



# Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Cupertino 17.9.x

---

**First Published:** 2022-08-26

**Last Modified:** 2024-02-28

## Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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/c/en/us/about/legal/trademarks.html>. 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. (1721R)

## About Cisco ASR 1000 Series Aggregation Services Routers

The Cisco ASR 1000 Series Routers carry a modular yet integrated design, so network operators can increase their network capacity and services without a hardware upgrade. The routers are engineered for reliability and performance, with industry-leading advancements in silicon and security to help your business succeed in a digital world that's always on. The Cisco ASR 1000 Series is supported by the Cisco IOS XE Software, a modular operating system with modular packaging, feature velocity, and powerful resiliency. The series is well suited for enterprises experiencing explosive network traffic and network service providers needing to deliver high-performance services.




---

**Note** For more information on the features and specifications of Cisco ASR 1000 Series Routers, refer to the Cisco ASR 1000 Series Routers [datasheet](#).

For information on the End-of-Life and End-of-Sale Announcements for Cisco ASR 1000 Series routers, refer to the [ASR 1000 Series End-of-Life and End-of-Sale Notices](#).

---




---

**Note** Cisco IOS XE Cupertino 17.9.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Cupertino 17.9.x release series.

---




---

**Note** Starting from IOS XE 17.5, the following consolidated platforms (or with dual IOSd) will move to monolith packaging and will not enable upgrade/downgrade using separate packages:

- ASR 1001-X
  - ASR 1001-HX
  - ASR1002-X
  - ASR 1002-HX
- 

Instead, use the **install add file bootflash:<file name> activate commit** command to upgrade using a single image that combines all the separate packages improves the boot time.

Starting from IOS XE 17.6, the ISSU on Cisco ASR 1000 Series Aggregation Services Routers will migrate to an install workflow that provides step-by-step upgrade/downgrade commands.

The ISSU load version commands will be deprecated and these commands include:

- abortversion
- acceptversion
- checkversion

- commitversion
- config-sync
- image-version
- loadversion
- runversion.

Additionally, dual IOSd ISSU commands and Bundle mode ISSU workflows will also be disabled.



**Note** The In-Service Software Upgrade (ISSU) in ASR 1000 is being migrated to an install workflow that provides a step-by-step upgrade/downgrade. Starting from IOS-XE 17.6.1, the following items will be disabled:

- The ISSU load version command set including **issu loadversion**, **issu runversion**, **issu acceptversion**, and **issu commitversion**.
- Dual IOSd ISSU commands.
- Bundle mode ISSU workflow.

## Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see <https://www.cisco.com/c/en/us/support/web/field-notice-overview.html>.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from <https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories>.

## New and Changed Hardware Features

There are no new hardware features for this release.

## New and Changed Software Features in Cisco IOS XE 17.9.4a

There are no new features in this release. This release provides a fix for [CSCwh87343](#): Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see the Security Advisory: [cisco-sa-iosxe-webui-privesc-j22SaA4z](#).

## New and Changed Software Features in Cisco IOS XE 17.9.4

There are no new software features in this release.

## New and Changed Software Features for Cisco IOS XE 17.9.3a

Feature	Description
---------	-------------

<p>Support for broadband features and functionalities with DNA Network Advantage Tier 3 License</p>	<p>From Cisco IOS XE 17.9.3 release, the following functionalities and features are supported on ESP100-X &amp; ESP200-X platforms:</p> <ul style="list-style-type: none"> <li>• Layer 2 Tunnel Protocol Network Server (LNS)</li> <li>• Layer 2 Access Concentrator (LAC)</li> <li>• Broadband Network Gateway (BNG)</li> <li>• Intelligent Services Gateway (ISG)</li> <li>• Intelligent Wireless Access Gateway (iWAG).</li> <li>• PPP and IP sessions</li> </ul> <p>For more information, see:</p> <p><a href="#">Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide, Cisco IOS XE 17 - Broadband Scalability and Performance [Cisco IOS XE 17] - Cisco</a></p> <p><a href="#">Broadband Access Aggregation and DSL Configuration Guide, Cisco IOS XE 17 - Broadband Smart Licensing [Cisco IOS XE 17] - Cisco</a></p> <p><a href="#">Intelligent Wireless Access Gateway Configuration Guide - iWAG Scalability and Performance [Cisco ASR 1000 Series Aggregation Services Routers] - Cisco</a></p>
---	--

## New and Changed Software Features in Cisco IOS XE 17.9.2a

There are no new software features in this release.

## New and Changed Software Features for Cisco IOS XE 17.9.1a

Feature	Description
<a href="#">Asymmetric Lease for DHCPv4</a>	<p>This feature allows you to manage or change the lease renewal in a shorter period of time than the actual lease that is granted by the DHCP server. You can enable this using the <code>ip dhcp relay short lease</code> command on the server or relay agent.</p>
<a href="#">Displaying link and prefix cache, and ISIS LSP TLV neighbor</a>	<p>The <code>show isis node</code> command is updated to display information about link and prefix cache, and the <code>show isis lspgen tlv neighbor</code> command is introduced to display information about ISIS LSP TLV neighbors.</p>
<p>Increase ACE Scale Limit Per OGACL</p>	<p>This feature provides an increase in the ACE scale limit per ACL and OGACL as the current implementation of CACE has a total limit of only 64K entries. The scale for this feature is 1D and the scale information for OGACL is 3000 ACE entries per OGACL, 2400 OGs and 100 networks per OG.</p>

