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

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

Support for broadband features and functionalities with DNA Network Advantage Tier 3 License	From Cisco IOS XE 17.9.3 release, the following functionalities and features are supported on ESP100-X & ESP200-X platforms: • Layer 2 Tunnel Protocol Network Server (LNS) • Layer 2 Access Concentrator (LAC) • Broadband Network Gateway (BNG) • Intelligent Services Gateway (ISG) • Intelligent Wireless Access Gateway (iWAG). • PPP and IP sessions For more information, see: Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide, Cisco IOS XE 17 - Broadband Scalability and Performance [Cisco IOS XE 17] - Cisco Broadband Access Aggregation and DSL Configuration Guide, Cisco IOS XE 17 - Broadband Smart Licensing [Cisco IOS XE 17] - Cisco Intelligent Wireless Access Gateway Configuration Guide - iWAG Scalability and Performance [Cisco ASR 1000 Series Aggregation Services Routers] - Cisco

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
Asymmetric Lease for DHCPv4	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 ip dhcp relay short lease command on the server or relay agent.
Displaying link and prefix cache, and ISIS LSP TLV neighbor	The **show isis node** command is updated to display information about link and prefix cache, and the **show isis lspgen tlv neighbor** command is introduced to display information about ISIS LSP TLV neighbors.
Increase ACE Scale Limit Per OGACL	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.

Feature	Description
Logging Destination IP Address and Port Details	The **ip nat settings log-destination** 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.
Cisco Unified Border Element (CUBE) Features	
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.
Programmability Feature	
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
Smart Licensing Using Policy Features	
New mechanism to send data privacy related information	A new mechanism to send data privacy related information was introduced. This information is no longer included in a RUM report. If data privacy is disabled (**no license smart privacy** {**all**|**hostname**|**version**} command in global configuration mode), data privacy related information is sent in a separate sync message or offline file. 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. For more information, see license smart (global config).
Hostname support	Support for sending hostname information was introduced. If you configure a hostname on the product instance and disable the corresponding privacy setting (**no license smart privacy hostname** command in global configuration mode), hostname information is sent from the product instance, in a separate sync message or offline file. 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. For more information, see license smart (global config). **Note** 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).

Feature	Description
RUM Report Throttling	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. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). 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. You can override the reporting frequency throttling, by entering the **license smart sync** 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. 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 *all* subsequent releases.
Virtual Routing and Forwarding (VRF) Support	On a product instance where VRF is supported, you can configure the **license smart vrf** *vrf_string* command and use a VRF to send licensing data to CSSM, or CSLU, or SSM On-Prem. **Note** When using a VRF, the supported transport types are **smart** and **cslu** only.) For more information, see license smart (global config)

Resolved and Open Bugs for Cisco IOS XE 17.9.x

Resolved Bugs for Cisco IOS XE 17.9.5a

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

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

Bug ID	Description
CSCwd17272	UTD Packet drop due to fragmentation for ER-SPAN traffic.
CSCwe91898	Environmental syslog is not appearing when the power cord is disconnected from the redundant power supply.
CSCwf55243	Device is crashing while adding a trust point to the router.
CSCwh49644	Compliance failure: Use of 3DES by IPSEC is denied.
CSCwh32386	Unexpected reload on device due to critical process fman_fp_image.
CSCwe30514	Device reboots with SSL proxy and UTD enabled.
CSCwh30377	Device data plane crash in DNS security processing due to incorrect UDP length.
CSCwf34171	**configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwf96980	Unexpected reboot after configuring application redundancy.
CSCwe64779	Router software forced reset during high IPC congestion with IPSec.
CSCwh01425	ITU channel configuration seems not working on the device.
CSCwh20577	Crashed by TRACK Client thread at access to invalid memory location.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on the device.
CSCwh36801	Crash in IP Input process during tunnel encapsulation.
CSCwh96415	Can't disable DMVPN logging.
CSCwe85301	Crypto process crash when PKI trust point is being deleted.
CSCwh20734	Crypto process crash when PKI trust point is requested and deleted.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwc97579	Spoke-spoke cache refresh not working correctly in case of multiple cache entries for the same next hop.
CSCwf11394	Debug log should mention port-hop and reason prior to DISTLOC.
CSCwf04866	Keyman process crash seen while re-generating SSH key in the device.
CSCwh00332	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
CSCwi51234	Unable to properly activate the Foundation Suite License on the device.

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

Bug ID	Description
CSCwh22414	Warning and critical CPU utilization thresholds not recomputed when using data-plane-heavy mode.
CSCwi46997	NAT Command not readable after reload.
CSCwi01046	PoE module is not providing enough power to activate the ports after an unexpected reload.
CSCwc30418	Segmentation fault observed in ikev2_dupe_delete_reason.
CSCwi16111	IPv6 TCP adjust-mss not working after delete and reconfigure.
CSCwi63042	Packet drops observed between LISP EID over GRE Tunnel.
CSCwi53306	Unknown appID in ZBFW HSL log.
CSCwb25507	CWMP: Add vendor specific parameter for NBAR protocol pack version.
CSCwi59202	Device with SwitzerCC can't boot up.
CSCwh91136	Traffic not encrypted and dropped over IPSEC SVTI tunnel.

