

Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Amsterdam 17.3.x

First Published: 2020-03-04

Last Modified: 2023-10-02

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 The Cisco IOS XE 17.3 release is the last release in which subpackage upgrade is supported for the following platforms:

- ASR 1004
- ASR 1002-X
- ASR 1001-X
- ASR 1001-HX
- ASR 1002-HX

The [subpackage upgrade](#) for these platforms will not be supported from Cisco IOS XE 17.4 release. These hardware platforms continue to support software redundancy.



Note Some YANG models are not fully compliant with all the IETF guidelines. The errors and warnings shown while executing pyang with `--lint` flag is currently deemed to be non-critical as they do not impact the semantic of the models or prevent the models from being used as part of the toolchains. To determine the issues with the models, run the `check-models.sh` script with `--lint` flag enabled.

It is recommended to ignore LEAFREF_IDENTIFIER_NOT_FOUND and STRICT_XPATH_FUNCTIONS errors types when running pyang for validation as they are non-critical errors and do not impact the YANG model functionality



Note When you upgrade from one IOS XE release to another, you may see `%Invalid IPv6 address` error in the console log file. To rectify this error, enter global configuration mode, and re-enter the missing IPv6 alias commands and save the configuration. The commands will be persistent on subsequent reloads.



Note Starting with Cisco IOS XE 17.3.x, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

The licensing utilities and user interfaces that are affected by this limitation include only the following:

- Cisco Smart Software Manager (CSSM),
- Cisco Smart License Utility (CSLU), and
- Smart Software Manager On-Prem (SSM On-Prem).

New and Enhanced Software Features for Cisco IOS XE Amsterdam 17.3



Note The Cisco IOS XE Amsterdam 17.3.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Amsterdam 17.3.1 release series.

Table 1: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE 17.3.x

Feature	Description
Support for IP Multicast over UDL functionality for PIM	The unicast and multicast routing protocols forward data on interfaces from which they have received routing control information using a bidirectional link. However, some network links are unidirectional, where the physical send-only interface is on the upstream router and the physical receive-only interface is on the downstream router. To control routing information in these unidirectional environments, use the IP multicast over UDL functionality.

Feature	Description
Support for openconfig-lldp 0.2.1	This release supports version openconfig-lldp 0.2.1 of LLDP protocol. No additional configuration is required.
Improved output for show ip nat pool command	The output of the show ip nat pool command is improved to display extra details.
Improved output for show diagnostic command	The output of the show diagnostic command now includes details of the serial number of the card in the slot.
Partial Configuration on CPE	This feature introduces limited support for following multicast modules in native operational YANG models: <ul style="list-style-type: none"> • PIM • MROUTE • MFIB
Show platform software cef ipv4 feature-all command	This command displays CEF information from the following commands without having to run each command individually : <ul style="list-style-type: none"> • show ip route <network> <network mask> • show ip cef <network> <network mask> internal • show adjacency <adj_id> internal • show platform software ip rp active cef prefix <network>/<mask_length> detail • show platform software adjacency rp active index <platform_adj_id> • show platform software ip fp active cef prefix <network>/<mask_length> detail • show platform software adjacency fp active index <platform_adj_id> • show platform hardware qfp active feature cef-mpls adjacency handle <cpp_handle_id>
BGP EVPN Route Reflector for Route Types	L2 Tenant Routed Multicast (L2 TRM) relies on new route types in the EVPN overlay to achieve the IGMP/MLD proxy functionality using the BGP route reflector with the following route types: <ul style="list-style-type: none"> • Selective Multicast Ethernet Tag Route (+6) • EVPN Multicast Join Synch Route (+7) • Multicast Leave Synch Route (+8)

Feature	Description
Policy-Based Routing support to categorise Office365 traffic for Direct Internet Access	To identify and differentiate Office 365 network traffic, Microsoft provides a web service to publish Office 365 endpoints and services. The Cisco Software-Defined AVC (SD-AVC) and Cisco Network-Based Application Recognition (NBAR) use this web service to improve first packet classification of Office 365 traffic to categorize it as as either “optimize or “non-optimize.”
Show packet tracer command	The output of the show platform packet-trace command now includes additional trace information for packets either originated from IOSd or destined to IOSd or other BinOS processes.
New cipher suites for IP ssh Client and Server Algorithm:	To configure the HMAC algorithm of HMAC-SHA2-256-ETM@openssh.com or HMAC-SHA2-512-ETM@openssh.com as a cryptographic algorithm for IP SSH client. These cipher suites can be used with the ip ssh client algorithm mac and ip ssh server algorithm mac commands.
Advertisement of Loopback Prefix SIDs of a Border Router in Multiple ISIS Domains	A border router can advertise loopback interface prefixes and the associated prefix Segment Identifiers (SIDs) in multiple ISIS domains. With such an advertisement, the routers in each associated domain can communicate with the border router using the same prefixes and prefix SIDs.
BGP Best External Path with MPLS VPN Inter-AS Options B and C	In autonomous Systems, you can configure border routers in MPLS VPN Inter-AS Option B and Inter-AS Option C deployments to compute the best external paths to PE nodes. The primary border router advertises best external paths to internal BGP (iBGP) peers as back-up paths so that if a link in a best path fails, traffic flows along the best external path.
Enable debug information for Multicast:	The following debug commands are introduced to enable the debugging information for Multicast via ConfD/NetConf: <ul style="list-style-type: none"> • debug platform condition feature multicast controlplane level • debug platform condition interface gigabitEthernet 0/0/1.2 ipv4 access-list mcast • debug platform condition feature multicast dataplane v4mcast submode • debug platform condition feature multicast dataplane v6mcast submode

Table 2: New and Enhanced Features for Cisco Unified Border Element (CUBE)

Feature	Description
Support for Cisco ASR-1006	The Cisco CUBE is supported on Cisco ASR 1006-X with RP3 and ESP 100.

Feature	Description
Support for 100 VRFs	The current support limit is 54 VRF instances on a CUBE box. This requires customers to purchase additional hardware to meet requirements. For deployments such as HCS support greater number of tenants per box, the limit of VRF instances is improved to 100 VRFs. This feature is also introduced on CUBE enterprise.
Dial Peer Binding with Live Traffic	The Live Bind feature allows you to either change or add binding on a dial-peer that does not have any active calls, while other dial-peers with the same binding has active calls.
Media Proxy Multi-forking using SIPREC	The SIPREC-based CUBE Media Proxy solution supports forking to multiple recorders.
OPUS Codec Negotiation	Support is introduced for OPUS audio codec with CUBE.
TLS Server Name Indication (SNI) - RFC6066	Support is introduced for Server Name Indication (SNI). SNI is a TLS extension that allows a TLS client to indicate the name of the server that it is trying to connect during the initial TLS handshake process.
Consumption of INVITE with Replaces	Currently, CUBE has a known limitation in handling re-INVITE with replace headers. With this feature, this limitation is addressed with CUBE consuming the INVITE with Replaces header and bridging the call dialogs appropriately. This feature enhancement is essential for interoperability of CUBE with Microsoft Teams.