Feature	Description
Logging Destination IP Address and Port Details	The <b>ip nat settings log-destination</b> command is introduced in Carrier Grade Network Address Translation (CGN) mode to include the destination IP address and the destination port details in the add and delete HSL records.
Support for BGP additional paths with label-unicast unique mode	This enhancement introduces support for configuring BGP additional paths when label-unicast unique mode is configured.
Support for PFP with RIB Path	Previously, a separate PDP policy was created for every default IGP/RIB learned path. This implementation would eventually increase the number of policies and would not scale. From Cisco IOS XE 17.9.1, RIB path is supported for PFP. This feature enables you to configure forwarding class in a per flow policy using the RIB path option. Instead of configuring a per destination policy, the RIB option uses the IGP shortest path to the policy destination.
Support for Unicast-to-Multicast Destination Reflection	This feature introduces support for configuration of unicast-to-multicast destination reflection to facilitate unicast-to-multicast destination translation and unicast-to-multicast destination splitting. It also provides the capability for users to translate externally received unicast destination addresses to multicast addresses.
<b>Cisco Unified Border Element (CUBE) Features</b>	
CUBE: End-to-end Secure Calling for Courtesy Call Back and Unified Contact Center Survivability	With the Cisco Voice Portal (CVP) application, a caller may request an automatedcallback, rather than wait in a queue for an extended period. When an agent becomes available, CVP sends a request to place a call to the original caller. When the call is answered, the agent is connected. With this update, outbound calls over a secure SIP PSTN trunk are possible.
CUBE: Load Balancing for DNS SRV Host	This enhancement to the DNS session target feature, provides effective call distribution and load balancing of calls based on the preference, priority and availability of hosts provided in DNS SRV Resource Records. This feature further simplifies configuration by allowing effective call distribution with a single dial-peer.
CUBE: Options Ping for DNS SRV Hosts	Previously, CUBE (Local Gateway) had to be configured with separate dial-peers to monitor the availability of individual proxies used in services such as Webex Calling. To simplify this configuration, all targets resolved from a DNS SRV record may now be monitored using a common Options Ping policy defined for a single dial-peer. If a remote server becomes unresponsive, CUBE will busy out that destination, allowing calls to be sent to alternative destinations.
Transfer of Call Detail Records Using SFTP	Cisco IOS gateways can use FTP and now SFTP servers to transfer call accounting files.
<b>Programmability Feature</b>	
Pubd Restartability	The pubd process is restartable on all platforms in this release. Prior to this release, pubd was restartable only on certain platforms. On other platforms, to restart the pubd process, the whole device had to be restarted.

Feature	Description
<b>Smart Licensing Using Policy Features</b>	
New mechanism to send data privacy related information	<p>A new mechanism to send data privacy related information was introduced. This information is no longer included in a RUM report.</p> <p>If data privacy is disabled (<b>no license smart privacy {all hostname version}</b> command in global configuration mode), data privacy related information is sent in a separate sync message or offline file.</p> <p>Depending on the topology you have implemented, the product instance initiates the sending of this information in a separate message, or CSLU and SSM On-Prem initiates the retrieval of this information from the product instance, or this information is saved in an offline file.</p> <p>For more information, see <a href="#">license smart (global config)</a>.</p>
Hostname support	<p>Support for sending hostname information was introduced.</p> <p>If you configure a hostname on the product instance and disable the corresponding privacy setting (<b>no license smart privacy hostname</b> command in global configuration mode), hostname information is sent from the product instance, in a separate sync message or offline file.</p> <p>Depending on the topology you have implemented, the hostname information is received by CSSM, CSLU, and SSM On-Prem. It is then displayed on the corresponding user interface.</p> <p>For more information, see <a href="#">license smart (global config)</a>.</p> <p><b>Note</b> With the introduction of this enhancement, the hostname limitation which existed from Cisco IOS XE Amsterdam 17.3.2 to Cisco IOS XE Cupertino 17.8.x – is removed. In these earlier releases, hostname information is not sent or displayed on various licensing utilities (CSSM, CSLU, and SSM On-Prem).</p>

Feature	Description
RUM Report Throttling	<p>For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day.</p> <p>The affected topologies are: <i>Connected Directly to CSSM</i>, <i>Connected to CSSM Through CSLU</i> (product instance-initiated communication), <i>CSLU Disconnected from CSSM</i> (product instance-initiated communication), and <i>SSM On-Prem Deployment</i> (product instance-initiated communication).</p> <p>This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down that was caused by an excessive generation of RUM reports.</p> <p>You can override the reporting frequency throttling, by entering the <b>license smart sync</b> command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data.</p> <p>RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to <i>all</i> subsequent releases.</p>
Virtual Routing and Forwarding (VRF) Support	<p>On a product instance where VRF is supported, you can configure the <b>license smart vrf vrf_string</b> command and use a VRF to send licensing data to CSSM, or CSLU, or SSM On-Prem.</p> <p><b>Note</b> When using a VRF, the supported transport types are <b>smart</b> and <b>cslu</b> only.)</p> <p>For more information, see <a href="#">license smart (global config)</a></p>

## Resolved and Open Bugs for Cisco IOS XE 17.9.x

### Resolved Bugs for Cisco IOS XE 17.9.5a

Bug ID	Description
<a href="#">CSCwh22451</a>	Packets appeared out of order when using Embedded Packet Capture (EPC).
<a href="#">CSCwf89154</a>	EZMAN posted stats to APIs: Ingress and Egress Bytes counters suddenly jump for sub-interfaces.
<a href="#">CSCwh85803</a>	The MACsec session is in a secured state but stuck without sending any traffic.
<a href="#">CSCwf34341</a>	Device experiences a crash under @crypto_dev_proxy_ipc_ipsec_sa_crt_hdlr.
<a href="#">CSCwb79943</a>	Device ICMP replies should not be NATted.
<a href="#">CSCwi28781</a>	EPBR will generate an error when the policy is added and deleted multiple times.
<a href="#">CSCwe25815</a>	There is a crash due to DTL push/pop in the wait loop.
<a href="#">CSCwi21548</a>	EntSensorStatus is displaying as non-operational.

Bug ID	Description
<a href="#">CSCwh25168</a>	A CPLD upgrade failed error message is logged during ROMmon upgrade.
<a href="#">CSCwf51206</a>	In EVPN, BUM traffic is not flooded to the bridge domain interface.
<a href="#">CSCwh93257</a>	The device creates a crooked NAT entry if two or more IP phones from the NAT outside register to the same server.
<a href="#">CSCwh59064</a>	Depletion in the process memory pool/IOSd after enabling virtualization on the IOS-XE platform.
<a href="#">CSCwf99947</a>	Crash when modifying tunnel after running <b>show crypto</b> commands.
<a href="#">CSCwe29301</a>	AOM objects (FMAN_OBJ_ACL_REF) might be missing intermittently after MMA flapping.
<a href="#">CSCwh59411</a>	Device's fifty-gig port returns a link-flap err-disabled status when the peer device reloads or bounces.
<a href="#">CSCwh73350</a>	Router keeps crashing when processing a firewall feature.
<a href="#">CSCwf67564</a>	Device observes memory leak at process SSS Manager.
<a href="#">CSCwf23291</a>	<b>write</b> or <b>do write</b> saves configuration, but RSA keys/SSH are lost after reload.
<a href="#">CSCwc79115</a>	Policy commit failure notification and alarm from management software.
<a href="#">CSCwh06834</a>	Using special characters in the password while generating a token generates an invalid token.
<a href="#">CSCwh68508</a>	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
<a href="#">CSCvo01546</a>	NHRP reply processing may dequeue an unrelated request.
<a href="#">CSCwf82676</a>	CPU usage mismatch in <b>show sdwan system status</b> vs <b>show process CPU platform</b> .
<a href="#">CSCwf03193</a>	Device crash with crash info files generated with segmentation fault, process IPSEC key engine.
<a href="#">CSCwh08434</a>	OMP route is being advertised although the route is not available.
<a href="#">CSCwf26875</a>	Interface from Port-channel going to suspended status after applying <b>platform QoS port-channel-aggregate</b> .
<a href="#">CSCwf24164</a>	NetFlow stops working when flow monitor reaches cache limit in the device.
<a href="#">CSCwh63061</a>	Certification: Modem is showing 4 additional NR bands support - 1, 3, 7, and 28.
<a href="#">CSCwf65540</a>	Running more than 4 tests on network agent causes tracebacks on device running software in a docker container.
<a href="#">CSCwi28227</a>	NAT HSL logging vrf-filter not working.
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication.



