robust, platform-level security, advanced performance engineering thorough routing and SD-WAN, and on-premises, infrastructure-as-code, or cloud management flexibility that enables businesses to seamlessly scale and grow. Each class of secure routers is designed to deliver risk reduction, enhanced reliability, and future readiness.

Cisco 8300 Series Secure Routers are engineered for large branch locations and provide scalable, high-throughput connectivity with embedded platform-level security. With hardware-native assurance, post-quantum cryptography, and unified infrastructure as code, the Cisco 8300 Series enables large branches to support bandwidth-intensive applications and evolving threat landscapes with confidence.

For information on the hardware features supported on the Cisco 8300 Series Secure Routers, refer to the Cisco 8300 Series Secure Routers datasheet.

New hardware features

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

New hardware features for Cisco IOS XE 17.15.3a

Table 1. New hardware features for Cisco 8300 Series Secure Routers, Release 17.15.3a

Feature	Description
Cisco 8300 Series Secure Routers.	From Cisco IOS XE17.15.3a, Cisco Secure Series Routers are available in these models: C8375-E-G2

Resolved issues

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

Note: This software release may contain open bugs first identified 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> site:cisco.com.

Resolved issues in Cisco IOS XE 17.15.6

Table 2. Resolved issues for Cisco 8500 Series Secure Routers, Release 17.15.6

Bug ID	Description
CSCws96978	Policy download fails after modifying SGACL on ISE and pushing using COA.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwu02602	DBAL EVENTS crash seen while trying to push config group to device in SDWAN and SD-Routing.
CSCwt09078	Enhanced logging for file system read failure.
CSCwq54131	Device crash when configuration replace is performed using VTY session.
CSCwo90776	Messages in MQIPC buffer queue may not get drained during connrent and eagain conditions in race condition.
CSCws68876	Unexpected reload due to ISSU client ISSU Virtual-Template Client.
CSCwu04279	System instability and potential service disruption after invalid GPM load.
CSCwr77437	Seg Fault in HTTP CORE potentially due to SDAVC-related Corruption.
CSCwt35490	Config-Sync: Log the errno value for all file open operation failure.
CSCwq82256	Already committed SMU packages are removed from R0 on SMU activation failure later.
CSCwt00254	Anonymous memory leak due to missing SSL async FD deselect in WebAuth.
CSCwt86654	IKEv2 process crash caused by stack buffer overflow during AnyConnect EAP credential parsing.
CSCwt29087	After performing forced switchover and pushing COA for SGACL change, old SGACL is seen on switch.
CSCws66419	Unexpected Reload due to block overflow in RSA verification.
CSCwt69624	TCP application (LISP/BGP) can stuck in write blocked state forever.
CSCwt00262	OPSSL changes for SSL async job memory leak.
CSCwt87294	mDNS Cache-Flush behavior not consistent.
CSCwo26985	Wireless client authentication fails due to RADIUS client unable to parse Microsoft MPPE-Send-Key VSA; In another scenario, certificate reassembly may fail for retransmissions.

Resolved issues in Cisco IOS XE 17.15.5

Table 3. Resolved issues for Cisco 8300 Series Secure Routers, Release 17.15.5

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwp06956	NGFW Policy Deployment Fails Due to Long Rule Name
CSCwr03611	LWM " memory free low-watermark processor" value its changing itself after upgrade to 17.12
CSCwr83968	Unexpected Reload on device with Static NAT When Polling NAT Translation Data
CSCwq79503	Router May Reload Unexpectedly During Startup Due To Segmentation Fault
CSCwr19450	Stuck locally originates BGP EVPN type-2 route
CSCws30834	Device ignore the keepalive command under the SIG tunnel interface pushed by the vmanage
CSCwq29468	[XE BGP] BGP routes are advertised with 0 in AS PATH attribute when replacing ASN
CSCwr51490	DMVPN hub routers could experience an unexpected reload after tunnel down in specific timing scenario.
CSCwn18874	DMVPN spoke crashed at Process = NHRP
CSCwo14975	Memory Leak in DNS Proxy/SKA Triggers Unexpected Reloads
CSCwp67808	ZBFW Invalid Zone drops after upgrade to 17.15
CSCwr37828	BGP neighborship flap during configure replace
CSCwq22471	Device May Unexpectedly Reboot When Importing CA Chains
CSCwq26347	object-group service TCP port range
CSCwk55051	Device polaris_vconfd_cfgpull_t denials during config push trigger
CSCwm01063	Device May Reload During IP SLA Updates With Periodic Hostname Resolution
CSCwr19564	Stuck EVPN BGP type-2 local route and L2RIB route
CSCwo92849	ip community-list standard CLI template attach failure
CSCwo70548	Ping failure from VRRP backup to VRRP primary virtual address when enabling security policy
CSCwr83214	Device is sending lots of fib-updates alarms to vManage filling max alarms in vManage

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwp36696	IP aliases stuck in VRF even NAT statements removed
CSCwj24696	IPv6 ND HA Memory Leak from IPv6 NS on Mgmt port
CSCwp40010	RP Crash While Debugging IKEv2

Resolved issues in Cisco IOS XE 17.15.3a

There are no customer impacting bugs that were fixed in this release.

Open issues

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

Note: This software release may contain open bugs first identified 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> site:cisco.com.

Open issues in Cisco IOS XE 17.15.6

There are no customer impacting bugs that were identified for this release.

Open issues in Cisco IOS XE 17.15.5

Table 4. Open issues for Cisco 8300 Series Secure Routers, Release 17.15.5

Bug ID	Description
CSCws71815	Behaviour change for " ip dhcp use class" command on sdwan router
CSCws51814	Increased CPU Utilization Caused by BGP Scanner Process
CSCws75443	IPv6 neighbour table entries are not timing out causing High TCAM utilisation (no default timers configured).

Open issues in Cisco IOS XE 17.15.3a

Table 5. Open issues for Cisco 8300 Series Secure Routers, Release 17.15.3a

Bug ID	Description
CSCwm08691	Upgrade from 17.15 to 17.16, CRC error interwork with router.
CSCwo49208	EL3 Exception seen when remove Cessna with traffic running.

Compatibility

ROMMON compatibility matrix

The table lists the ROMMON releases supported in Cisco IOS XE 17.15.x releases.

© 2025 Cisco and/or its affiliates. All rights reserved.

Platforms	Cisco IOS XE Release	Minimum ROMMON Release supported for IOS XE	Recommended ROMMON Release supported for IOS XE
C8375-E-G2	17.15.3a	17.15(3.1r)	17.15(3.1r)

Upgrade ROMMON

To upgrade the ROMMON version of your device, use these steps:

1. Check the existing version of ROMMON by using **show rom-monitor r0** command. If you are installing Cisco IOS XE software on a new device, skip this step.
2. Review ROMMON Compatibility Matrix to identify the recommended version of ROMMON software for the device you plan to upgrade.
3. Go to https://software.cisco.com/# and download the ROMMON package file.
4. Copy the ROMMON file to flash drive:

   copy ftp://*username*:*password*@*IP address*ROMmon *package file* **flash:**
5. Upgrade the ROMMON package using the following command:

   upgrade rom-monitor filename bootflash:*ROMmon package name* **all**
6. Execute **reload** command to complete the ROMMON upgrade process.
7. Execute **show rom-monitor r0** command to ensure the ROMMON software is upgraded.

Related resources

- Hardware Installation Guide for Cisco 8300 Series Secure Routers
- Software Installation Guide for Cisco 8300 Series Secure Routers
- Cisco 8000 Series Secure Routers Licensing

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.