Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Dublin Release 17.12.x

First Published: 2023-08-22

Last Modified: 2026-08-05

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.

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 Dublin 17.12.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Dublin 17.12.x release series.

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 17.12.8

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.7b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.6

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5d

There are no new features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5a

There are no new features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.4b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.4a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.3

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.2

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.

Table 1: New Software Features

Feature	Description
Cisco Managed Cellular Activation (eSIM)	The Managed Cellular Activation solution provides a programmable subscriber identity module (SIM), called an eSIM, a physical SIM card that you can configure with a cellular service plan of your choice. When ordering a pluggable interface module (PIM) to provide cellular connectivity for your router, choose a PIM model with a preinstalled eSIM. The Managed Cellular Activation solution comes with a "bootstrap" cellular plan to provide internet connectivity with a limited amount of data intended only for Day 0 onboarding of the device to your cellular plan. For information about configuring Cisco SD-WAN Manager with the details of your cellular plan in preparation for onboarding the device, see the Cisco Managed Cellular Activation Configuration Guide. Prepare the configuration in Cisco SD-WAN Manager before powering on and onboarding the device, to avoid running out of the limited data in the bootstrap cellular plan. Added Cisco Managed Cellular Activation (eSIM) support for the following Pluggable Interface Module (PIM) model: • 5G Sub-6 GHz PIM, model P-5GS6-R16-GL **Note** In this context, eSIM refers to a removable SIM pre-installed by Cisco. In other contexts, eSIM can refer to a non-removable SIM embedded in a cellular-enabled device.

New and Changed Software Features in Cisco IOS XE 17.12.1a

Feature	Description
Managing the SD-Routing Devices Using Cisco SD-WAN Manager	This feature allows you to perform management operations for SD-Routing devic SD-WAN Manager. You can use a single network manage system (Cisco Catalys to monitor all the SD-Routing devices and therefore help in simplifying solution
Segment Routing over IPv6 Dataplane	Segment Routing (SR) can currently be applied on Multiprotocol Label Switchin From Cisco IOS XE 17.12.1a, SR is supported over the IPv6 dataplane for the fo • Interior Gateway Protocol (IS-IS only) • Border Gateway Protocol (BGP) In addition, the following functionalities are available for Segment Routing over • Segment Routing Traffic Engineering Policies • Static Routes • Performance Management • Operations, Administration and Maintenance (OAM)

Feature	Description
Support for Automatic Log Deletion	This feature allows you to delete the entries from the logging buffer. You can retention period after which the entries are purged from the device automatica use the **logging purge-log buffer days** command.
Support for a Minimum Frame Size of 72 Bytes	This feature helps users to set a minimum frame size of 72 bytes on an EPA i **min-frame-length 72byte** command.
Cisco Unified Border Element (CUBE) Features	
CUBE: IPv6 Flows in High Availability	From Cisco IOS XE Dublin 17.12.1a onwards, High Availability in CUBE su
CUBE/LGW: Cover Buffer Enhancements for VoIP Trace	From Cisco IOS XE Dublin 17.12.1a onwards, VoIP Trace for SIP messages cover buffer.

Resolved and Open Bugs for Cisco IOS XE 17.12.x

Resolved Bugs in Cisco IOS XE 17.12.8

Identifier	Headline
CSCwu02602	DBAL EVENTS crash seen while trying to push config group to device in SDWAN and SD-Routing.
CSCws75769	Netconf process doesn't start on 9130 AP in EWC mode and generates repeated dmiauthd subscription failures for invalid route-map YANG path.
CSCws80808	Loopback interface in Mgmt-intf VRF becomes unreachable via Management interface.
CSCwt87294	mDNS Cache-Flush behavior not consistent.

Open Bugs for Cisco IOS XE 17.12.8

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

Resolved Bugs for Cisco IOS XE 17.12.7b

Identifier	Headline
CSCwm67178	Cannot configure MD5 for the hash under the ikev2 proposal when compliance shield is disabled.
CSCwo57783	"NHRP Encap Error for Purge Request" populates on spoke despite correct routing at HUB.
CSCwn85623	Missing Calling-Station-ID in radius messages.
CSCwr83968	Unexpected Reload on cEdge with Static NAT When Polling NAT Translation Data.
CSCwm62981	Device crashes with PKI "revocation-check ocsp none" enabled.

Identifier	Headline
CSCwp28682	Update GeoDB version.
CSCwp96706	Memory leak in MallocLite and Crypto IKEv2.
CSCwq22471	Device may unexpectedly reboot when importing CA chains.
CSCwq21566	HSL entries are missing when config is pushed via vManage.
CSCwq51358	Device may experience high memory utilization and unexpected reloads during IKEv2 operations.
CSCwn18874	DMVPN spoke crashed at Process = NHRP.
CSCwo14975	Memory leak in DNS Proxy/SKA triggers unexpected reloads.
CSCwp40010	RP crash while debugging IKEv2.
CSCwp38609	CTS Trustpoint loop triggers PKI segfault.
CSCwq49981	Call Failures due to FPI resource leaks.

Open Bugs for Cisco IOS XE 17.12.7b

Identifier	Headline
CSCwj79930	Loading an image to device with firewall config crashed.
CSCwi03502	Create CLI to push at#enadis=0 followed with at#reboot to FN980 required when configuring Multi-PDN.
CSCwr00088	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP.
CSCwj33723	Config not synced between active and 3rd member of stack.
CSCwn29062	Router may see cosmetic "DATACORRUPTION" logs during IPSec Tunnel Up/Down events.
CSCwk55051	polaris_vconfd_cfgpull_t denials during config push trigger.
CSCwm54978	Selinux: Subject polaris_iosd_t denials.

Resolved Bugs for Cisco IOS XE 17.12.6

Bug ID	Description
CSCwp03641	[XE CGN] Multiple inside local addreses are translated to same inside global IP address and port.
CSCwo91955	Endpoint tracker remains up status when DNS is reachable from the other interface.
CSCwn99822	Large number of BFD sessions stuck due to out of window drops reported with control connections NAT flaps.