Bug ID	Description
<a href="#">CSCwd17272</a>	UTD Packet drop due to fragmentation for ER-SPAN traffic.
<a href="#">CSCwe91898</a>	Environmental syslog is not appearing when the power cord is disconnected from the redundant power supply.
<a href="#">CSCwf55243</a>	Device is crashing while adding a trust point to the router.
<a href="#">CSCwh49644</a>	Compliance failure: Use of 3DES by IPSEC is denied.
<a href="#">CSCwh32386</a>	Unexpected reload on device due to critical process fman_fp_image.
<a href="#">CSCwe30514</a>	Device reboots with SSL proxy and UTD enabled.
<a href="#">CSCwh30377</a>	Device data plane crash in DNS security processing due to incorrect UDP length.
<a href="#">CSCwf34171</a>	<b>configure replace</b> command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
<a href="#">CSCwf96980</a>	Unexpected reboot after configuring application redundancy.
<a href="#">CSCwe64779</a>	Router software forced reset during high IPC congestion with IPsec.
<a href="#">CSCwh01425</a>	ITU channel configuration seems not working on the device.
<a href="#">CSCwh20577</a>	Crashed by TRACK Client thread at access to invalid memory location.
<a href="#">CSCwh00963</a>	Unable to migrate from ADSL to VDSL without reboot on the device.
<a href="#">CSCwh36801</a>	Crash in IP Input process during tunnel encapsulation.
<a href="#">CSCwh96415</a>	Can't disable DMVPN logging.
<a href="#">CSCwe85301</a>	Crypto process crash when PKI trust point is being deleted.
<a href="#">CSCwh20734</a>	Crypto process crash when PKI trust point is requested and deleted.
<a href="#">CSCwf71557</a>	IPv4 connectivity over PPP not restored after reload.
<a href="#">CSCwe97579</a>	Spoke-spoke cache refresh not working correctly in case of multiple cache entries for the same next hop.
<a href="#">CSCwf11394</a>	Debug log should mention port-hop and reason prior to DISTLOC.
<a href="#">CSCwf04866</a>	Keyman process crash seen while re-generating SSH key in the device.
<a href="#">CSCwh00332</a>	B2B NAT: When configuring IP NAT inside/outside on the interface, ACK/SEQ number abnormal.

### Open Bugs for Cisco IOS XE 17.9.5a

Bug ID	Description
<a href="#">CSCwi51234</a>	Unable to properly activate the Foundation Suite License on the device.

Bug ID	Description
<a href="#">CSCwf48967</a>	Failure to upgrade the FPGA version on the standby RP module.
<a href="#">CSCwi31110</a>	Traceback seen @_nhp_cache_delete due to a negative global cache count.
<a href="#">CSCwb55514</a>	Unexpected reboot of the ESP observed after enabling <b>platform qos port-channel-aggregate</b> .
<a href="#">CSCwf25735</a>	QoS with more than four remarks using set-cos does not work.
<a href="#">CSCwi34743</a>	Device's Tx queue depth is twice the q-limit, resulting in output discards.
<a href="#">CSCwe69338</a>	Duplicate telemetry updates for the environment-sensors path.
<a href="#">CSCwe84306</a>	Unable to configure the CIR rate higher than 67G.
<a href="#">CSCwi62239</a>	%IOSXE_MGMTVRF-3-INTF_ATTACH_FAIL error after configuring a loopback management VRF and then removing it.
<a href="#">CSCwi06843</a>	Endpoint tracker triggers a CPU usage spike.
<a href="#">CSCwe24491</a>	Static NAT with HSRP stops working after removing/adding standby.
<a href="#">CSCwi53951</a>	Packets with unicast MAC get dropped on a Port Channel Layer 2 sub-interface after a device reboot.
<a href="#">CSCwh80441</a>	Cosmetic issue causing distress to customers - Modem WCDMA 900 is displayed as Unknown.
<a href="#">CSCwh50510</a>	Device crash with segmentation fault (11), Process = NHRP when processing NHRP traffic.
<a href="#">CSCwi51326</a>	CPP CP SVR crash after decoding all packets to text (using L2 copy) on FIA trace.
<a href="#">CSCwi33168</a>	DSP reporting out-of-range utilization values in SNMP.
<a href="#">CSCwi10735</a>	Zone-Based Firewall drops transit packets due to 'Invalid ACK number'.
<a href="#">CSCwi08171</a>	Router might crash due to Cryptographic IKMP Process.
<a href="#">CSCwh12093</a>	Enable SOS/ROC feature for DSL.
<a href="#">CSCwf84960</a>	Device LED L remains green after port shutdown.
<a href="#">CSCwh18120</a>	IKEv2 - Diagnose feature is taking 11% CPU during session set up.
<a href="#">CSCwh41497</a>	DDNS update retransmission timer fails to work, resulting in a traceback error.
<a href="#">CSCwi04547</a>	Custom Application is marked as invalid.
<a href="#">CSCwi25737</a>	Router should discard IKE Notification messages with incorrect DOI.
<a href="#">CSCwi06404</a>	PKI crash after failing a CRL Fetch.