New and Enhanced Software Features for Cisco IOS XE Amsterdam 17.3.2

Table 3: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE 17.3.2

Feature	Description
Smart Licensing Using Policy	<p>An enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use.</p> <p>With this licensing model, you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. Only export-controlled and enforced licenses require Cisco authorization before use. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date.</p> <p>Multiple options are available for license usage reporting – this depends on the topology you implement. You can use the Cisco Smart Licensing Utility (CSLU) Windows application, or report usage information directly to CSSM. A provision for offline reporting for air-gapped networks, where you download usage information and upload to CSSM, is also available</p> <p>For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.</p>

Feature	Description
Cisco DNA Support for Smart Licensing Using Policy	<p>Cisco DNA Center supports Smart Licensing Using Policy functionality starting with Cisco DNA Center Release 2.2.2. The corresponding minimum required Cisco IOS XE Release for this platform is 17.3.2.</p> <p>Implement the “Connected to CSSM Through a Controller” topology to have Cisco DNA Center manage a product instance. When you do, the product instance records license usage, but it is the Cisco DNA Center that initiates communication with the product instance to retrieve and report usage to Cisco Smart Software Manager (CSSM) and returns the acknowledgement (RUM ACK).</p> <p>In order to meet reporting requirements, Cisco DNA Center provides ad hoc or on-demand reporting, as well as scheduled reporting options. Cisco DNA Center also provides workflows for the installation and removal of the Smart Licensing Authorization Code (SLAC) for a product instance, if applicable.</p> <p>Note On the Cisco DNA Center GUI, you can generate a SLAC only for HSECK9 licenses, and only for certain product instances. See the configuration guide for details.</p>

New and Enhanced Software Features for Cisco IOS XE Amsterdam 17.3.3

Table 4: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE Amsterdam 17.3.3

Feature	Description
Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy	<p>SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM. Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. The product instance can be configured to <i>push</i> the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to <i>pull</i> the required information from a product instance at a configurable frequency. After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Offline and online options are available for synchronization between CSSM and SSM On-Prem.</p> <p>Minimum Required SSM On-Prem Version: Version 8, Release 202102</p> <p>Minimum Required Cisco IOS XE Version: Cisco IOS XE Amsterdam 17.3.3</p> <p>For more information, see Smart Licensing Using Policy for Cisco Enterprise Routing Platforms.</p>

Cisco Bug Search Tool

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

Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3

Resolved Bugs for Cisco IOS XE Amsterdam 17.3

Caveat ID Number	Description
CSCvh24730	PfRv3: Crash while Printing the Same TCA Message
CSCvi67613	Protocol type for GRE header doesn't work consistently with "cts sgt inline" enable over auto-tunnel
CSCvo26639	ASR 1000: All platforms having overrun drops after 24 hrs while traffic running at NDR

Caveat ID Number	Description
CSCvp24405	Router crash after adding macsec reply-protection command on an interface
CSCvp79052	vManage is not exhibiting the correct hostname of cEdge
CSCvp88044	Performance Monitor crash
CSCvq42698	Update "bandwidth remaining percent" doesn't take effective reliably on datapath
CSCvq70448	Unable to create EOS choice root table at the moment of connect SDHSL circuit
CSCvq93850	Passive FTP will fail when going over NAT and either client or server are off a SM-X-ES3
CSCvr42504	ping is not working on port-channel after router reload
CSCvr48928	Template push stuck on vManage Cluster when pushing new System IP to Edge router
CSCvr89957	CFT crashed frequently
CSCvr93635	flows not moving to unutilized link even after the hardthreshold
CSCvs02000	%IOSXE-3-PLATFORM: R0/0: kernel: DMA: Out of SW-IOMMU space
CSCvs27907	Ctrl+Z causes syntax error: unknown argument
CSCvs28073	IOS-XE device has memory leak in linux_iods-imag
CSCvs29412	x509 SSH authentication incorrect UPN value selected
CSCvs38028	cEdge_Policy_regression: Service IPv6 ping is failing if the interface vrf forwarding is replaced
CSCvs42498	NAT Alias not created for some configuration when using application redundancy
CSCvs43170	[vManage] Firewall inspect/drop stat values are incorrect on device dashboard
CSCvs45107	AnyConnect fails to reconnect when original session expires
CSCvs45215	Some CLI typo "policing" not "policying"
CSCvs45388	Failed to clear allocated ports for PAT after PAT CLI removal
CSCvs47682	Router crashed when attempting to remove a nonexistent trustpoint from dspfarm profile
CSCvs48162	Seeing IsecOutput drop for cEdge even though ip packet size is less than 1442.
CSCvs51630	cEdge: 'security ipsec replay-window' needs to support 8192
CSCvs53749	EVPN RMAC stale routes seen
CSCvs55489	XE RII flaps with NAT64 w/o ipv4 route
CSCvs56559	show crypto pki server shows wrong expire certificate date

Caveat ID Number	Description
CSCvs56721	spoke-to-spoke PLR packets should not change the interface PLR status
CSCvs57212	NGIO Lite is crashed when MT SMS with special characters (EMS) is received
CSCvs59402	Random IPSEC drops on ESP200 with esp-gcm transform set
CSCvs60195	ASR 1000 ucode crash after too many locks in ZBF pair setup
CSCvs60310	Punt Policer rates not defined for multiple platforms
CSCvs61402	CFLOW_INSERT ABORT errors continue to increment
CSCvs65950	IOS PKI: P12 not generated on IOS Sub CA at rollover certificate generation
CSCvs66091	XE SD-WAN Router SSH might get disabled followed by software reset and another reload
CSCvs70052	ALG with NAT trigger a crash when a DNS writeback occurs
CSCvs75868	esg:destination overwhelmed messages are seen on sending high rate TCP traffic leading to iosd crash
CSCvs78594	NAT doesn't translate SIP header's original source for return traffic on 16.9.3 and 16.9.4
CSCvs81098	Orthrus : With "sh hw-module subslot <> status" cli interface flapping
CSCvs81791	Fix for kernel driver issue causing wake up for empty block, packet too large to process
CSCvs88686	ISR4K / ASR / CBR8 crash in cpp_cp_svr due to watchdog timeout
CSCvs92239	PnP always fails in both 17.2.1 throttle and 17.3.1.
CSCvs96344	ASR 1000 : OIR after clock set doesn't save the time in RTC(recommit of CSCvr27554)
CSCvs96540	SDWAN device admin-tech has empty "show running config" in /tech/ios file
CSCvs96719	ASR 1000: Unicast DHCPREQUEST dropped when received on a EoGRE tunnel configured with VRF
CSCvs98586	Skip SDWAN tunnel encapsulated packets in UTD DP and set inspected flag when skipping inspection
CSCvs99705	PKI CLI - no warning that rsakeypair name starting from 0 (zero) is not working for cert regenerate
CSCvt01186	Interface does down when "l2vpn xconnect" command is removed
CSCvt01532	SD-WAN router running 16.10.3 crashes with cpp_cp_svr fault
CSCvt03869	Router reloads due to crypto pki crl request <trustpoint-name> during get a fresh copy of CRL
CSCvt04864	cpp_cp_svr fault and fman_fp_image fault on ASR 1002-x routers running 16.12.2r