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
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z

Open Bugs for Cisco IOS XE 17.9.4a

Bug ID	Description
CSCwd39257	IOS-XE CPP crash when entering **no ip nat create flow-entries**.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwf41492	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
CSCwf52751	CLI template fails to attach to device with error **access-denied**.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites.
CSCwf34171	**configure replace** command fails due to the **license udi PID XXX SN:XXXX** line on IOS-XE devices.
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.

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

Resolved Bugs for Cisco IOS XE 17.9.4

Bug ID	Description
CSCwf48808	Stale client routes stuck in RIB on flex server.
CSCwe93905	NAT ALG is changing the call-ID within SIP message header causing calls to fail.
CSCwf02225	Device freezes for **show SDWAN** commands.
CSCwe24210	SNMP MIB does not show correct firmware version for device LTE module.
CSCwe18124	MACsec remains marked as SECURED, but the traffic stops working randomly.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.

Bug ID	Description
CSCwd87195	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.
CSCwf08698	Device crashes unexpectedly due to a fault in the 'TLSCLIENT_PROCESS'.
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwf47796	NHRP cache entries flood matching a /32 default route.
CSCwf09758	Crashes while importing big CRL file into switch.
CSCwe41946	DTMF is failing through IOS MTP during call on-hold.
CSCwe18058	Unexpected reload with IPS.
CSCwe12194	Auto-Update cycle incorrectly deletes certificates.
CSCwd49309	Crash seen on device with traffic pointing to segfault in coff handler.
CSCwe33793	Memory allocation failure with extended antireplay enabled.
CSCwe66318	NAT entries expire on standby router.
CSCwe31471	Segmentation fault in device PB rx when per-tunnel QoS config is withdrawn.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwe70374	Device Punt-Policer is not configurable.
CSCwe20008	[LTE] SNMP MIB OID changing its last index.
CSCwf47563	Device is crashing after importing the trustpoint with rsakeypair.
CSCwe37123	Device uses excessive memory when configuring ACLs with large object groups.
CSCwd73783	Observed qfp-ucode-wlc crash.
CSCwe39011	GARP on port up/up status from device is not received by remote peer device.
CSCwf39490	MCID (Malicious Call Identification) gets broken due to custom prefix setting under STCAPP FAC.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwe69783	Device can lose its configuration during a triggered resync process if lines are in an off-hook state.
CSCwe89404	No way audio when using secure hardware conference with secure endpoints.
CSCwe41234	VMWI race condition causes no ringing for analog phones.
CSCwa96399	Configuring **entity-information** xpath filter causes syslogs to print, does not return data.

Bug ID	Description
CSCwc89823	Router crashes due to CPUHOG when walking Cisco Flash MIB @snmp_platform_get_flash_file_info.
CSCwe32862	Router IOS-XE crash while executing AES crypto functions.
CSCwf37888	Device Packet Duplication: Duplicate packets are counted on Primary Tunnel Interface Statistics.
CSCwd68994	ISAKMP profile doesn't match as per configured certificate maps.
CSCwd35047	Failed to ping gateway while configuring **SharedLOM** with console , te1 interface until router reload.
CSCwd49177	ISG: L2-connected subscriber. IPv6 prefix delegation is not reachable when packet are switched.
CSCwe22838	ARP is not completing on interface having CISCO-OPLINK SFP.
CSCwe80684	QFP Ucode crash when clearing MACs under BD in EVPN scenario.
CSCwe12090	No error log generated when EVC/bridge-domain reaches maximum MAC learning limit on device.
CSCwe22353	IpFormatErr drops on device when bridge-domain/EVC MAC learning limit is exhausted.
CSCwd93401	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM.
CSCwd81813	**startup-config** not parsed correctly after upgrading.
CSCwe16371	Device going in disabled state after **hw-module <slot> reload**.
CSCwf45769	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
CSCwd39257	IOS-XE CPP crash when entering **no ip nat create flow-entries**.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwf41492	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
CSCwf52751	CLI template fails to attach to device with error **access-denied**.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites.

Bug ID	Description
CSCwf34171	**configure replace** command fails due to the **license udi PID XXX SN:XXXX** line on IOS-XE devices.
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.
CSCwf41450	Device reloads changing the resource profile.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write configuration with same crypto value.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit in 8500L
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list.
CSCwf03193	Device crash with crashinfo files were generated with segmentation fault, rocess IPSEC key engine.
CSCwf25735	Device QoS more than four remark with set-cos not work.
CSCwf11394	IOS XE - device debug log should mention port-hop and reason prior to DISTLOC.
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwe51910	SNMP ifindex persist does not work.
CSCwd61988	Output packet bytes calculation biase when we enable QoS on port channel.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config.
CSCwf48967	Failure to upgrade FPGA version to standby RP module.
CSCwf47789	dot3StatsDuplexStatus gives unknown for tengig and gig interfaces.
CSCwe25815	Crash due to DTL push/pop on wait loop.
CSCwe69338	Duplicate telemetry updates for environment-seensors path.
CSCwe84306	Unable to configure CIR rate higher then 67G.
CSCwh60848	CUBE - SIP Message Queuing Fails to Resume Transmission

Resolved Bugs for Cisco IOS XE 17.9.3a

Bug ID	Description
CSCwd45402	MSR Unicast-To-Multicast not working if DST and SRC are the same in Service Reflect configuration.