Bug ID	Description
CSCwp28915	SNMP walk fails to consistently return tunnel names due to incomplete tunnel setup.
CSCwn52179	Traffic with TTL 2 is punted to CPU when CEF holds MPLS labels set to None.
CSCwo89784	Unexpected reload of Standby during PKI Trustpoint removal.
CSCwn99723	Deprecate "request platform software package expand" commands for upgrades.
CSCwp12923	IKEv2 fails to parse certain route-set prefix Cisco VSA attributes from Radius server.
CSCwn89026	CEF DPI loadbalancing incorrect distribution for tunnel-l2tp.
CSCwb24403	BFD flap on public IP change on a private color tloc.
CSCwo66822	Cedge reloaded with reason: Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69).
CSCwo90396	Serial interface configuration lost after reload.
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned.
CSCwo12453	Configuring "access-class xx in vrf Mgmt-vrf" on line vty causes the âLogin Block" to be inactive.
CSCwo51627	IOS-XE: Unexpected reload due Critical process linux_iosd_image fault on rp_0_0 (rc=139).
CSCwn39832	Adding "authorization bypass" to vDSP EEM scripts.
CSCwo03915	Unexpected reload on cEdge due to performance monitor with packet service insertion from spoke.
CSCwp81333	Cache Coherency rare timing race condition.
CSCwo15543	Functional SJC Alpha 9840 eWLC HA- Standby eWLC reloads after upgrade to 17.17.1.
CSCwk56650	cEdge unexpected reboot during dialer initialization.
CSCwj27134	IP vrf receive command adds connected route to vrf table even though interface admin down.
CSCwo34430	Terminal Server Drops protocol Sessions upon executing "Show Memory" Command
CSCwo05166	Memory leak on Chunk Manager via DBAL EVENTS process.
CSCwo99641	Out of CGM (Class-Group Manager) memory intermittently with scaled ZBFW policy.
CSCwn53302	Administrative distance of IPv6 static route to Cellular interface overwrite with 254.
CSCwn37412	NTP will not authenticate with open source NTP servers using 32B cmac-aes-128.
CSCwk05523	Catalyst switch crashes with "Bad magic number in chunk header", with ACL logging hash-generation.

Bug ID	Description
CSCwm01063	Unexpected reload due to Segmentation fault on IP SLA DynHostName Process.
CSCwn53778	Unexpected reload on router (IOSd shim QOS).
CSCwo70548	Ping failure from VRRP backup to VRRP primary virtual address when enabling security policy.
CSCwp35552	Missing Calling-Station-ID (31) in Radius Accounting.
CSCwn92976	PPP is not establishing when l2tp over IPsec.
CSCwn24036	Tx/Rx optical power values diffrent for "show int" and "show hw-module".
CSCwk98236	Port 5152 is reused simultaneously in nat interface overload scenario on platform.
CSCwo66011	Config Parser Issue for NAT with reversible and redundancy.
CSCwo47118	17.12.3 - Crash when clearing L2TP tunnels with the command "clear vpdn tunnel l2tp <ID>".
CSCwn54648	High CPU on Virtual EXEC and TTY Background.
CSCwp59954	Unexpected reboot on IOS-XE due prune on mcast.
CSCwj60804	ACL delete and reapply removes PBR mapping but TCAM is populated.
CSCwo22585	cEdge device crashes when running a NWPI trace initiated from vManage on version 20.12.4.
CSCwp02071	Tunnels dropping when CAC configured for VDPN when CPU over threshold due to SSH request for SH tech.
CSCwi59338	Enable strict-kex support in IOS-SSH to address CVE-2023-48795 (aka Terrapin Attack).
CSCwn59814	FLOWDB_OOM condition can lead to packet loss with GRE non-IPSEC tunnel.
CSCwn60286	IOS-XE: Memory Leak observed in IPSEC/IKE session bringup with Cert-based Authentication.
CSCwn65589	DMVPN Tunnel bounces a 2nd time after RP3 failover and recovery .
CSCwo84747	Tunnel delete/create flaps unexpectedly for PWK case for private control NAT changes.
CSCwn15850	IOS-XE 17 Crash When "show running-config full | format" Begins to Print QoS Policy-map Config.
CSCwp17220	Continous fman_fp related traceback seen at interval of 10s.
CSCwn50935	Crash occurs during haripin call.
CSCwo98465	Crash when receiving BGP MVPN update/withdraw with BGP MVPN update debug enabled.

Bug ID	Description
CSCwq01226	ESP crash @stile_check_and_run_mpe_after_ft ().
CSCwn93483	cEdge: confd_cli high cpu utilization after executing "show zbfw-dp sessions | tab".
CSCwo38144	entSensorthresholdrelation reporting wrong value.
CSCwn18584	17.15.2/17.12.5: Traecbacks seen on curie router while applying config on a clean router.
CSCwp15054	Memory leak in nbar-sdavc-scheduler.
CSCwq31287	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability.
CSCwn98779	Multihome DC publication has inconsistent domain and mh id.

Open Bugs for Cisco IOS XE 17.12.6

Bug ID	Description
CSCwn85623	Missing Calling-Station-ID in radius messages.
CSCwq22471	IOS-XE unexpected reload after importing subca chain.
CSCwp40010	RP Crash While Debugging IKEv2.
CSCwq08151	Unexpected reload while running a Speed Test from vManage and leaving the page before it completes.
CSCwo57783	"NHRP Encap Error for Purge Request" populates on spoke despite correct routing at HUB.
CSCwm54978	SIT-SDWAN: Selinux: Subject polaris_iosd_t denials 2024-09-16 06:43:22.
CSCwp38609	CTS Trustpoint loop triggers PKI segfault.
CSCwq49981	Call Failures due to FPI resource leaks.