Caveat ID Number	Description
CSCvt05373	SDWAN device and vmanage is not in sync when manual software reset is done
CSCvt06296	AVL tree still points to a tree node which has been freed
CSCvt06922	hidden policies and classifiers IOS native yang model config from "show sdwan running-config"
CSCvt08357	Time mismatch on sum of lapsed times from FIA Trace output
CSCvt09354	Active RP running Polaris crash when standby running 3.X inserted
CSCvt10151	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability UTD
CSCvt10499	"Exporter Version" is not correct in the FNF cpp client exporter show command
CSCvt12245	16.12.3 ZBFW-Mismatch in firewall stats between the device and vmanage
CSCvt13776	TSN. prd17 image : Crash @ __be_socket_remove_event_buffer
CSCvt15167	Cedge QOS Policy-Map on Parent Interface Maps Traffic to Wrong Queue When Traffic on Sub-Int
CSCvt15551	Crash observed in QFP in ASR1001-X running 16.06.05 when GPM is running low
CSCvt19873	ASR 1000:Router stops forwarding traffic with MPLS TE & FRR when member link of port-channel is shut
CSCvt21263	Crash upon delete of virtual-access when virtual-template has "no tunnel protection ipsec initiate"
CSCvt21373	unexpected reload in CPP ucode forced by nat 514 .
CSCvt21691	VLAN1 is allowed on the trunk port even though it is not allowed in configurations of C111 interface
CSCvt28357	Cloudexpress Symlinks missing for httping, timeout, nslookup utility in ASR1K
CSCvt28541	XE SD-WAN : cflowd not working after re attaching template
CSCvt30545	Probe reported 100% Loss for SaaS while network and configuration are all good.
CSCvt31561	TBAR is not disabled in GM when it is disabled in KS
CSCvt33018	MACsec 128/256 XPN on 40g/100g, stop passing traffic for one of AN and interface link flap seen
CSCvt33028	Part of double encapsulated frames dropped with TunnelDecapTooManyTimes code reason
CSCvt33799	Virtual address not reachable: "mac:0000:0c07:xxxx download to DP failed" for HSRP / VRRP over BDI.
CSCvt35947	Duplicate ipv6 address while connecting to remote client

Caveat ID Number	Description
CSCvt40523	GETVPN: KS 16.12.x - COOP switchover causes GMs to immediately use new TEK rekey
CSCvt46779	Route export not working as desired during failover testing
CSCvt49705	Device Crash observed with NAT and once there is traffic from outside
CSCvt52051	IPsec tunnel is getting established for a backup NHS DMVPN hub
CSCvt52168	SSH Process Thrash During Normal Operations
CSCvt52825	Memory leak in SCCP TLS Client on unexpected deregister event
CSCvt53726	Packet Duplication fails to duplicate packets in Cedge Devices
CSCvt54305	Device crashed after Boost license expire
CSCvt57538	IOSd crash due to Segfault in Crypto IKEv2 in ikev2_free_id
CSCvt59311	ASR 1000 crash when modifying crypto keyring configuration
CSCvt65588	FlexVPN IKEv2 Tunnel route removed after establishing new IKEv2 SA to another peer
CSCvt80422	RTP-NTE to OOB DTMF Interworking Failure over BDI with Dot1q Tagging
CSCvt99461	Remove duplicate license keyword from show platform software license command
CSCvu57682	ASR1001-X 16GB: Kernel crashes repeatedly after upgrading from 16.12.2 to 17.2.1
CSCvu82189	Enabling guestshell gives "float division by zero"
CSCvu89033	Template push error due to NAT-MIB process helper traceback/warm restart

Open Bugs for Cisco IOS XE Amsterdam 17.3

Caveat ID Number	Description
CSCvt32383	ASR1000 / RP2 upgrade fails from 16.9.4 to the 16.9.5
CSCvt35331	Console port goes unresponsive, reboot required to restore it.
CSCvt50136	ASR 1000 - all Platform : Observing IpFragErr for EMIX traffic with basic IPSEC config
CSCvt70321	Non-recurring summer-time IOSd config is incorrectly replicated to BinOS TZ environment
CSCvt75633	It takes long until FlexVPN IKEv2 tunnel re-establishes when tunnel flaps
CSCvt79205	ASR1001-X: 'show environment' is no longer monitoring R0 voltage sensors
CSCvt97086	ESPx : CMAN-FP process crash for get_fpga_version API fails

Caveat ID Number	Description
CSCvt97326	ASR 1000: harddisk usage is always zero in "show platform resource" for consolidated platforms
CSCvt97642	MIP100 - Continuous %SCOOBY-5-SERIAL_BRIDGE_BLOCK_EVENT flooding on the console
CSCvu00804	AnyConnect authentication fails when password contains "&" character
CSCvu06483	Data consistency errors seen on configuring mac-sec on the underlay interface with ipsec configured
CSCvu06877	Regression: vEdge2000 cannot exceed more than 65K NAT sessions over GRE or IKE IPsec tunnel
CSCvu26585	"req plat software trace archive" fails with "STORAGE_TARGET: unbound variable Operation failed"
CSCvu30539	Inbound CoPP policy causes outbound packets to fail to show up in EPC
CSCvu46417	ASR1k crash when doing a FIB lookup
CSCvu53184	cEdge - CLI should ask for confirmation of request software reset
CSCvu65369	Link auto-negotiation fails between C1111-4P ES-4 switch module and Meraki MX100
CSCvu67351	No traffic passing into the router on Everest or Fuji releases.
CSCvu67687	Packet Drops when EPC is off and MTU is over 1500
CSCvu70249	ASR1001X:SDWAN Default Throughput is not Scaling to Max supported
CSCvu73323	AAR policy does not work properly after Poweroff/Poweron Cedge ISR4451
CSCvu75453	ESP20 Rommon upgrade fails from 15.3(3r)S to 16.2(1r)
CSCvu77711	Missing Mandatory Transform Type (ESN) in IKEv2 ESP Protocol
CSCvu81329	sec policy pushing fail when remove L7 app from rule and action to drop
CSCvu82790	SIP2: kernel: write adm1075 register at D3 failed rtn=-16 seen during SOAK run
CSCvu85056	HTX memory hold increases, till a point, in longevity test
CSCvu89214	IOS-XE+ZBFW+CUBE: One-way-audio. TCP 5060 is not recognized as SIP.
CSCvu92277	Memory leak observed for FTM process leading to a device crash eventually.
CSCvu95098	GETVPN group member drops traffic due to replay failure every 497 days
CSCvu95121	Static NAT outside breaks locally generated TCP/UDP traffic
CSCvv00755	Static ip is pingable before interface cell goes up/up
CSCvv00899	Adaptive QoS history record LOCAL-LOSS is always 0 on ISR1000 platform