Bug ID	Description
<a href="#">CSCwh22414</a>	Warning and critical CPU utilization thresholds not recomputed when using data-plane-heavy mode.
<a href="#">CSCwi46997</a>	NAT Command not readable after reload.
<a href="#">CSCwi01046</a>	PoE module is not providing enough power to activate the ports after an unexpected reload.
<a href="#">CSCwc30418</a>	Segmentation fault observed in ikev2_dupe_delete_reason.
<a href="#">CSCwi16111</a>	IPv6 TCP adjust-mss not working after delete and reconfigure.
<a href="#">CSCwi63042</a>	Packet drops observed between LISP EID over GRE Tunnel.
<a href="#">CSCwi53306</a>	Unknown appID in ZBFW HSL log.
<a href="#">CSCwb25507</a>	CWMP: Add vendor specific parameter for NBAR protocol pack version.
<a href="#">CSCwi59202</a>	Device with SwitzerCC can't boot up.
<a href="#">CSCwi30529</a>	Template push fail when AAA authorization is set to local.
<a href="#">CSCwh91136</a>	Traffic not encrypted and dropped over IPSEC SVTI tunnel.
<a href="#">CSCwj04085</a>	Device has multiple crashes, with cpp_cp_svr crash pointing to cpp_sdwan_policy_vrf_delete.

### Resolved Bugs - Cisco IOS XE 17.9.4a

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwh87343</a>	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: <a href="#">cisco-sa-iosxe-webui-privesc-j22SaA4z</a>

### Open Bugs for Cisco IOS XE 17.9.4a

Bug ID	Description
<a href="#">CSCwd39257</a>	IOS-XE CPP crash when entering <b>no ip nat create flow-entries</b> .
<a href="#">CSCwe85301</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
<a href="#">CSCwf41492</a>	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
<a href="#">CSCwf52751</a>	CLI template fails to attach to device with error <b>access-denied</b> .
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication.
<a href="#">CSCwc86434</a>	Static NAT DIA inside static routes being advertised over OMP to remote sites.

Bug ID	Description
<a href="#">CSCwf34171</a>	<b>configure replace</b> command fails due to the <b>license udi PID XXX SN:XXXX</b> line on IOS-XE devices.
<a href="#">CSCwd17272</a>	UTD packet drop due to fragmentation for ER-SPAN traffic.
<a href="#">CSCwf41450</a>	Device reloads changing the resource profile.
<a href="#">CSCwf51206</a>	EVPN: BUM traffic is not flooded to bridge domain interface.
<a href="#">CSCvz82148</a>	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write configuration with same crypto value.
<a href="#">CSCwf24164</a>	Netflow stops working when flow monitor reaches cache limit in 8500L
<a href="#">CSCwe95072</a>	Unexpected reload due to memory corruption when modifying and access list.
<a href="#">CSCwf03193</a>	Device crash with crashinfo files were generated with segmentation fault, rocess IPSEC key engine.
<a href="#">CSCwf25735</a>	Device QoS more than four remark with set-cos not work.
<a href="#">CSCwf11394</a>	IOS XE - device debug log should mention port-hop and reason prior to DISTLOC.
<a href="#">CSCwf00276</a>	Packets with L2TP headers cause device to crash.
<a href="#">CSCwf55243</a>	Device is crashing while adding a trustpoint to the router.
<a href="#">CSCwe51910</a>	SNMP ifindex persist does not work.
<a href="#">CSCwd61988</a>	Output packet bytes calculation biase when we enable QoS on port channel.
<a href="#">CSCwf60120</a>	Static NAT entry gets deleted from running config; but remains in startup config.
<a href="#">CSCwf48967</a>	Failure to upgrade FPGA version to standby RP module.
<a href="#">CSCwf47789</a>	dot3StatsDuplexStatus gives unknown for tengig and gig interfaces.
<a href="#">CSCwe25815</a>	Crash due to DTL push/pop on wait loop.
<a href="#">CSCwe69338</a>	Duplicate telemetry updates for environment-sensors path.
<a href="#">CSCwe84306</a>	Unable to configure CIR rate higher then 67G.

#### Resolved Bugs for Cisco IOS XE 17.9.4

Bug ID	Description
<a href="#">CSCwf48808</a>	Stale client routes stuck in RIB on flex server.
<a href="#">CSCwe93905</a>	NAT ALG is changing the call-ID within SIP message header causing calls to fail.
<a href="#">CSCwf02225</a>	Device freezes for <b>show SDWAN</b> commands.
<a href="#">CSCwe24210</a>	SNMP MIB does not show correct firmware version for device LTE module.

Bug ID	Description
<a href="#">CSCwe18124</a>	MACsec remains marked as SECURED, but the traffic stops working randomly.
<a href="#">CSCwe25076</a>	ALG breaks NBAR recognition impacting application firewall performance.
<a href="#">CSCwd87195</a>	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.
<a href="#">CSCwf08698</a>	Device crashes unexpectedly due to a fault in the 'TLSCLIENT_PROCESS'.
<a href="#">CSCwd34941</a>	NAT configuration with no-alias option is not preserved after reload.
<a href="#">CSCwf47796</a>	NHRP cache entries flood matching a /32 default route.
<a href="#">CSCwf09758</a>	Crashes while importing big CRL file into switch.
<a href="#">CSCwe41946</a>	DTMF is failing through IOS MTP during call on-hold.
<a href="#">CSCwe18058</a>	Unexpected reload with IPS.
<a href="#">CSCwe12194</a>	Auto-Update cycle incorrectly deletes certificates.
<a href="#">CSCwd49309</a>	Crash seen on device with traffic pointing to segfault in coff handler.
<a href="#">CSCwe33793</a>	Memory allocation failure with extended antireplay enabled.
<a href="#">CSCwe66318</a>	NAT entries expire on standby router.
<a href="#">CSCwe31471</a>	Segmentation fault in device PB rx when per-tunnel QoS config is withdrawn.
<a href="#">CSCwd59722</a>	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
<a href="#">CSCwe70374</a>	Device Punt-Policer is not configurable.
<a href="#">CSCwe20008</a>	[LTE] SNMP MIB OID changing its last index.
<a href="#">CSCwf47563</a>	Device is crashing after importing the trustpoint with rsakeypair.
<a href="#">CSCwe37123</a>	Device uses excessive memory when configuring ACLs with large object groups.
<a href="#">CSCwd73783</a>	Observed qfp-ucode-wlc crash.
<a href="#">CSCwe39011</a>	GARP on port up/up status from device is not received by remote peer device.
<a href="#">CSCwf39490</a>	MCID (Malicious Call Identification) gets broken due to custom prefix setting under STCAPP FAC.
<a href="#">CSCwe19084</a>	NAT: Traffic is not translated to the same global address though PAP is configured.
<a href="#">CSCwe69783</a>	Device can lose its configuration during a triggered resync process if lines are in an off-hook state.
<a href="#">CSCwe89404</a>	No way audio when using secure hardware conference with secure endpoints.
<a href="#">CSCwe41234</a>	VMWI race condition causes no ringing for analog phones.