Resolved Bugs for Cisco IOS XE 17.12.5d

Bug ID	Description
CSCwo38924	Cisco IOS XE Software Secure Boot Bypass Vulnerability .
CSCwo38903	Cisco IOS XE Software Secure Boot Bypass Vulnerability.
CSCwn48408	Cisco IOS XE Software HTTP API Command Injection Vulnerability.
CSCwm57073	Cisco IOS XE Software WebUI Reflected Cross-Site Scripting Vulnerability.
CSCwm41327	Cisco IOS XE Software CLI Argument Injection Vulnerability.

Bug ID	Description
CSCwm99306	Cisco IOS and IOS XE Software TACACS+ Authentication Bypass Vulnerability.
CSCwp03900	Cisco IOS XE Software Simple Network Management Protocol Denial of Service Vulnerability.
CSCwq31287	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability.

Open Bugs for Cisco IOS XE 17.12.5d

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

Resolved Bugs for Cisco IOS XE 17.12.5c

Bug ID	Description
CSCwp81333	Cache Coherency rare timing race condition.
CSCwq01226	ESP crash @stile_check_and_run_mpe_after_ft ().
CSCwp66926	FNF AOR might have double-free risk.
CSCwo19997	QFP crash with stuck threads while attempting to lock cft policy under Autonomous mode.

Open Bugs for Cisco IOS XE 17.12.5c

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

Resolved Bugs for Cisco IOS XE 17.12.5b

Bug ID	Description
CSCwo67161	IPsec-related crash on an IOS-XE device.

Open Bugs for Cisco IOS XE 17.12.5b

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

Resolved Bugs in Cisco IOS XE 17.12.5a

Table 2: Resolved Bugs in Cisco IOS XE 17.12.5a

Bug ID	Description
CSCwk61238	RRI static not populating route after reload if stateful IPSec is configured.
CSCwk23723	Router: Mean queue calculation is incorrect on WRED hierarchical QoS.
CSCwf77488	IOSd crash after Radium boot up and online.

Bug ID	Description
CSCwm93092	Incorrect window size value for Anti replay >= 4096.
CSCwn13650	Multiple address range support in a local pool.
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration.
CSCwm11819	Crash due to SIGSEGV | fman_fp_image fault on fp_0_0 (rc=139).
CSCwf79399	IOS-XE Port-channel sub-interface overload Port-channel interface must be created first and delete.
CSCwj80411	Deleting and adding the rules in a ZBFW policy with 510 rules results in traffic drop.
CSCwk81360	Cisco IOS-XE Router can reboot unexpectedly while configuring NAT Static Translation.
CSCwk33173	EzPM application-performance profile cause memory leak and crash with long-lived idle TCP flows.
CSCwk52106	SNMP reports incorrect Transmit Power / Receive Power values for 100G AOC cables.
CSCwm14462	IPv6 flowspec nexthop redirect policy not redirecting the traffic on IOS XE.
CSCwm05524	Unexpected Reload Due to "cpp-mcplo-ucode" Process When Handling Fragments With SRv6 Routing.
CSCwj84949	Unencrypted Traffic Due to Non-Functional IPsec Tunnel in FLEXVPN Hub & Spoke Setup.
CSCwk56504	In NAT64 scenario, IPv4 packets that needs translation might be dropped.
CSCwm98642	OMP is redistributing summary routes in the service VPN even though the exact networks don't exist.
CSCwm07396	Few BFD sessions down after clear mka session on client.
CSCwm80356	LLDP packets dropped when came through active port-channel interface
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.
CSCwk79454	Endpoint Tracker does not fail if default route is removed.
CSCwn12370	Router with IOS XE Version 17.9.5a we canÂ´t update the CPLD-version from 19041800 to 20030413
CSCwk72795	No statistics for the SBFD protocol.
CSCwm12851	IOS-XE 17.12.3 uses 3DES as default rekey algorithm for GETVPN.
CSCwj86794	Router crashes while processing an NWPI trace.
CSCwk87452	Procyon synchronize DTL does not wait until complete due to compiler optimization.

Bug ID	Description
CSCwm79570	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm89600	Cisco IOS, IOS XE, and IOS XR SNMP Denial of Service Vulnerabilities.
CSCwm79581	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm79554	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm79596	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm79577	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm08791	Dial-peer never recovers an active state if it goes partial or busyout.
CSCwm01029	CUBE gets forked 180 and 183 with SDP, CUBE is not adding SRTP key when sending 183, causing failure.
CSCwn49403	CUBE incorrectly offers rtp instead of srtp in 200OK for srtp fallback scenario.
CSCwn19326	CDR file accounting creates dummy files.
CSCwm03319	Optimize voip trace handling with tenants
CSCwm73825	Crash observed on device, while performing the conference call.
CSCwn48914	Router crash during SGW sync in VOICE REG BG Process.
CSCwm32946	CUBE doesn't relay/pass 488 Media Unacceptable from one leg to another leg for FAX (T.38) Re-INVITEs.
CSCwi77331	IOS-XE unexpected reboot after CLI "show sip-ua connection".
CSCwn09710	Memory leak under *Dead* caused by AFW_application_proc.
CSCwn60303	Router cube sip-ua commands lost after reload.
CSCwn13988	CDR file accounting credentials exposure.
CSCwm91190	MWI app not registering on Vcube in 17.12.4.
CSCwk44855	Cannot dial to/from phone after it reboots in survivability mode.
CSCwm82247	CUBE memory leak for SIP out-of-dialog SUBSCRIBE under CCSIP_SPI_CONTROL process.
CSCwm79213	"setPthruCryptoData: mfPthruCrypto NULL" showing up excessively in the log.
CSCwm91175	OOD Subscribe with event message-summary is causing memory leak on CUBE.
CSCwm47634	No audio issue on call transfer and conference.
CSCwm39795	DATA_RECREATE_ERR: (STBY-Modify): HA Module DSP_MSP reported CALL_MODIFY RECREATE failure on standby.

Bug ID	Description
CSCwm79956	Memory leak under *Dead* caused by AFW_application_proc.

Open Bugs in Cisco IOS XE 17.12.5a

Table 3: Open Bugs in Cisco IOS XE 17.12.5a

Bug ID	Description
CSCwn97600	Some BFD flapping on PWK ipsec-rekey on all cEdge.
CSCwe23188	Upgrade from vmanage declared successful even though device boots up with different version than requested.
CSCwk87338	SNMPv3 user credentials to be stored as part of running-configuration with encryption.