Caveat ID Number	Description
CSCvv01250	IGMP reports are forwarded to mrouter port untagged regardless of which VLAN the group is in
CSCvv01497	ASR 1000 ESP100 crash due to Deadlock
CSCvv01509	Data policy `from-tunnel` is not programmed if `from-service` presented
CSCvv03229	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
CSCvv05364	ASR1001-HX, CCP crash due to invalid address accessed by DTL
CSCvv07867	IOS-XE-SDWAN ISR4451-X/K9 - Performance Throughput lower than expected
CSCvv08341	Netconf deleting wrong IKEv2 parameters
CSCvv08952	FirewallNotInitiator drops with ZBFW for DIA traffic over Dialer interface with UTD enabled
CSCvv09565	Cellular modem does not come up after router reload from "factory-reset all" command
CSCvv09651	NAT packet drops with IN_US_V4_PKT_FOUND_IPSEC_NOT_ENABLED sub-code
CSCvv09707	Secondary KS does not push new policy after merge if IPD3P is configured
CSCvv11071	vManage is attempting to strip multiple LTE modem configs from ISR1000 and template push fails
CSCvv12398	Packet Consumed Silently on ASR1001-X
CSCvv13444	Forty gigabit ethernet link down after repeated HA SSO (switchovers) on 9800-80
CSCvv14263	Day 0 Config Bringup after Power OFF/ON C1121X-8PLTEP
CSCvv16597	Upgrading to 16.9.5 breaks the xconnect functionality of forwarding Superior BPDUs in ASR1002-X
CSCvv16686	Date field in "show crypto pki server <> cert" output is getting misaligned
CSCvv17346	unexpected reload due to Crypto IKEv2 process
CSCvv17488	Memory leak in iomd
CSCvv17730	IP DHCP Snooping not working for the voice vlan
CSCvv18392	Champion One 10 Gig SFP is not recognized by ASR-1001HX running SDWAN code,

Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.2

Resolved Bugs for Cisco IOS XE Amsterdam 17.3.2

Caveat ID Number	Description
CSCvv85766	Memory leak upon ssh/scp connections to a router

Caveat ID Number	Description
CSCuz84374	SPA modules on ASR1002-X/ASR1001-X does not get recognized under show platform
CSCvh24730	PfRv3: Crash while Printing the Same TCA Message
CSCvp24405	Router crashes after adding macsec reply-protection command on an interface
CSCvp88044	Performance Monitor crash
CSCvq42698	Update "bandwidth remaining percent" doesn't take effective reliably on datapath
CSCvr09310	vManage should be able to work with cEdge banners in the same way as with vEdges
CSCvr42504	ping is not working on port-channel after router reload
CSCvr76593	Memory leak in CC-API_VCM and CCSIP_SPI_CONTROL
CSCvr85094	Enabling Telemetry can cause router to crash.
CSCvs30625	SRTP - RTP Crash on ASR with GCM Ciphers
CSCvs42075	crash with shared-line command
CSCvs59402	Random IPSEC drops on ESP200 with esp-gcm transform set
CSCvs63606	Ping fails on hundred gig primary interface with FRR configured though MPLS traffic is not impacted
CSCvs70206	CUBE DNS cache clear should be limited only to the matched connection id
CSCvs90555	Template push fails when enabling ipv4 addr family on BGP ipv4 neighbor
CSCvs92677	Crash when removing interface not running isis but has isis config
CSCvs96344	ASR1000 : OIR after clock set doesn't save the time in RTC(recommit of CSCvr27554)
CSCvt01186	Interface does down when "l2vpn xconnect" command is removed
CSCvt02567	bgp crash @ bgp_db_ipstr2address when get bgp neighbor via bgp-oper yang
CSCvt12245	16.12.3 ZBFW-Mismatch in firewall stats between the device and vmanage
CSCvt15007	Unable to detach device from Integration Management
CSCvt16595	IOS XE SDWAN routers experience slow memory leak over time in 'ncsshd' process
CSCvt16988	Existing configuration on a cEdge could not be modified by a new template
CSCvt18190	Router crash when doing 'show bgp ipv6 unicast summary'
CSCvt19472	ASR 1000 crash at SSS manager sss_info_get_next_lem()
CSCvt19772	Stackwise Virtual FMAN-RP IPC channel stuck (paused)
CSCvt21373	unexpected reload in CPP ucode forced by nat 514 .

Caveat ID Number	Description
CSCvt33018	MACsec 128/256 XPN on 40g/100g, stop passing traffic for one of AN and interface link flap seen
CSCvt33799	Virtual address not reachable: "mac:0000:0c07:xxxx download to DP failed" for HSRP / VRRP over BDI.
CSCvt38466	SNMP TIMETICKS difference between sysUpTime vs ipslaEtherJAggStatsStartTimeId
CSCvt40021	Omp-tag is not being set via route-map configuration under bgp
CSCvt46635	Traffic is not getting optimized and it goes as PT connections on CSR router reload in 17.2.1
CSCvt54359	BGP config does not rollback if template push errors out
CSCvt57181	Leaf sends packets to a wrong BVI MAC of ASR GOLF routers
CSCvt58616	L2VPN Crash @ Process = XC Mgr
CSCvt58858	Incorrect CEF programming for local SVI
CSCvt60040	VPLS:MAC learning not happening on SSO
CSCvt60979	1731: ODN Policy for Global prefix still UP even after withdrawing global routes
CSCvt65588	FlexVPN IKEv2 Tunnel route removed after establishing new IKEv2 SA to another peer
CSCvt67752	Object (IPv6 ACL) stuck in forwarding data plane. No ipv6 traffic goes towards the upstream router
CSCvt73592	missing/corrupt IOS-XE PKSC10 format
CSCvt74694	Cert validation failures seen for traffic after template push with SSL
CSCvt76409	Crash due to "Crimson flush transactions Process"
CSCvt78405	Code review: Just fire assert when we reach limit of counter
CSCvt89337	Incorrect Source IP when resolving DNS
CSCvt89441	IOS-XE device crashed with CGD shared memory corruption freed by FMAN-FP
CSCvt90424	CRC increasing on down int Te0/0/20
CSCvt94577	Incorrect CEF entry for LISP action signal-fwd
CSCvt98034	BGP communities: changes to route-map which sets BGP communities discards existing communities
CSCvu00280	RP3/ESP100/X: Traffic loss of over 1s at FP switchover (plain ipv4)
CSCvu21761	RAR: PADG and PADC are not being consumed properly. PPPoE session statistics are not matching.