Bug ID	Description
<a href="#">CSCwa96399</a>	Configuring <b>entity-information</b> xpath filter causes syslogs to print, does not return data.
<a href="#">CSCwc89823</a>	Router crashes due to CPUHOG when walking Cisco Flash MIB @snmp_platform_get_flash_file_info.
<a href="#">CSCwe32862</a>	Router IOS-XE crash while executing AES crypto functions.
<a href="#">CSCwf37888</a>	Device Packet Duplication: Duplicate packets are counted on Primary Tunnel Interface Statistics.
<a href="#">CSCwd68994</a>	ISAKMP profile doesn't match as per configured certificate maps.
<a href="#">CSCwd35047</a>	Failed to ping gateway while configuring <b>SharedLOM</b> with console , tel interface until router reload.
<a href="#">CSCwd49177</a>	ISG: L2-connected subscriber. IPv6 prefix delegation is not reachable when packet are switched.
<a href="#">CSCwe22838</a>	ARP is not completing on interface having CISCO-OPLINK SFP.
<a href="#">CSCwe80684</a>	QFP Ucode crash when clearing MACs under BD in EVPN scenario.
<a href="#">CSCwe12090</a>	No error log generated when EVC/bridge-domain reaches maximum MAC learning limit on device.
<a href="#">CSCwe22353</a>	IpFormatErr drops on device when bridge-domain/EVC MAC learning limit is exhausted.
<a href="#">CSCwd93401</a>	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM.
<a href="#">CSCwd81813</a>	<b>startup-config</b> not parsed correctly after upgrading.
<a href="#">CSCwe16371</a>	Device going in disabled state after <b>hw-module &lt;slot&gt; reload</b> .
<a href="#">CSCwf45769</a>	Ingress and Egress bytes counters can suddenly increase and are not accurate for sub-interfaces.

### Open Bugs for Cisco IOS XE 17.9.4

Bug ID	Description
<a href="#">CSCwd39257</a>	IOS-XE CPP crash when entering <b>no ip nat create flow-entries</b> .
<a href="#">CSCwe85301</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
<a href="#">CSCwf41492</a>	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
<a href="#">CSCwf52751</a>	CLI template fails to attach to device with error <b>access-denied</b> .
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication.

Bug ID	Description
<a href="#">CSCwc86434</a>	Static NAT DIA inside static routes being advertised over OMP to remote sites.
<a href="#">CSCwf34171</a>	<b>configure replace</b> command fails due to the <b>license udi PID XXX SN:XXXX</b> line on IOS-XE devices.
<a href="#">CSCwd17272</a>	UTD packet drop due to fragmentation for ER-SPAN traffic.
<a href="#">CSCwf41450</a>	Device reloads changing the resource profile.
<a href="#">CSCwf51206</a>	EVPN: BUM traffic is not flooded to bridge domain interface.
<a href="#">CSCvz82148</a>	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write configuration with same crypto value.
<a href="#">CSCwf24164</a>	Netflow stops working when flow monitor reaches cache limit in 8500L
<a href="#">CSCwe95072</a>	Unexpected reload due to memory corruption when modifying and access list.
<a href="#">CSCwf03193</a>	Device crash with crashinfo files were generated with segmentation fault, rocess IPSEC key engine.
<a href="#">CSCwf25735</a>	Device QoS more than four remark with set-cos not work.
<a href="#">CSCwfl11394</a>	IOS XE - device debug log should mention port-hop and reason prior to DISTLOC.
<a href="#">CSCwf00276</a>	Packets with L2TP headers cause device to crash.
<a href="#">CSCwf55243</a>	Device is crashing while adding a trustpoint to the router.
<a href="#">CSCwe51910</a>	SNMP ifindex persist does not work.
<a href="#">CSCwd61988</a>	Output packet bytes calculation biase when we enable QoS on port channel.
<a href="#">CSCwf60120</a>	Static NAT entry gets deleted from running config; but remains in startup config.
<a href="#">CSCwf48967</a>	Failure to upgrade FPGA version to standby RP module.
<a href="#">CSCwf47789</a>	dot3StatsDuplexStatus gives unknown for tengig and gig interfaces.
<a href="#">CSCwe25815</a>	Crash due to DTL push/pop on wait loop.
<a href="#">CSCwe69338</a>	Duplicate telemetry updates for environment-sensors path.
<a href="#">CSCwe84306</a>	Unable to configure CIR rate higher then 67G.
<a href="#">CSCwh60848</a>	CUBE - SIP Message Queuing Fails to Resume Transmission

### Resolved Bugs for Cisco IOS XE 17.9.3a

Bug ID	Description
<a href="#">CSCwd45402</a>	MSR Unicast-To-Multicast not working if DST and SRC are the same in Service Reflect configuration.

Bug ID	Description
<a href="#">CSCwd90168</a>	Unexpected reload after running <b>show voice dsp</b> command while an ISDN call disconnects.
<a href="#">CSCwd16559</a>	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table.
<a href="#">CSCwd79089</a>	Device-L controller crash when sending full line rate of traffic with >5 Intel AX210 stations,
<a href="#">CSCwc27307</a>	Service engine YANG support for ZBFW.
<a href="#">CSCwd16664</a>	GetVPN long SA - GM re-registration after encrypting 2^32-1 of packets in one IPSEC SA.
<a href="#">CSCwd81357</a>	QoS classification not working for DSCP or ACL + MPLS EXP.
<a href="#">CSCwd89338</a>	Clear ISG existing lite-session upon reception of DHCP packet for same client.
<a href="#">CSCwc99823</a>	FMAN crash seen in SGACL@ fman_sgacL_calloc.
<a href="#">CSCwc78021</a>	Standby WLC crash @ fman_acl_remove_default_ace.
<a href="#">CSCwd25107</a>	Interface VLAN placed in "shutdown" state when configured with <b>ip address pool</b> .
<a href="#">CSCwd61255</a>	Data plane crash on device when making per-tunnel QoS configuration changes with scale
<a href="#">CSCwe01015</a>	IKEv2/IPSec - phase 2 rekey failing when peer is behind NAT.
<a href="#">CSCwd03869</a>	CEF DPI load-balancing causes out of order packets.
<a href="#">CSCwc65697</a>	vCube crashing and restarting during call flow with new image.
<a href="#">CSCwd84599</a>	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
<a href="#">CSCwc88791</a>	DSL: erroneous atm interface counter at DSL retraining.
<a href="#">CSCwe03614</a>	CWMP : MAC address of ATM interface is not included in inform message.
<a href="#">CSCwd38943</a>	GETVPN: KS reject registration from a public IP.
<a href="#">CSCwd06372</a>	Unconditional excessive logging in EoGRE tunnel error handling case.
<a href="#">CSCvy14316</a>	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M).
<a href="#">CSCwd85580</a>	Device unexpected reload after set <b>ospfv3 authentication null</b> command.
<a href="#">CSCwd33202</a>	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface.
<a href="#">CSCwd06923</a>	Stale IP alias left after NAT statement got removed.
<a href="#">CSCwd47123</a>	ISG uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply.