Resolved Bugs - Cisco IOS XE 17.12.4b

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

Open Bugs - Cisco IOS XE 17.12.4b

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

Resolved Bugs in Cisco IOS XE 17.12.4a

Table 4: Resolved Bugs in Cisco IOS XE 17.12.4a

Identifier	Headline
CSCwi87546	CPP unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released.
CSCwj40589	Endpoint tracker using DNS does not log "DOWN" message when DNS server reachability is lost.
CSCwm60651	HTX: UTD snort crash at memif_shm_peek_first_packet (handle=0x0).
CSCwk84047	Memory Leak due to security violation by new MAC address and '"Del Pend" object increases - ACE_IPV4.
CSCwk54544	ZBFW TCAM misprogramming after rules are reordered on the device.
CSCwk50488	Memory leak in fman_rp under acl_db.

Open Bugs in Cisco IOS XE 17.12.4a

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

Resolved Bugs for Cisco IOS XE 17.12.4

Bug ID	Description
CSCwj70335	Crypto IKEv2 - Fragmented Authentication packets detected as malformed on 3rd party vendor device.
CSCwj04575	Router crashed during SNMPwalk when removing SFP.
CSCwj03621	Ping with smaller packet size is failing on macsec enabled port.
CSCwj25508	Router reports incorrect DOM values over SNMP.
CSCwj44868	GETVPN COOP KS | Wrong Severity for Rekey Acknowledgement configuration mismatch log message.
CSCwi88969	FMFP-3-OBJ_DWNLD_TO_DP_FAILED observed when delete and configure zone-pair back.
CSCwj21653	Kernel crash over continuous reloads.
CSCwi68865	Memory leak in Crypto IKEv2 due to C_NewObject.
CSCwj09284	Unexpected reboot in WLC due to SSL.
CSCwi40603	Memory leak in the Crypto IKMP process.
CSCwj24511	Tunnel QoS - WRED incorrect IP precedence classification with MPLS EXP.
CSCwi82405	mGRE Tunnels with shared ipsec profile cause ucode crash.
CSCwj34578	NAT46 translations are dropped when NAT64 router is also Carrier Supporting Carrier CE.
CSCwi55183	"crypto pki certificate pool" in Running Configuration.
CSCwk15127	Failure to communicate a period of time after the stp status changes.
CSCwh37024	PnP gets stuck when Verizon cellular backhaul is used.
CSCwj45130	Segmentation Fault - Process = IPSec dummy packet process.
CSCwj88872	IPsec tunnel fails to establish due to error IPSec policy invalidated proposal.
CSCwj73113	MGCP GW doesn't respond with 250 OK for a DLCX leading to DLCX loop from CUCM side.
CSCwi59854	'show sdwan policy service-path' command gives inconsistent results with app name specified.
CSCwj38106	Only one split-exclude subnet is pushed to client PC with IOS-XE headend for a RA VPN connection
CSCwh73320	NAT Pool doesn't working under prefix 16. Available address = zero
CSCwi56114	Secure datawipe should reset the configuration register.

Bug ID	Description
CSCwi89822	Unexpected reboot due cpp ucode on a router.
CSCwh86053	ENH: Config Parser Issue for NAT with Extendable and Redundancy.
CSCwj42249	Disabling PMTU-Discovery with MTU Change and BFD Flap Breaks Packet Duplication.
CSCwj36915	Device: macsec not working under LACP port-channel member port.
CSCwi78365	Trim installed certificate on upgrade.
CSCwj72888	Reload in tcp_sanity due to l4 pointer not set.
CSCwi93784	FW upgrade does not work properly on P-LTE-MNA with 17.12.1a and 17.12.2 IOS.
CSCwj33292	AnyConnect connection trough IPSec fails when connecting from an RDP user to an IOS/IOS-XE headend.
CSCwj06622	Segmentation fault and core files are seen on IOS-XE in controller-manged SD-WAN due to speedtest.
CSCwi16111	IPv6 tcp adjust-mss not working after delete and reconfigure.
CSCwj29947	AAA authorization failure during IKEv2 phase negotiation caused unexpected reboot.
CSCwj30334	Router rebooted when attempting merge on used CVLA block.
CSCwi62239	%IOSXE_MGMTVRF-3-INTF_ATTACH_FAIL error after configuring loopback managment vrf then removing it.
CSCwf87975	Router crashed when port-channel interface flap with scale of per-tunnel qos policies.
CSCwj74260	Default setting of Global Punt Policer burst needs to be increased.
CSCwj23735	CUBE - "rtp port range" configuration lost under "voice service voip" after reload.
CSCwj26668	IOS XE wrong audio rtp packet marking for SCCP SRST.
CSCwj23804	Password created with "key config-key password-encrypt" ending with a "\" are lost after reload.
CSCwj59262	SIPREC Secure media forking -1 of 2 Audio Streams is encrypted due to same key sent for both streams.
CSCwj95128	CUBE incorrectly change dtmf payload in asymmetric case.
CSCwj93967	History-Info header compatibility between CUBE and MS Direct Routing.
CSCwj05013	CUBE Media Proxy(CMP) dual forking not working after upgrade to 17.9.x.
CSCwj82258	IOS-XE router may crash during transfer call flow in SRST.
CSCwi69071	Unexpected reload caused by crash in 'Skinny Msg Server' process.

Bug ID	Description
CSCwj98360	Media forking not working in CUBE.
CSCwj54666	SIP cause code incorrect for CCAPI cause code 31.
CSCwk08864	"authentication" command under dial-peer is missing "challenge.
CSCwj61168	IOS-XE Router experiences memory leak in ucode_pkt_PPE0 process.
CSCwh81312	%DSMP-3-INTERNAL: Internal Error : NO MEMORY seen in standby router while checkpointing legs.
CSCwj41553	SGW calling to TDM, AOR is not getting changed to number.
CSCwj75508	SRST running on Catalyst 8200 fails to register SCCP phones after reload.