Caveat ID Number	Description
CSCvu22003	vManage FW dashboard doesn't show all matched applications
CSCvu22576	Keepalive CLI needs to be unhidden for GRE tunnel
CSCvu23567	RSP3: BGP crash seen on Stand by router when 100 BGP sessions are established.
CSCvu26678	Some qos config lost during upgrade to 17.02
CSCvu26741	Punt-Keepalive crash with lsmapi_lo_drv and container app traffic.
CSCvu27813	Complete Traffic drop seen on Head Node Post configuring Binding SID on PFP Policy
CSCvu34381	Packets are not dropped as expected in selfzone to zone vpn 0 firewall config
CSCvu52218	Router crashes frequently on NBAR
CSCvu54786	Crash on configuring a highest key identifier for OSPF authentication under an interface
CSCvu65669	Traffic drop from branch overlay ping to service side without zp vpn1 to vpn1 when FW & IPS enabled
CSCvu66723	Evaluation of CVE-2020-10188 - Cisco IOS XE Persistent Telnet
CSCvu70571	SD-WAN router ASR1001-X crashes when object-group service configuration is added
CSCvu80644	LSP Checksum error when default-info originate is configured
CSCvu87786	CUBE Segmentation Fault @ sipSPIFreeOneSCB due to corrupt ccb
CSCvu89033	Template push error due to NAT-MIB process helper traceback/warm restart
CSCvu99616	Snort initiate reset and Failed to load - Real websites in Browser
CSCvv05893	CUBE router crashed due to memory corruption in subscription control block
CSCvv05895	ASR1001-X: Issue a cpld reset instead of reboot in kcrash
CSCvv13193	Memory leak 'Admin group' with some triggers in ISIS
CSCvv16164	RSVP TE is not working for broadcast interfaces due to CSCvu94532
CSCvv20380	Removing and Adding Bulk ACL leads to Tracebacks and Error-Objects

Open Bugs for Cisco IOS XE Amsterdam 17.3.2

Caveat ID Number	Description
CSCvs87249	DHCP Server configuration inn Vmanage Template for a Cedge change order of the DNS servers
CSCvt51568	Unexpected Reload due to Sessmgr
CSCvt76844	ASR1002-X ESP crash in multikey_hash_ager_tw_timer_to()

Caveat ID Number	Description
CSCvt85954	IWAN routers ISR4K unexpected reload multiple times
CSCvu04160	Unexpected Reload in Device Classifier Code due to Segmentation Fault
CSCvu27910	Controller crashes when FNF is configured under physical interface
CSCvu41583	Controller crashes when FNF is configured under physical/port-channel interface
CSCvv03229	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
CSCvv11423	Remote EID space prefix not installed in CEF when overlapping prefix exists as Local EID
CSCvv47691	Reload: IOS-XE router crashing due to DN mismatch
CSCvv49841	ASR 1002-HX crashes due to stuck threads.
CSCvv65068	Crash after flexible netflow cache cleanup
CSCvv71238	Sup reload with cpp-bqs fatal

Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.3

Resolved Bugs for Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
CSCuv97577	Mishandling of dsmpSession pointer causes a crash
CSCvu23516	Static routes pointing to interface tunnel not valid after tunnel's source interface flaps.
CSCvu32771	IOSd Crash due to Segmentation fault at SISF Main Thread
CSCvv03229	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
CSCvv09342	Cloud Express probes fails when two default rules are present
CSCvv40006	Traceback: IP SLA triggers INJECT_HDR_LENGTH_ER and INJECT_FEATURE_ESCAPE log message
CSCvv61770	Crash seen in isis_sr_uloop_lspdb_dump with 'debug isis microloop' enabled
CSCvv64633	BGP: advertised community list is malformed due to GSHUT community
CSCvv71775	Cellular interface down/up frequently occurs with DoCoMo MVNO sim
CSCvv78028	No responder-bytes from cEdge when UTD is enabled
CSCvv79273	Router may crash when using Stateful NAT64
CSCvv88621	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage

Caveat ID Number	Description
CSCvv93925	ASR 1000 Series crashes when ACL deleted following object-group modification
CSCvv94743	Data Plane fails over L2TPv3 while disabling VLAN limit restrictions with ASR1002-HX
CSCvw06719	Platform ipsec reassemble transit" tail-drops unencrypted IPv4 Fragments with specific payload
CSCvw06780	DMVPN with ipv6 link-local address do not register to HUB
CSCvw09486	Router might crash after apply a class-map in input direction with bandwidth percentage
CSCvw10972	NAT64 ALG: Router crashes on nat64_process_token
CSCvw11902	Passive FTP doesn't work with NAT
CSCvw16643	Device Template failing to attach after changing few device variables
CSCvw19171	Smart license registration through explicit mode proxy server
CSCvw22760	MACSEC MKA stops forwarding data after every 3rd rekey
CSCvw23041	Crash seen on Fugazi due to %CPPHA-3-FAILURE: R0/0: cpp_ha: CPP 0 failure Stuck Thread(s)
CSCvw30128	"Sequence id not available" in ACL code after DNAC upgrade
CSCvw31389	Pktlog functionality is broken
CSCvw32481	EVPN Type-2 IP/MAC route is created for not-connected SVI
CSCvw33113	Unexpected reload in NHRP when access to an invalid memory region
CSCvw34157	APPNAV CFT Crashes
CSCvw37109	Pseudowire interface may be unexpectedly removed from VFI on unrelated configuration change
CSCvw38433	OMP-Agent Routes in EIGRP changes AD to 252 on non-SDWAN devices
CSCvw39383	CPP ucode crash with fw_base_flow_create
CSCvw40079	ASR 1000 Series crashes in ipv6 mgd timer code when removing vrf config
CSCvw41482	SSH with Certificate authentication does not work after upgrade to 17.3.1
CSCvw47640	ASR 1000 Seriesdoing KS role for GETVPN is sending malformed rekey packets
CSCvw47800	HSL Export over VASI Interface causes Netflow v9 Template Flooding
CSCvw48800	Unable to transfer 1500 byte IP packet when using BRI bundled Multilink
CSCvw54076	[SIT]: BFD sessions not established between Edges, with UTD enabled