Bug ID	Description
<a href="#">CSCwd72312</a>	GETVPN: Traffic drops seen on GM after rekey installing policies on image.
<a href="#">CSCwc14688</a>	Single WAN Interface subslot 0/0 timing.
<a href="#">CSCwe53849</a>	Observed crash in CPP, UCode & FMAN while upgrading to with crypto module present.
<a href="#">CSCwd07516</a>	Memory leak under linux_iosd-imag related to SNMP.

### Open Bugs for Cisco IOS XE 17.9.3a

Bug ID	Description
<a href="#">CSCwd39257</a>	IOS-XE CPP crash when entering <b>no ip nat create flow-entries</b> .
<a href="#">CSCwd63783</a>	Memory leak caused router reload.
<a href="#">CSCwe19084</a>	NAT: Traffic is not translated to the same global address though PAP is configured.
<a href="#">CSCwe09805</a>	OID for SNMP monitoring of DSP resources are not working as expected.
<a href="#">CSCwe25076</a>	ALG breaks NBAR recognition impacting application firewall performance.
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication.
<a href="#">CSCwe24491</a>	Static NAT with HSRP stops working after removing/adding standby.
<a href="#">CSCwd17272</a>	UTD packet drop due to fragmentation for ER-SPAN traffic.
<a href="#">CSCwe32862</a>	Router IOS-XE crash while executing AES crypto functions.
<a href="#">CSCwe07055</a>	Device frequent reloads.
<a href="#">CSCwe28468</a>	Device always fails to push any template to device if device is running in FIPS mode.
<a href="#">CSCwd68994</a>	Unable to match on customer profile based on certificate-map.
<a href="#">CSCwe06327</a>	PFP policy in SRTE, RIB resolution in FC bring down ipsec tunnel interface- stuck at linestate down.
<a href="#">CSCwe38732</a>	IP CEF load sharing command is being changed by the device.
<a href="#">CSCwd34941</a>	NAT configuration with no-alias option is not preserved after reload.
<a href="#">CSCwe37184</a>	Device seeing out of service on switch modules when using with new DC power supply.
<a href="#">CSCwh60848</a>	CUBE - SIP Message Queuing Fails to Resume Transmission

## Resolved Bugs for Cisco IOS XE 17.9.2a

Bug ID	Description
<a href="#">CSCwc21739</a>	NAT not requesting further for low ports after initial allocation when CLI knob reserved-ports set.
<a href="#">CSCwc39012</a>	Crash saving tracelogs after Too many open files error.
<a href="#">CSCwc37320</a>	RP switchover causes linecard NFS mount failure resulting in memory leak.
<a href="#">CSCwc03478</a>	VTCP does not support L2 correctly.
<a href="#">CSCwc82140</a>	QFP crash when ZBFW configuration features log dropped-packets configuration.
<a href="#">CSCwd12591</a>	Device ucode crash during FW classification, session frees.
<a href="#">CSCwc99668</a>	Routes added by IKEv2 getting deleted at responder.
<a href="#">CSCwc23077</a>	Firewall drop seen stating FirewallL4 seen on device.
<a href="#">CSCwc78528</a>	DSPware 60.1.1 release targeting throttle.
<a href="#">CSCwc44851</a>	Bootstrap failing on device.
<a href="#">CSCwc96444</a>	Device is not programming correct next-hop for unicast prefix with multicast config present.
<a href="#">CSCwc49715</a>	Carsh @ UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps, having PPPoe with cwpmp configs.
<a href="#">CSCwd06118</a>	IKEv2 Cert-based IPSEC not working between IOS-XE and AWS.
<a href="#">CSCwb52324</a>	Device unexpected reload due to QFP ucode crash.
<a href="#">CSCwc43794</a>	Device VRF+NAT Outside Source Static - Drop packets during FTP (Active-mode) execution.
<a href="#">CSCwc77183</a>	Packet duplication is causing drops in payment transactions.
<a href="#">CSCwc20170</a>	Device reloads unexpectedly due to critical FTMD fault when VRF configuration is pushed.
<a href="#">CSCwb89958</a>	Unified Policy HSL not sending properly NBAR application information.
<a href="#">CSCwc89328</a>	Multiple devices experienced crashes every 4-5 min.
<a href="#">CSCwc52538</a>	Flows are not distributed and load-balanced evenly and consistently.
<a href="#">CSCwc45950</a>	ZBFW self zone policy drops ssh session on Mgmt-intf 512 ports.
<a href="#">CSCwb90252</a>	Automatically freeing up filesystems stale image or recovered folder (lost+found).
<a href="#">CSCwc79145</a>	Throughput degrades when Local TLOC specified in Data Policy goes down.
<a href="#">CSCwc32595</a>	BFD sessions remains down if interface flap form up/down/up.

Bug ID	Description
<a href="#">CSCwb65396</a>	CLI template push fails with error: 'Error: on line 48: line-mode single-wire line 0'.
<a href="#">CSCvz91309</a>	Crash due to IOSXE-WATCHDOG due to management port traffic storm.
<a href="#">CSCvz89354</a>	Router running crashes due to CPUHOG when walking cisco flash MIB.
<a href="#">CSCwc39865</a>	Subscriber session getting stuck and needs clearing it manually.
<a href="#">CSCwb48953</a>	Device speed test failing with Device Error: Speed test in progress.
<a href="#">CSCwd11365</a>	Needs cert update - Azure CGW creation fails due to NVA provisioning failure.
<a href="#">CSCwc72923</a>	ERROR info: Router configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt.
<a href="#">CSCwc84967</a>	Intermittent double DTMF due to changing timestamp on a DTMF event.
<a href="#">CSCwb08057</a>	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
<a href="#">CSCwc29629</a>	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication.
<a href="#">CSCwd13352</a>	SSH from device getting closed after update.
<a href="#">CSCwc77177</a>	BFD and control packets are dropped when ACL is applied on gigi to which loopback is bind.
<a href="#">CSCwc68132</a>	SIG tunnel tracker packets are dropped by firewall with self zone policy.
<a href="#">CSCwc76044</a>	Interface stats are not getting updated for port-channel.
<a href="#">CSCwd56015</a>	UTD skipped when interface UTD config is used to enable/disable UTD.
<a href="#">CSCwd56336</a>	BFD sessions are not coming up after flapping the interface due to low ftn rate.