Open Bugs for Cisco IOS XE 17.12.4

Bug ID	Description
CSCwi03502	Create CLI to push at#enadis=0 followed with at#reboot to FN980 required when configuring Multi-PDN.
CSCwk31560	NAT Command is not readable after reload.
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration.
CSCwk58303	Watchdog crash during IPv6 cef adjacency routines.
CSCwk63722	Startup Configuration Failure Post PKI Server Enablement.
CSCwj06950	Device DSL module gets stuck in a booting state.
CSCwj21653	Device Kernel crash over continuous reloads.
CSCwk33173	EzPM application-performance profile may cause memory leak with certain long-lived idle TCP flows.
CSCwk52106	SNMP reports incorrect Transmit Power / Receive Power values for 100G AOC cables.
CSCwj77594	IOS XE Controller Mode - WAN IP is allowed to be configured as SYSTEM IP.
CSCwk57979	emd fault on cc_0_0 (rc=134) due to ensor has exceeded it's maximum number of read errors.
CSCwk54544	SD-WAN ZBFW TCAM misprogramming after rules are reordered on device.
CSCwb47658	Repeated and endless messages "Network change event - activated 4G Carrier Aggregation."
CSCwk56504	In NAT64 scenario, IPv4 packets that needs translation might be dropped by device.
CSCwj90614	High CPU utilisation for confd_cli.

Bug ID	Description
CSCwk03686	Crash due a segmentation fault due a negative value.
CSCwj92560	STCAPP command removed from device after reload.
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwh45389	Key manager crash after hostname change with usage keys.
CSCwk12524	Device reloaded due to ezManage mobile app Service.
CSCwk53680	Inbound calls through device results in phantom calls .(64.3.0, 60.1.4, 62.3.3)
CSCwk65071	Unexpected reboot due to IOSXE-WATCHDOG DBAL EVENTS after Cellular interface flap.
CSCwf91481	Device crashed unexpectedly after a successful WGB/AP config deployment from OD.
CSCwi96187	P-5GS6-GL FN980 modem fW upgrade failing when two modems on device.
CSCwh91136	IOS XE:Traffic not encrypted and droped over IPSEC SVTI tunnel.
CSCwk52677	Device / DSL router crashing due to %PLATFORM-3-ELEMENT_CRITICAL memory level / iomd process.
CSCwj84949	Unencrypted Traffic Due to Non-Functional IPsec Tunnel in FLEXVPN Hub & Spoke Setup.
CSCwj86794	Device crashes while processing an NWPI trace.
CSCwk30527	IKEv2 session is down after reload if identity local address is assigned to interface on Switch.
CSCwj54638	Device EVC Q-in-Q configuration may filter out certain vlans
CSCwi31110	Traceback seen @_nhrp_cache_delete due to negative global cache count .
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.
CSCwk68564	Device running 17.9.5 ES crashed with multiple core files.

Resolved Bugs - Cisco IOS XE 17.12.3a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Description
CSCwk21189	Template attach fail with unknown element: ssh-version in /ios:native/ios:ip/ios:ssh
CSCwk20843	PPPoE with NAT DIA feature validation failed post upgrade.

Resolved Bugs for Cisco IOS XE 17.12.3

Bug ID	Description
CSCwh73350	Device keeps crashing when processing a firewall feature.
CSCwh18120	The diagnose feature for IKEv2 is consuming 11% CPU during the session initiation phase.
CSCwh68508	Unexpected reboot after establishing the control plane of EVPN MPLS and receiving packets.
CSCwi28227	NAT HSL logging with VRF filtering is not functioning correctly.
CSCwh22414	Warning and critical CPU utilization thresholds are not recalculated when using data-plane-heavy mode.
CSCwi01046	PoE module does not provide sufficient power to activate the ports after an unexpected reload.
CSCwh77221	SNMP unable to poll tunnel data after a minute.
CSCwh96578	SKA_PUBKEY_DB leak in TDL.
CSCwh69765	Security policy with IPS external syslog configuration fails to generate for specific device models.
CSCwi06843	Endpoint tracker triggers a CPU Hog.
CSCwh87619	ZBFW is unable to detect packets on TenGig interface for device.
CSCwh10813	Add verbose log to indicate grant when grant ra-auto configuration unconfigures grant auto in the PKI server.
CSCwi60312	Device can't boot up in full configuration.
CSCwh93257	Device creates incorrect NAT entry if two or more IP phones from NAT outside register to the same server.
CSCwi59121	Mobile application causing excessive authorization attempts with a null username on a specific device model.
CSCwi08171	Device may crash due to Crypto IKMP process.
CSCwi49231	Audio loss experienced for four seconds on a Voice Gateway device.
CSCwi06404	PKI service crash following an unsuccessful CRL fetch.
CSCwh50510	Device crash with segmentation fault (11), Process = NHRP when processing NHRP traffic.
CSCwh75800	Device unexpectedly reloads during Trustpool retrieval for SIP TLS certificate.
CSCwi28781	EPBR generates an error when the policy is added and deleted multiple times.
CSCwi49240	One-way RTP issue including DSP timeout messages (63.2.0 / 62.3.1).