Caveat ID Number	Description
CSCvw55030	Dynamic Nat pool "ip aliases" are not created on the device
CSCvw55658	EPA-QSFP-1X100GE / IOS XE 17.3 / incorrect LED and link status
CSCvw56517	LMR Unable to hear first seconds of audio
CSCvw57670	ASR 1000 Series: Critical process plogd fault on rp_0_0
CSCvw57860	Duplicate entries seen in MAC filter table.
CSCvw58560	FlexVPN reactivate primary peer feature does not work with secondary peer tracking
CSCvw62284	ASR1000 ISG: Crash when processing DHCP Request
CSCvw62805	SDWAN ZBFW CPU punted traffic mishandling -- Out2In packet looped
CSCvw64559	Throughput license grace period starts counting down after upgrade router software
CSCvw68171	Duplicate Bytes & Packet when Q in Q is configured
CSCvw76715	OpenSSL vulnerability (CVE-2020-1971) evaluation for IOS-XE
CSCvw77485	Router may not send PIM Register message if RP is reachable over TE tunnel
CSCvw80173	BGP AS-path prepend: cEdge won't update correctly better prepended route.
CSCvw84759	Device is crashing after Device Access Policy is attached
CSCvw84883	DDNS feature triggers crash on 16.X/17.X releases due to memory corruption
CSCvw86295	Crash while configuring l2vpn evpn instance for VXLAN
CSCvx08852	Not able to create VFI instances
CSCvx12686	ACL: Crash triggers after 'clear ip access-list counters' is used with more than 1k ACEs
CSCvx19209	ISIS crash in isis_sr_tilfa_compute_protection
CSCvx36844	Control plane hitting EID prefix entry limit for MAC after upgrade

Open Bugs for Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
CSCvv82322	Link issue when using macsec
CSCvv99281	BQS crash on PPPoE session churn overnight
CSCvw11607	Crash in DSP causing an mcpcce-lc-ms core file
CSCvw67366	ASR1002-X: Punt keepalive crashed due to bqs related interrupt
CSCvw80667	Severe traffic disruption due to non-stop flapping of MACSEC enabled interfaces post RP3 switchover

Caveat ID Number	Description
CSCvw87256	ASR 1000 Series cpp_cp_svr crash with frequent underlay route removal and tunnel source changed every 1 second
CSCvw89147	Crash at the moment of calculating tcp header
CSCvw92643	Netflow crash at fnf_ipv6_output_feature_final_internal with flow record on IPv6 IPsec tunnel.
CSCvx08118	Bug to further address CSCvt08179 : QFP crash due to hardware interrupt
CSCvx24332	ucode crash with firewall timer lock
CSCvx24707	bgp-neighbor down when push banner configuration failure
CSCvx25680	IOS-XE Memory Leak in SSS Manager
CSCvx26652	Router crash observed when AppNav Cluster delete with service-insertion enabled on LAN interface
CSCvx32807	False positive alarm: IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL Fan Tray Bay 1 Fan Tray Module Missing
CSCvx35902	fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash

Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.4a

Resolved Bugs for Cisco IOS XE Amsterdam 17.3.4a

Caveat ID Number	Description
CSCvv92064	App-aware policy need to be honored when queuing is not set by localized policy
CSCvv95280	Cisco 1001-X ASR may crash when ZBFW HSL(High Speed Logging) is configured
CSCvv99281	BQS crash on PPPoE session churn overnight
CSCvw05211	Pre-mature session deletion leading to churn and lower TPS at scale
CSCvw11607	Crash in DSP causing an mcpc-c-ic-ms core file
CSCvw21378	Cisco 1001-X ASR built-in Tengig interfaces' counters increasing continuously and port stay up/up w/o SFP
CSCvw52574	Cisco 1000 Series ASR configured with 'no ip unreachable' sending ICMP Type 3 Code 13
CSCvw81572	Multiple crashes cpp_cp_svr and qfp-ucode on 16.12.4
CSCvw88098	cEdge crashes while running web traffic testing with security features enabled

Caveat ID Number	Description
CSCVw90220	Crash at #12 0x00007f010f4cb9db in cpp_bqs_rm_yoda_get_flush_obj while subscriber bringup
CSCVw94434	BQS crash seen at cpp_qm_event_proc_defer_cb
CSCVw98579	BQS crash seen in 17.3 while bringing up 30k PPPOE sessions
CSCVx02009	cEdge running 17.3.2 crashed - Critical software exception / IOSXE-WATCHDOG: Process = SNMP ENGINE
CSCVx21270	SDWAN custom policy that does not look to be programmed correctly on the cedge platform
CSCVx23159	FW-4-ALERT_ON: (target:class)-():getting aggressive seen when no half open feature configed
CSCVx32670	Wrong reload reason reflected after a power outage.
CSCVx36146	DCHP offer frame getting dropped on cEdge ISR4431 due to Policy
CSCVx36205	Removing and Adding Bulk ACL leads to dataplane programming failure
CSCVx36763	Zone Based Firewall on cEdge router dropping web traffic with the reason Zone-pair without policy
CSCVx44834	Cisco 1000 Series ASR- ACE entry added after object-group is missing in hardware causing packets drops
CSCVx45788	cannot apply ciscosdwan.cfg due to vpg-log-server-acl ACL on VirtualPortGroup0 for logging
CSCVx53049	Crash when TPOOL is updating and 'wr mem' is issues at same time
CSCVx57615	ZBFW blocking ACK packets for applications using cloudexpress SaaS set to use a Gateway with synsent
CSCVx64846	"show sdwan policy service-path/tunnel-path" command cause device crash
CSCVx69830	Cisco 1000 Series ASR: BQS crash seen at cpp_qm_event_proc_defer_cb
CSCVx72232	rbuf-ooh crash in HSL
CSCVx73741	custom app not getting detected after attached removed and re-attached- app-visibility is disabled
CSCVx75330	fman_rp memory leak in acl_config_bind_v4_acl_message function.
CSCVx77203	[17.5] Router crashed when sending traffic through non-SDWAN interface with DIA NAT + debug enabled
CSCVx78215	An IOS XE device might crash at DoubleExceptionVector
CSCVx79113	SDWAN cedge : traffic simulation tool shows traffic blackhole

Caveat ID Number	Description
CSCvx88246	Packets dropped due to firewall + data policy interop issue
CSCvx89710	SCEP: CA server fails to rollover CA certificate with error: "Storage not accessible"
CSCvx97718	vtcp frees rx buffer when packet with expected next sequence arrives with no payload; phones reset
CSCvy30209	IOS-XE cpp ucode crash with fragmented packets
CSCvy32673	GD/1hx-Interface doesn't come up when reboot/upgrade device with autoneg enabled on 10G SFP+ Port

