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

First Published: 2023-08-22

Last Modified: 2024-03-22

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 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 17.12.3

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) models: • 5G Sub-6 GHz PIM, model P-5GS6-R16-GL • LTE CAT 18 PIM, model P-LTEAP18-GL • LTE CAT 6 PIM, models P-LTEA-EA, P-LTEA-LA • LTE CAT 7 PIM, models P-LTEA7-NA, P-LTEA7-EAL, P-LTEA7-JP **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 d SD-WAN Manager. You can use a single network manage system (Cisco Cata to monitor all the SD-Routing devices and therefore help in simplifying solut

Feature	Description
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)
Support for Automatic Log Deletion	This feature allows you to delete the entries from the logging buffer. You can cor retention period after which the entries are purged from the device automatically. 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 inter **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 suppo
CUBE/LGW: Cover Buffer Enhancements for VoIP Trace	From Cisco IOS XE Dublin 17.12.1a onwards, VoIP Trace for SIP messages disp cover buffer.

Resolved and Open Bugs for Cisco IOS XE 17.12.x

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.

Bug ID	Description
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).
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.

Bug ID	Description
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.
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.

Bug ID	Description
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.
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.

Bug ID	Description
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.
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.

Bug ID	Description
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.
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.

Bug ID	Description
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.
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).

Bug ID	Description
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).
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.

Bug ID	Description
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**.
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.

Bug ID	Description
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.
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.

Bug ID	Description
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.
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.

Bug ID	Description
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.

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.