Bug ID	Description
CSCwh45169	Unexpected reboot while displaying information from a cleared SSS session.
CSCwh70449	PMTUD is not properly converging as it does not attempt to learn a higher MTU value.
CSCwh96415	Inability to disable DMVPN logging on recent software versions.
CSCwi25737	Device should discard IKE Notification messages with incorrect DOI.
CSCwh50628	Race condition crash on device.
CSCwf86207	Frame Relay DTE router crashes due to EXMEM exhaustion.
CSCwh72869	cpp_mcplo_ucode crash with Port-channel and NAT configurations.
CSCwh99399	FTMD crash observed in ENCS platform while running PWK suite.
CSCwi76087	ATO: Session fails to come up when the tunnel is repeatedly shut and no shut (similar to a customer unplugging and replugging a cable).
CSCwi55379	IPSec traffic is being dropped strongSwan when PPK is implemented.
CSCwi63042	Packet drops observed between LISP EID over GRE Tunnel.
CSCwi79584	Upgrade failure on a device via management system due to a system configuration error.
CSCwi30529	AAA template push fails when AAA authorization is configured for local use.
CSCwi51234	Unable to properly activate the Foundation Suite license on a device running software version.
CSCwh22451	Device packets appeared out of order when using Embedded Packet Capture.
CSCwf89154	EZMAN posted statistics to APIs show sudden jumps in Ingress and Egress Bytes counters for Sub-Interfaces.
CSCwh85803	MACsec session is in a secured state but is not sending any traffic.
CSCwh26209	Device crashed with no microcode due to possible dataplane memory corruption in the NAT client.
CSCwj02110	Process mcpcc-lc-ms crash seen due to due to MKA session SAK rekey.
CSCwh59411	Fifty-gigabit port returns a link-flap error-disabled status when peer device reloads or bounces.
CSCwi21548	EntSensorStatus is displayed as Nonoperational.

Open Bugs for Cisco IOS XE 17.12.3

Bug ID	Description
CSCwi03502	Create CLI push at#enadis=0 followed with at#reboot to FN980 required when configuring Multi-PDN on a device.
CSCwj08744	Unexpected reload when using **show running-config full | format** command.
CSCwi16111	IPv6 TCP adjust-MSS not working after deletion and reconfiguration.
CSCwi46997	NAT command not readable after reload.
CSCwi67621	Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69).

Resolved Bugs for Cisco IOS XE 17.12.2

Bug ID	Description
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwf84960	LED L remains green after port shutdown.
CSCwf26875	Ten0/0/2 from Port-channel going to suspended status applying **platform QoS port-channel-aggregate**.
CSCwf82676	CPU usage mismatch in **show sdwan system status** vs **show proc cpu platform**.
CSCwf49390	Device crashes@crypto_map_unlock_map_head.
CSCwe91898	Environmental syslog is not appearing when power cord is disconnected from the redundant PS.
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands.
CSCwh30377	Device data plane crash in Umbrella/OpenDNS 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.
CSCwh01425	ITU channel configuration seems not working on device.
CSCwh20577	Crashed by TRACK Client thread at access invalid memory location.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on device.
CSCwh36801	Crash in IP Input process during tunnel encapsulation.
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error.
CSCwh20734	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested & deleted.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwh29805	Custom-app based policy triggering protocol deactivation and CPP traceback with traffic failure.

Bug ID	Description
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwf80191	Flowspec on device does not revoke.
CSCwf55830	No dial tone on analog phones due to DSP going into power denial state.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config.
CSCwh00332	B2B NAT: when configration ip nat inside/outside on VASI intereface, ack/seq number abnormal.
CSCwf67564	Device observes memory leak at process SSS manager.
CSCwh25168	**CPLD upgrade failed** error message logged during ROMmon upgrade.
CSCwh59064	Depletion in process memory pool/IOSd after enabling virtualization on Cisco IOS-XE platform.
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.
CSCwf67564	Device observes memory leak at process SSS Manager.
CSCwf60151	Memory leak with pubd.
CSCwh60190	**ip name-server** command not pushed.
CSCwf56463	IOS process crash during VRRP hash table lookup.
CSCwh11858	Device running IOS-XE crashes when removing FQDN ACL.
CSCwf99906	NTP authentication removed after reload using more than 16 bytes.
CSCwf59173	Segmentation fault at IPv6 BGP backup route notification.
CSCwf67351	Cisco IOx application hosting environment privilege escalation vulnerability.
CSCwf68612	WLC unexpected ueload due to segmentation fault in WNCD process.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.
CSCwf41084	Extranet multicast code improvements for better handling of data structure.
CSCwh04884	VC down due to control-word negotiation.
CSCwf26494	BDI + NTP configuration puts DMI process in degraded mode.
CSCwh96700	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper

Open Bugs for Cisco IOS XE 17.12.2

Bug ID	Description
CSCwh73350	Router keeps crashing when processing a firewall feature.

Bug ID	Description
CSCwh94906	WLC segmentation fault crash with Network Mobility Services Protocol (NMSP).
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCwi01046	PoE module is not providing enough power to bring the ports after an unexpected reload.
CSCwh16901	HSEC license installation from the workflow does not complete.
CSCwh77221	SNMP Unable to poll Tunnel Data after a minute.
CSCwh10813	Renewal of certificates on PKI client fails after a few rollovers.
CSCwh79161	WP7607 Requires Shut/No Shut to populate IP address from modem to host.
CSCwh57544	Silent Reload due to LocalSoftADR causes crash without core file.
CSCwh50510	Router crash with segmentation fault (11), process = NHRP when processing NHRP traffic.
CSCwh75800	Router unexpectedly reloads while fetching certificate Trustpool for SIP TLS.
CSCwh73320	NAT Pool does not work under prefix 16. Available address = zero.
CSCwh96700	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper.
CSCwh45169	Unexpected reboot while dispalying information from cleared SSS session.
CSCwh70449	PMTUD incorrectly converging without attempting to learn a higher MTU.
CSCwf91481	IR1835 crashed unexpectedly after a successful WGB/AP config deployment from OD.
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwh83228	NHRP phase 3 spoke-spoke cache got purged after 5-6 hours with always on traffic running.
CSCwh91136	Traffic not encrypted and droped over IPSEC SVTI tunnel.
CSCwh96415	Cannot disable DMVPN logging.
CSCwh12093	Enable SoS/ROC feature for DSL.
CSCwf86207	Frame Relay DTE router crashes due to EXMEM exhaustion.
CSCwh22451	Device packets appeared out of order when using Embedded Packet Capture.
CSCwh72869	cpp_mcplo_ucode crash with Port-channel and NAT.
CSCwh26209	Router crashed with no UCode due to possible dataplane memory corruption in NAT client.