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

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

Open Bugs for Cisco IOS XE 17.9.3a

Bug ID	Description
CSCwd39257	IOS-XE CPP crash when entering **no ip nat create flow-entries**.
CSCwd63783	Memory leak caused router reload.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwe24491	Static NAT with HSRP stops working after removing/adding standby.
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.
CSCwe32862	Router IOS-XE crash while executing AES crypto functions.
CSCwe07055	Device frequent reloads.
CSCwc28468	Device always fails to push any template to device if device is running in FIPS mode.
CSCwd68994	Unable to match on customer profile based on certificate-map.
CSCwc06327	PFP policy in SRTE, RIB resolution in FC bring down ipsec tunnel interface- stuck at linestate down.
CSCwe38732	IP CEF load sharing command is being changed by the device.
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwe37184	Device seeing out of service on switch modules when using with new DC power supply.
CSCwh60848	CUBE - SIP Message Queuing Fails to Resume Transmission

Resolved Bugs for Cisco IOS XE 17.9.2a

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

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

Open Bugs for Cisco IOS XE 17.9.2a

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

Bug ID	Description
CSCvz55282	Serviceability enhancements for config migration failures between releases.
CSCwd17381	NAT/DIA traffic is skipping UTD in forward direction after SSNAT path from service-side.
CSCwd13050	After upgrade, device moves into Out of Sync status.
CSCwd12955	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured.
CSCwd15560	With 2 sequences, should not skip if the match is different and action is same.
CSCwd36621	CERM may kick in due to IPSec sessions initiated for on-demand tunnels.
CSCwd44586	Login banner config is changed after upgrade.
CSCwd37410	0365 and MS Teams applications access issues when using DIA with app-list match in data-policy.
CSCwc28468	Device always fails to push any template if it is running in FIPS mode.
CSCwc99823	fman crash seen in SGACL@ fman_sgacl_calloc.
CSCwd29334	Upgrade failures due to inability to establish netconf connection from device to upgrade-confirm.
CSCwd45508	Device does not form BFD across Serial link when upgrading.
CSCwa96399	Configuring entity-information xpath filter causes syslogs to print, does not return data.
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwd18028	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
CSCwb03893	When MACSEC dot1q-in-clear 1 is enabled on interfaces there is traffic drop.
CSCwa52627	Incorrect Tx/Rx optical power values reported for QSFP transceivers.
CSCwb44275	Simulated flows with PPPoE with NAT DIA result in crash consistently.
CSCwb26560	Router linecard crashed on doing issu-mdr-force issu.
CSCwa68540	FTP data traffic broken when UTD IPS enabled in both service VPN.
CSCvx00230	Device may show input/output rate values even if the interface is in admin down state.
CSCvz65764	Peer MSS value showing incorrect.

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

Bug ID	Description
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes.
CSCwa78348	Traceback: IOS-XE reload after Segmentation fault on Process = SSS Manager.
CSCvz81664	Enabling or disabling OMP overlay AS prevents connected routes from being advertised in OMP.
CSCwb43423	Device image installation fails.
CSCwa08847	ZBFW policy stops working after modifying the zone pair.
CSCwb15331	Keyman memory leak using public keys.
CSCvw50622	NHRP network resolution not working with link-local IPv6 address.
CSCwb59736	CSR BFD tunnel are zero.
CSCwa57873	Incorrect reload reason - last reload reason: LocalSoft for Netconf Initiated request.
CSCwb51595	Missing IOS config (voice translation rule) on upgrade.
CSCwb18315	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
CSCvz91309	Crash due to IOSXE-WATCHDOG due to management port traffic storm.
CSCwb68897	"Total output drops" counter in "show interface" on Port-channel doesn't work properly.
CSCwb55514	Crash seen after enabling "platform qos port-channel-aggregate".
CSCvz89354	Router crashes due to CPUHOG when walking Cisco Flash MIB.
CSCwc20171	Fragmented packets crashes while allocating memory.
CSCwc17032	cpp_cp_svr crash when port-channel configured.
CSCwc19171	High CPU on SIP (mip100) due to mcpcc-lc-ms caused by link up/down interrupts.
CSCwc26669	TLB miss for lock address during FNF cache lookup.
CSCwc39012	Crash saving tracelogs after "Too many open files" error.
CSCwc56896	Crash in IPv6_tunnel_macaddr while adding/removing GRE multi-point tunnel mode.
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCwc23077	Firewall drop seen stating “FirewallL4”.
CSCwb74821	Yang-management process confd is not running, controller mode.
CSCwc44851	Bootstrap failing on device.

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

Bug ID	Description
CSCwc27208	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES.
CSCwc68132	SIG tunnel tracker packets are dropped by firewall with self zone policy.
CSCwc70511	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.