Open Bugs for Cisco IOS XE Amsterdam 17.3.4a

Caveat ID Number	Description
CSCvt62123	DMVPN - after removing IPsec, traffic is dropped on a tunnel interface
CSCvu06483	Data consistency errors seen on configuring mac-sec on the underlay interface with ipsec configured
CSCvv17346	unexpected reload due to Crypto IKEv2 process
CSCvv38438	Watchdog timeout due to Crypto IKMP
CSCvv48885	can not update local-address in a crypto keyring
CSCvv82322	Cisco 1001-X ASR and Cisco 9000 Series ASR: Link issue when using macsec
CSCvw48943	crypto ikev2 proposals are not processed separately
CSCvw60359	cEdge-policy: set next-hop-ipv6 is not working next-hop-ip (ipv4) is working.
CSCvw67366	Cisco 1002-XASR: Punt keepalive crashed due to bqs related interrupt
CSCvw73769	17.4 ZBFW:Cpp_cp crash seen when a rule is added at beginning in automation on Cisco 1000 Series ASR
CSCvw91361	Crash when issuing "show crypto isakmp peers config"
CSCvw94166	IKE should have a mechanism to alert or mitigate resource exhaustion due to QM flooding
CSCvx08118	Cisco 1001-X ASR: Bug to further address CSCvt08179 : QFP crash due to hardware interrupt
CSCvx32807	False positive alarm: IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL Fan Tray Bay 1 Fan Tray Module Missing
CSCvx41588	Rapid memory exhaustion due to excessive logging
CSCvx74212	IKEv1 IPsec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ

Caveat ID Number	Description
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
CSCvy35853	Cisco 1000 Series ASR- egress byte counter on MIP100 10GE interface is inaccurate
CSCvy54314	Data-policy local-tloc with app-route is dropping packets when SLA is not met
CSCvy58115	Cedge : Cloudexpress Office 365 probes are hitting 100% loss
CSCvy78123	cEdge: High CPU usage due to Multicast and Data Policy configuration.
CSCvy82696	cEdge dropping packets [combination /16, /17 data prefix with multiple ports in policy]
CSCvy91411	AAR not correctly programmed in Cisco 1001-X ASR
CSCvy69555	Unable to fetch eigrp prefix, nexthop, omptag, and route origin
CSCvu62879	Crash@bgp_perform_general_scan

Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.5

Resolved Bugs for Cisco IOS XE Amsterdam 17.3.5

Caveat ID Number	Description
CSCvw84019	show access-lists template summary not reflecting correct data
CSCvo41609	GETVPN: Clearing members on Key Server causing rekey processing failure on GMs
CSCvz26211	flow monitor statistics missing when reloading with configuration
CSCvy67657	crypto ipsec security-association dummy leads to packet loss
CSCvy74799	Ucode crash observed at tw_bad_timer_bucket () at ../../infra/tw_timer.c:918
CSCwa15132	DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum
CSCvy85281	Crash triggered by "crypto gdoi ks rekey replace-now"
CSCvy54606	CVLA need to reserve at least 50M memory for low-end DRAM platform
CSCwa10915	ASR1k PFRv3: Elephant flow will trigger performance monitor exporting more than 50% byte loss
CSCvy64468	ASR1002-HX crashed after removing then applying the ZBF configuration.
CSCvx39529	IKEv1/IKEv2 "show crypto session brief" output empty
CSCvy24571	Static NAT conflicts/overwrites with Port-forwarding
CSCvx22349	After reload or switchover, redundant ESP goes offline->online (transient issue)
CSCvy50292	Standby router crashes ZBFW on VASI interfaces with FTP or SIP TCP traffic

Caveat ID Number	Description
CSCvy39195	ESP200-X crash PA2_CSR32_TOP_CSR_PA_ERR_LEAF_INT__INT_PPE_INT1 with PPPoE/L2TP sessions
CSCvz86591	VRF-aware static NAT with route-map and reversible not working
CSCvx32807	False positive alarm: IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL Fan Tray Bay 1 Fan Tray Module Missing
CSCvy44951	ESP Unexpected Reboot on Broadband Intelligent Services Gateway During Session Clean-up
CSCwa36699	Prefetch CRL Download Fails
CSCvy35853	ASR1k- egress byte counter on MIP100 10GE interface is inaccurate
CSCvz34290	no ip nbar resources flow max-session does not restore default platform session limits
CSCvz73780	memory leak with fman_cc process when SM-X-G4M2X module installed
CSCvy52359	Segmentation fault(11), Process = CTS CORE - crash in ISR 4k
CSCvx41588	Rapid memory exhaustion due to excessive logging
CSCvt66541	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted
CSCvv38438	Watchdog timeout due to Crypto IKMP
CSCvv17346	unexpected reload due to Crypto IKEv2 process
CSCvz58895	IOS-XE unable to export elliptic curve key
CSCvy89785	OSPFv3 adjacency won't come up after "ospfv3 authentication ipsec" is applied on Tunnel interface
CSCvz03342	Multicast boundary command on tunnel interface DMVPN network is sending ttl=1 packet
CSCvw91361	Crash when issuing "show crypto isakmp peers config"
CSCvy69846	Guestshell:.py files stored under /home/guestshell are lost after reboot on 1ng device
CSCvw48943	crypto ikev2 proposals are not processed separately
CSCvz11362	ASR fails to install rekey causing traffic drop

Open Bugs for Cisco IOS XE Amsterdam 17.3.5

Caveat ID Number	Description
CSCvy78087	Qos download failed with FW policy when rebooting device
CSCvv81296	Protocol specific change for base path

Caveat ID Number	Description
CSCvw81274	Opflex generated Route Distinguisher is not globally unique on ASR1k
CSCvw70009	ASR1K: fman_rp crash seen on 16.9.X when "show platform software nat RP active logging" is run
CSCvx94323	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut
CSCwa49902	MGCP automatic configuration fails after IOS-XE upgrade on ISR4k
CSCvx35902	fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash.
CSCwa58911	Removing service-policy from the Zone-pair causes device crash
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
CSCvv92630	PKI http client fails to handle 1xx and 2xx responses
CSCvy79601	ASR1001X gets rebooted when Tunnel move across two egress interfaces with QoS MPoL policy config
CSCwa39615	Unexpected reload due to cpp-mcpl0-ucode failure
CSCwa17720	Router rebooted de to watchdogs after issuing the commands sh crypto mib ipsec commands
CSCvw67366	ASR1002-X: Punt keepalive crashed due to bqs related interrupt
CSCvz74322	"Shutdown" command visible in running config after reload of ASR 1002-HX
CSCvz53819	ZBFW : ARStandby drops seen on New Active during RG switchover
CSCwa34648	Incorrect OMP Labels in On-Demand Tunnel H/S Topology
CSCvz54262	ASR1001X crash at CFT after scaling up to 4M flows when internet link up from 2Gbps to 10Gbps
CSCvx64449	%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: mac verify failed due to ip rtp header-compression iphc-format
CSCvw13048	crash observed at NHRP while using summary-map
CSCvy57681	Unexpected reboot of IOS-XE Router in BQS QM @ cpp_qm_proc_rt_commit
CSCvx74212	IKEv1 IPsec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ
CSCwa51837	Crash on cpp process when QoS policy configuration is being applied
CSCvv82322	ASR1001-X and ASR9K: Link issue when using macsec
CSCwa18588	IOSd Nhrp core due to a segmentation fault when disabling Pfr IWANs