Bug ID	Description
CSCwh77925	Malformed packet when there is QinQ and L2TPV3 configured.
CSCwh45579	Unexpected reload on device UCode core @l2_dst_output_goto_output_feature_ext_path.
CSCwh93257	Device creates crooked NAT entry if 2 or more IP phone from NAT outside register to same server.
CSCwh99427	Device reload due to memory corruption [GKM KS PROCESS].
CSCwh64981	Unexpected reboot due to invalid rte_eth_tx_burst.
CSCwf48967	Failure to upgrade FPGA version to standby RP module.
CSCwh59411	Device fiftygig port returns link-flap err-disabled status when peer device reloads or bounces.
CSCwh87619	ZBFW is not able to detect packets on TenGig interface for device.
CSCwh92627	Device port-channel stuck IHQ after remote LC flap.
CSCwh32386	Unexpected reload on device due to Critical process fman_fp_image.
CSCwh58252	IPv6 SPD min/max defaulting to values 1 and 2.
CSCwh14083	High CPU due to MPLS MIB poll.
CSCwh22981	WNCD process crashes.
CSCwh99513	VPLS IRB not working when traffic came from VPNv4 and next-hop is learned over VPLS.
CSCwh90851	pubd process showing high CPU utilization.
CSCwh83532	1Gig int on device using GLC-SX-MMD are down/down after changing connection.
CSCwh96891	Memory leak with pubd.
CSCwh91085	Convergence improvement after device reboot with MVPN profile 14.
CSCwh58919	NETCONF: DMI enters degraded mode caused by BGP neighbor configured under the SCOPE command.
CSCuu85298	FIB/LFIB inconsistency after BGP flap.
CSCwf83684	IOS XE router may experience %FMANRP_QOS-4-MPOLCHECKDETAIL: errors.
CSCwh59926	EEM is running daily instead of weekly or monthly if special strings @weekly or @monthly are used.
CSCwh24280	Mismatch between the resource allocation and **app-resource profile custom** configuration.
CSCwh82668	Incorrect local MPLS label in CEF after BGP flap.

Bug ID	Description
CSCwh95036	Cisco IOS-XE IPv6 based subscription telemetry does not work.
CSCwh99464	Guestshell connectivity not working with NAT overload.
CSCwh30928	SDA - using **spt-threshold infinity** and having LHR+FHR can cause the S,G to be pruned on the RP.
CSCwh01738	Unexpected reload when using rsh/rcmd.
CSCwh04124	Locally generated traffic received on incorrect interface inbound and dropped by ACL.
CSCwh67285	WLC unable to get telemetry data due to pubd unexpected reload and fail.
CSCwh96332	Device crash due to dhcpd_binding_check.
CSCwh56940	Site tag change wncd working/failing EAP-TLS.
CSCwh44418	ARP incomplete in VRF Mgmt-intf - G0/0/0 - Switch -G0.
CSCwh46559	LLDP location information not sent when configured.
CSCuv36790	**clear bgp** command does not consider AFIs when used with update-group option.
CSCwh02698	Device sending incomplete SGT to ISE.
CSCwh05869	Only portion of HSRP config being pushed via CLI ADDON template.
CSCwf53750	**match pktlen-range** does not work with GRE/IPSEC GRE.
CSCwh60107	In the show tech file, **enable secret** does not get hidden.
CSCwh45579	Unexpected reload on device ucode core @l2_dst_output_goto_output_feature_ext_path.
CSCwh95024	ISIS crash in local Uloop.
CSCwh41155	Wrong /32 self, complete map-cache entry for fabric hosts on IBN when overlapping summary exists.
CSCwh31485	Member interface config not applied with mis-match in pcakages.conf files.
CSCwh72437	WLC not sending accounting start for user auth after machine auth on 9105AXW RLAN dot1x port.
CSCwi00680	Router unexpectedly reloads while using DHCP for ISG.
CSCwh96823	IOS-XE router not installing classless-static-routes from DHCP option 121.
CSCwh77706	SVL, 10G link on the active chassis will go down after reload.
CSCwh02592	Device sync fails when device prompt comes along with device banner and TACACS is used.
CSCwh84850	Unexpected reboot in device due to SISF and STP initialization.

Bug ID	Description
CSCwh64903	Crash on device polling SPA sensor data.
CSCwh53432	VLAN name mismatch when authorizing vlan name from radius server and enable vlan fallback.
CSCwh21796	Password getting visible for the mask-secret in show logging.
CSCwh50104	Upgrade failing with config check track-id-name.
CSCwf59929	CTS CORE process crash after configuring role based ACL.
CSCwh81471	IPv6 traffic is passing through when the client is in Webauth Pending state (CWA).
CSCwh93772	Option 121 never requested by IOS-XE client.
CSCwh06087	[IPv6 BGP] multiple sourced paths present for the same prefix.
CSCwh29120	IP SPD queue thresholds are out of range.
CSCwh14953	CBQoS polling for the object cbQosCMPostPolicyBitRate returns incorrect value.
CSCwh89096	Device unexpected reload.
CSCwh99597	After migration MAC/IP only MAC is advertised.
CSCwh75992	BGP Router process crash.
CSCwh48058	Memory leak under MallocLite/AAA proxy with NETCONF/RESTCONF.
CSCwh76920	Memory leak in linux_iosd-imag due to SNMP.
CSCwh75112	After a reboot, EAP-FAST/PEAP does not authenticate unless credentials are changed.

Resolved Bugs for Cisco IOS XE 17.12.1a

Bug ID	Description
CSCwe82666	Not all HSL entries get pushed to device if more than 1 HSL entries are configured.
CSCwe31226	Issues/discrepancies around CPU alarms generated and sent to device.
CSCwe43341	TLS control-connections down, traffic from controller dropped with SDWANImplicitACLDrop.
CSCwe18124	MACsec remains marked as Secured, but randomly the traffic stops working.
CSCwe18276	Route-map not getting effect when its applied in OMP for BGP routes.
CSCwf83850	With Pure IPv6, minimal bootstrap unable to onboard Non-Fabric - IPv6 config missing in wan int G1.
CSCwb74821	Unexpected behavior due to unstable power source.
CSCwe81182	(EPC, packet-trace) for IPsec running COFF (Crypto Offload).