### Open Bugs for Cisco IOS XE 17.9.2a

Bug ID	Description
<a href="#">CSCwd44006</a>	Control Connection on device doesn't come-up with reverse proxy using Enterprise Certificate.
<a href="#">CSCwd33966</a>	Unable to configure the local BGP as-path-list via device.
<a href="#">CSCwd23810</a>	A high CPU utilization caused by NHRP.
<a href="#">CSCwd17579</a>	Router crashing with reason CPU usage due to Memory Pressure exceeds threshold (Reboot).
<a href="#">CSCwa14636</a>	Device stopped forwarding traffic. Suspect OMPd is busy.
<a href="#">CSCwd38626</a>	Repeating SYS-2-PAK_SUBBLOCK_BADSIZE: 4 -Process="&lt;interrupt level&gt;".

Bug ID	Description
<a href="#">CSCvz55282</a>	Serviceability enhancements for config migration failures between releases.
<a href="#">CSCwd17381</a>	NAT/DIA traffic is skipping UTD in forward direction after SSNAT path from service-side.
<a href="#">CSCwd13050</a>	After upgrade, device moves into Out of Sync status.
<a href="#">CSCwd12955</a>	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured.
<a href="#">CSCwd15560</a>	With 2 sequences, should not skip if the match is different and action is same.
<a href="#">CSCwd36621</a>	CERM may kick in due to IPsec sessions initiated for on-demand tunnels.
<a href="#">CSCwd44586</a>	Login banner config is changed after upgrade.
<a href="#">CSCwd37410</a>	0365 and MS Teams applications access issues when using DIA with app-list match in data-policy.
<a href="#">CSCwc28468</a>	Device always fails to push any template if it is running in FIPS mode.
<a href="#">CSCwc99823</a>	fman crash seen in SGACL@ fman_sgac1_alloc.
<a href="#">CSCwd29334</a>	Upgrade failures due to inability to establish netconf connection from device to upgrade-confirm.
<a href="#">CSCwd45508</a>	Device does not form BFD across Serial link when upgrading.
<a href="#">CSCwa96399</a>	Configuring entity-information xpath filter causes syslogs to print, does not return data.
<a href="#">CSCwd34941</a>	NAT configuration with no-alias option is not preserved after reload.
<a href="#">CSCwd18028</a>	After delete CSP, new CCM bring up on existing CSP is stuck in Initializing CCM on MT cluster.

### Resolved Bugs for Cisco IOS XE 17.9.1a

Bug ID	Description
<a href="#">CSCwb03893</a>	When MACSEC dot1q-in-clear 1 is enabled on interfaces there is traffic drop.
<a href="#">CSCwa52627</a>	Incorrect Tx/Rx optical power values reported for QSFP transceivers.
<a href="#">CSCwb44275</a>	Simulated flows with PPPoE with NAT DIA result in crash consistently.
<a href="#">CSCwb26560</a>	Router linecard crashed on doing issu-mdr-force issu.
<a href="#">CSCwa68540</a>	FTP data traffic broken when UTD IPS enabled in both service VPN.
<a href="#">CSCvx00230</a>	Device may show input/output rate values even if the interface is in admin down state.
<a href="#">CSCvz65764</a>	Peer MSS value showing incorrect.

Bug ID	Description
<a href="#">CSCwa95092</a>	When object-group used in a ACL is updated, it takes no effect.
<a href="#">CSCwb33968</a>	Device failed to display active flows when flow count is high on the device.
<a href="#">CSCwb02142</a>	Traceback: fman_fp_image core after clearing packet-trace conditions.
<a href="#">CSCwb49857</a>	Memory leaks on keyman process when key is not found.
<a href="#">CSCwa65728</a>	Large number of DH failures.
<a href="#">CSCwb11389</a>	NAT translation stops suddenly (ip nat inside doesn't work).
<a href="#">CSCwa84919</a>	"Revocation-check crl none" does not failover to NONE DNAC-CA.
<a href="#">CSCwb39098</a>	Router crashed after new IPv6 address assigned when router use specific configuration.
<a href="#">CSCwa69101</a>	ISG: initiator unclassified ip-address LQIPv4 command has no effect.
<a href="#">CSCwa67886</a>	UDP based DNS resolution doesn't work with IS-IS EMCP on IOX-XE/
<a href="#">CSCvz84588</a>	Destination prefix packets getting dropped because forwarding plane is not programming the next hop.
<a href="#">CSCwb27486</a>	New key for NBAR app and NBAR category without OGREF optimized.
<a href="#">CSCwa72273</a>	ZBFW dropping return packets from tunnel post upgrade.
<a href="#">CSCwa49101</a>	OMP origin protocol comparison cleanup.
<a href="#">CSCwb17282</a>	Router crashing when clearing a VPDN session.
<a href="#">CSCwa49721</a>	Hub with firewall configured incorrectly dropping return packets when routing between VRFs.
<a href="#">CSCwb21645</a>	NAT traffic gets dropped when default route changes from OMP to NAT DIA route.
<a href="#">CSCwa98617</a>	Memory Leak in AEM chunks related to firewall.
<a href="#">CSCwb18223</a>	SNMP v2 community name encryption problem.
<a href="#">CSCwb16723</a>	Traceroute not working with NAT.
<a href="#">CSCwb31587</a>	Subject-alt-name attribute in certificate trustpoint causes Windows NDES/CA to reject SCEP requests.
<a href="#">CSCwb51238</a>	Router reload unexpectedly two times when enter netflow show command.
<a href="#">CSCwb12647</a>	Router crash for stuck threads in epp on packet processing.
<a href="#">CSCwa48512</a>	CoR intercepted DNS reply packets dropped with drop code 52 (FirewallL4Insp) if UTD enabled also.
<a href="#">CSCwa93664</a>	ThousandEyes container may fail to get installed on device.