Bug ID	Description
CSCwe63222	Certificate output is not getting changed on renew when cloud certificate authorization is automated.
CSCwd61988	Output packet bytes calculation biase when we enable QoS on port channel.
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
CSCwe90501	Device upgrade fails due to **advertise aggregate** with VRF.
CSCwe85195	AAR: BoW feature ignoring color preference from Tiered Transport preference configuration.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwe65036	Device crashed and reboot history **shows IntelResetRequest** on upgrade.
CSCwd53710	Crash seen when umbrella/zscaler template pushed to device when name_lookup takes > 30 sec.
CSCwe66318	NAT entries expire on standby router.
CSCwf83985	With Pure IPV6 overlay, vbond vpn 0 ge0/0 interface if-oper-status down after power off/on.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwe70374	Device punt-policer is not configurable.
CSCwe73408	For some error condition platform_properties may double free.
CSCwd42523	Same label is assigned to different VRFs.
CSCwe12194	Auto-Update Cycle incorrectly deletes certificates.
CSCwe12090	No error log generated when EVC/bridge-domain reaches Maximum MAC Learning Limit on device.
CSCwe57239	All USB internal communcation is closed when using **platform usb disable** command.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwe85421	Device BFD Session Down with interface flap.
CSCwe95606	Double GR_Additional log enablement defect.
CSCwe31471	Segmentation fault in PB rx when per-tunnel QoS config withdraw.
CSCwe89404	No way audio when using secure hardware conference with secure endpoints.
CSCwd39257	IOS-XE cpp crash when entering **no ip nat create flow-entries**.

Bug ID	Description
CSCwe70642	AAR overlay actions are applied to DIA traffic.
CSCwa96399	Configuring **entity-information** xpath filter causes syslogs to print, does not return data.
CSCwe79007	Device unexpected reload when doing ips test with UTD IPS engine.
CSCwe31281	Autotunnel IPSec tracker: Tracker does not come up at all on device.
CSCwe80684	QFP UCode crash when clearing MACs under BD in EVPN scenario.
CSCwd93401	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM.
CSCwf65696	Non-fabric- Load the minimal bootstrap configs again if device rebooted without saving the configs.
CSCwd76648	Port-channel DPI Load-Balancing not utilizing all the member-links.
CSCwe39011	GARP on port up/up status from C8300 router is not received by remote peer device.
CSCwb39206	Enable VFR CLI.
CSCwe85022	Telstra Cert: FN980 modem (P-5GS6-GL) is showing 4 additional NR bands support - 1, 3, 7, and 28.
CSCwe84306	Unable to configure CIR rate higher then 67G.

Open Bugs for Cisco IOS XE 17.12.1a

Bug ID	Description
CSCwf70854	Changes to speed on the interface via CLI/GUI don't go through unless first done via shell access.
CSCwf48967	Failure to upgrade FPGA version to standby RP module.
CSCwf72079	Device unexpectedly reloads due to 'LocalSoft'.
CSCwf87292	Punt keep alive failure crash on controller managed device apparently due to data packets.
CSCwf89219	CISCO-ENTITY-PERFORMANCE-MIB for SNMP crypto load monitoring on device.
CSCwf83850	With Pure IPV6, minimal bootstrap unable to onboard Non-Fabric - ipv6 config missing in WAN int G1.
CSCwf94294	Misprograming during VPN-list change under data policy.
CSCwf55145	SFP transceiver DOM not working after some time. However, interface forwards the traffic as expected.
CSCwf94052	BFD going down for newly onboarded device.

Bug ID	Description
CSCwh02580	Hierarchical QoS shaping policy causes data plane and control plane disruption.
CSCwh01095	Rapid memory leak on ngiolite process.
CSCwf61720	No licenses in use after upgrading from Traditional to Smart licensing IOS-XE versions.
CSCwf80927	Speed tests to internet from device triggered will fail sometimes.
CSCwh01313	Unexpected reboot due QFP UCode due to IPSec functions.
CSCwf84522	Device unexpected reboot while classifying packet with CTF (Common Flow Table).
CSCwh00320	**show run** and other show commands not in sync after removing GigabitEthernet3.
CSCwf44703	NAT64 prefix is not originated into OMP.
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands.
CSCwf77252	SIP calls not working on device with ZBFW enabled.
CSCwf96416	Could not access any device show commands at all.
CSCwf67564	Device observes Memory Leak at process SSS Manager.
CSCwf34171	**configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwe26895	Device has LocalSoftADR crash, writes flat core, and reloads.
CSCwf80191	FlowSpec on device won't revoke.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on device.
CSCwf69062	SDRA-SSLVPN: The SSL VPN session closes with re-authentication error after some interval of time.
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwf79264	Device traffic forwarded to wrong VPN hence traffic gets wrong zonepair matched and gets dropped.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwf45486	OMP to BGP redistribution leads to incorrect AS_Path installation on chosen next-hop.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwh00101	Crash in fman_fp due to error binding an IPSec SA.
CSCwf95527	BFD entries removed.
CSCwf58356	Tail Drops are incrementing continuously on Ten Gig Interfaces.
CSCwh01318	Multiple crashes observed on device platform due to memory exhaustion.

Bug ID	Description
CSCwf71116	Static route keep advertising via OMP even though there is no route.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config.
CSCwh00332	B2B NAT: when configration ip nat inside/outside on VASI intereface, ack/seq number abnormal.
CSCwf49390	Device crashes@crypto_map_unlock_map_head.
CSCwf78735	Device uses the NIM-1T/4T card for interconnection, and NAT+ GRE over IPSec cannot be applied.
CSCwf84960	C-NIM-2T: LED L remains green after port shutdown.
CSCwh67812	Unable to configure **crypto map** on a physical interface due to which crypto map-based VPN's cannot be formed.

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.

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 results 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.

© 2023–2026 Cisco Systems, Inc. All rights reserved.