Bug ID	Description
<a href="#">CSCvz28950</a>	DMVPN phase 2 connectivity issue between two spokes.
<a href="#">CSCwa78348</a>	Traceback: IOS-XE reload after Segmentation fault on Process = SSS Manager.
<a href="#">CSCvz81664</a>	Enabling or disabling OMP overlay AS prevents connected routes from being advertised in OMP.
<a href="#">CSCwb43423</a>	Device image installation fails.
<a href="#">CSCwa08847</a>	ZBFW policy stops working after modifying the zone pair.
<a href="#">CSCwb15331</a>	Keyman memory leak using public keys.
<a href="#">CSCvw50622</a>	NHRP network resolution not working with link-local IPv6 address.
<a href="#">CSCwb59736</a>	CSR BFD tunnel are zero.
<a href="#">CSCwa57873</a>	Incorrect reload reason - last reload reason: LocalSoft for Netconf Initiated request.
<a href="#">CSCwb51595</a>	Missing IOS config (voice translation rule) on upgrade.
<a href="#">CSCwb18315</a>	Umbrella DNS security policy doesn't work with Cloud on Ramp with SIG tunnels.

### Open Bugs for Cisco IOS XE 17.9.1a

Bug ID	Description
<a href="#">CSCvz91309</a>	Crash due to IOSXE-WATCHDOG due to management port traffic storm.
<a href="#">CSCwb68897</a>	"Total output drops" counter in "show interface" on Port-channel doesn't work properly.
<a href="#">CSCwb55514</a>	Crash seen after enabling "platform qos port-channel-aggregate".
<a href="#">CSCvz89354</a>	Router crashes due to CPUHOG when walking Cisco Flash MIB.
<a href="#">CSCwc20171</a>	Fragmented packets crashes while allocating memory.
<a href="#">CSCwc17032</a>	cpp_cp_svr crash when port-channel configured.
<a href="#">CSCwc19171</a>	High CPU on SIP (mip100) due to mcpc-ic-ms caused by link up/down interrupts.
<a href="#">CSCwc26669</a>	TLB miss for lock address during FNF cache lookup.
<a href="#">CSCwc39012</a>	Crash saving tracelogs after "Too many open files" error.
<a href="#">CSCwc56896</a>	Crash in IPv6_tunnel_macaddr while adding/removing GRE multi-point tunnel mode.
<a href="#">CSCwb89958</a>	Unified Policy HSL not sending properly NBAR application information.
<a href="#">CSCwc23077</a>	Firewall drop seen stating "FirewallL4".
<a href="#">CSCwb74821</a>	Yang-management process confd is not running, controller mode.
<a href="#">CSCwc44851</a>	Bootstrap failing on device.

Bug ID	Description
<a href="#">CSCwc55684</a>	Layer 7 health check doesn't work on loopback interfaces.
<a href="#">CSCwc52538</a>	Device flows are not distributed and load-balanced evenly and consistently.
<a href="#">CSCwc55260</a>	Memory leak due to FTMD process.
<a href="#">CSCwc69881</a>	Device lost configuration due to multiple power cycles on site.
<a href="#">CSCwc20170</a>	Device reloads unexpectedly due to critical FTMD fault when VRF configuration is pushed.
<a href="#">CSCwb88621</a>	Device unable to establish control connection with vBond due to out of order DTLS packets.
<a href="#">CSCwc37465</a>	Static NAT configuration in CLI with the no-alias keyword cannot be retrieved via NETCONF/YANG.
<a href="#">CSCwc59598</a>	Statistics collection causing service-side BFD to flap on every collection interval.
<a href="#">CSCwc50477</a>	Device crashed in IPv4_nat_create_out2in_session_entry.
<a href="#">CSCwc67465</a>	Router can not be upgraded.
<a href="#">CSCwc59650</a>	Show device app-fwd cflowd flows vpn X format tabled does not show all flows for vpn X.
<a href="#">CSCwc32595</a>	BFD sessions remains down if interface flap form up/down/up.
<a href="#">CSCwc38529</a>	Traffic seems not inspected by UTD when umbrella is set.
<a href="#">CSCwc63563</a>	Unable to set specific speed and duplex values on SFP ports on IOS-XE routing platforms.
<a href="#">CSCwc39865</a>	Subscriber session getting stuck and needs clearing it manually.
<a href="#">CSCwc43973</a>	DLC is not completing after upgrading to Smart licensing from CSL.
<a href="#">CSCwc53885</a>	IOS-XE "no ip nat" config is allowed to be committed and removes NAT routes among other NAT config.
<a href="#">CSCwc55467</a>	BFD tunnel on router is not staying up, 1 out of 40 tunnels.
<a href="#">CSCwc42978</a>	Device loses all BFD sessions with invalid SPI.
<a href="#">CSCwc67171</a>	Tracebacks at cgm_avlmgm_class_init and cpuhog_key_init.
<a href="#">CSCwb08057</a>	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
<a href="#">CSCwc63337</a>	Destination not reachable if configured as a next for a static route resolvable via non /32 OMP.
<a href="#">CSCwc29629</a>	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication.

Bug ID	Description
<a href="#">CSCwc27208</a>	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES.
<a href="#">CSCwc68132</a>	SIG tunnel tracker packets are dropped by firewall with self zone policy.
<a href="#">CSCwc70511</a>	Router reloaded unexpectedly.

## ROMmon Release Requirements

For more information on ROMmon support for Route Processors (RPs), Embedded Services Processors (ESPs), Modular Interface Processors (MIPs), and Shared Port Adapter Interface Processors (SIPs) on Cisco ASR 1000 Series Aggregation Services Routers, see <https://www.cisco.com/c/en/us/td/docs/routers/asr1000/rommon/asr1000-rommon-upg-guide.html>.



**Note** After upgrading the ROMmon to version 17.3(1r), you cannot revert it to a version earlier than 17.3(1r) for the following platforms:

- ASR 1001-X
- ASR 1001-HX
- ASR 1002-HX

This restriction is only applicable for these platforms. If you have upgraded to ROMmon version 17.3(1r) on any other platform, reverting to an earlier version of ROMmon is permitted and does not cause any technical issues.

## Related Documentation

- [Release Notes for Previous Versions of ASR 1000 Series Aggregation Services Routers](#)
- [Hardware Guides for Cisco ASR 1000 Series Aggregation Services Routers](#)
- [Configuration Guides for ASR 1000 Series Aggregation Services Routers](#)
- [Product Landing Page for ASR 1000 Series Aggregation Services Routers](#)
- [Datasheet for ASR 1000 Series Aggregation Services Routers](#)
- [Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers](#)
- [Cisco ASR 1000 Series Aggregation Services Routers ROMmon Upgrade Guide](#)
- [Field Notices](#)
- [Cisco Bulletins](#)

## Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).



- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

### Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

## Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

## Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at <https://www.cisco.com/en/US/support/index.html>.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.