Caveat ID Number	Description
CSCvz87460	ASR 1000-RP2 VID>V07 16.9.7 MD5 signature does not match failure while upgrading to 17.3(1r) rommon
CSCvt62123	DMVPN - after removing IPSec, traffic is dropped on a tunnel interface
CSCwa51443	Incorrect check of the TCP sequence number causing return ICMP error packets to drop (Thousandeyes)
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes
CSCvy54048	CPP Unexpected Reboot While Freeing CVLA Chunk
CSCvz62601	ASR1000-MIP100 / IOS XE 17.3.2 / high CPU on LC process mcpecc-lc-ms and link flaps
CSCwa58533	C1100 Unexpected reboot with Critical process fman_fp_image fault on fp_0_0
CSCvu77711	Missing Mandatory Transform Type (ESN) in IKEv2 ESP Protocol
CSCwa30988	CoS preservation not working for the services EVPL and EPL tunnel
CSCvy30606	Device: sdn-network-infra-iwan key does not update successfully under network disruption situation
CSCvz65545	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535
CSCvv55742	GETVPN-ipv6 & LISP support on C900 platforms
CSCwa29964	SCEP fails if AAAA DNS reply is received and source interface has no IPv6 address
CSCwa52627	ASR1K / 17.3 / "sh int transceiver" reports incorrect Tx/Rx optical power values
CSCwa57462	The router reload unexpectedly due to Cellular CNM process.
CSCwa61238	FlexVPN per-user inline ACL from Radius not installed
CSCvx28426	Router may crash due to Crypto IKMP process
CSCvy37152	%CRIMSON-3-DATABASE_MEMLEAK: Database memory leak detected
CSCwa37243	TenGigabitEthernet0/0/0-1 port keeps up/up status even the peer connecting port had been link down

Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.6

Resolved Bugs for Cisco IOS XE Amsterdam 17.3.6

Bug ID	Description
CSCwb46649	NAT translation don't show (or use) correct timeout value for an established TCP session.
CSCvy78087	Qos download failed with FW policy when rebooting device.

Bug ID	Description
CSCvz91309	Crash due to IOSXE-WATCHDOG due to management port traffic storm.
CSCwa95092	When object-group used in a ACL is updated, it takes no effect.
CSCwc36274	CPP crash with performance monitor.
CSCwc19758	CRC counter doesn't increase in "show interfaces" on device with EPA/MIP.
CSCvz87460	MD5 signature does not match failure while upgrading to 17.3(1r) rommon.
CSCvy52143	ENH: Address the memory fragmentation in "IPSEC Key" process.
CSCwc37320	RP switchover causes linecard NFS mount failure resulting in memory leak.
CSCwa47219	Crash on ipv4_nat_get_all_mapping_stats due to NULL pointer of mapping_hash_table.
CSCvz81956	CHASSIS_MONITOR_ONLINE_TIME_EXCEEDED: R0/0: cmand: Reloading F0 because it has failed to come online.
CSCwc43794	Device VRF+NAT Outside Source Static - Drop packets during FTP (Active-mode) execution.
CSCwc20005	[XE ETA] IDP record is incomplete when traffic is fragmented.
CSCwa25614	%SCHED-3-SEMLOCKED: SIP0/1: Exec attempted to lock a semaphore, already locked by itself.
CSCvz62601	High CPU on LC process mcpcclc-ms and link flaps.
CSCvy37152	Oper database memory leak detected.
CSCwc10160	Device with EPA interface - "giants" counter keeps increasing after initial reception of giant.
CSCvz95158	IPSec LED doesn't lit even though module is correctly installed.
CSCwb23043	MACSEC not working on subinterfaces using dot1q >255.
CSCwc06967	IOS PKI client uses incorrect search filter for CRL retrieval using LDAPv3.
CSCvz92994	Lack of MAC address in inform event message.
CSCwcl3013	IPSec Key engine process holding memory continuously and not freeing up.
CSCwa17720	Router rebooted due to watchdogs after issuing the commands SH Crypto MIB IPSec commands.
CSCwb65455	Renewing hardware wan edge cert shows old cert serial/valid date in control local-properties.
CSCwb85046	Device reloads when group-range is configured under an interface Group-Async.
CSCwb91026	Traffic is hitting wrong sequence in the data policy.
CSCwa66916	VG450 - SCCP auto-configuration issues with multiple protocols.

Bug ID	Description
CSCwb25913	(Rework): After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwb04815	NHRP process taking more CPU with IP NHRP redirect configured.
CSCwa72273	ZBFW dropping return packets from Zscaler tunnel post cedge upgrade.
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map.
CSCvy69405	Appnav-XE connections are going as passthrough unsupported.
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored.
CSCwa80826	Platforms running 17.x - crypto ipsec policy installation fails.
CSCwa67398	NAT translations do not work for FTP traffic.
CSCwa51443	Incorrect check of the TCP sequence number causing return ICMP error packets to drop (Thousandeyes).
CSCwb24123	Registration of spoke fails with dissimilar capabilities w.r.t to HUB.
CSCvw16093	Secure key agent trace levels set to Noise by default.
CSCwa84919	"Revocation-check crl none" does not failover to NONE DNAC-CA.
CSCwb14020	Serial interface stuck in "line protocol is down" state after it went down and it is recovered.
CSCvu70609	Observed crash in device with prd10 image.
CSCwb15331	Keyman memory leak using public keys.
CSCvy30606	Device fails to update sdn-network-infra-iwan key after 1 year.
CSCwb76988	IKEv2 fragmentation causes wrong message ID used for EAP authentication.
CSCwb99793	CRL verification failure result 400 Bad Request with DigiCert.
CSCvz34668	Static mapping for the hub lost on one of the spokes.
CSCwb95559	Packet sanity failed for resolution reply on spoke due to missing SMEF capability.
CSCwa68540	FTP data traffic broken when UTD IPS enabled in both service VPN.

Open Bugs for Cisco IOS XE Amsterdam 17.3.6

Caveat ID Number	Description
CSCvz65764	Peer MSS value showing incorrect.
CSCwb53709	PRP trailer frames were trunked in xconnect on Utah platform.

Caveat ID Number	Description
CSCvw81274	Opflex generated Route Distinguisher is not globally unique on device.
CSCvw70009	Device crash seen when "show platform software nat RP active logging" is run.
CSCwc18977	Crash with "IPE_CPE_U14_CSR32_IPE_CPE_ERR_CPE_MISC_LEAF_INT__INT_CPE_MALGN_ADDR_ERR" error.
CSCwc03478	VTCP does not support L2 correctly.
CSCvx35902	fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash.
CSCwb61073	BQS Failure - Qos policy is missing in hardware for some Virtual-Access tunnels after session flaps.
CSCvu06483	Data consistency errors seen on configuring mac-sec on the underlay interface with ipsec configured.
CSCvw67366	Punt keepalive crashed due to bqs related interrupt.
CSCwb55514	Crash seen after enabling "platform qos port-channel-aggregate".
CSCvz74322	"Shutdown" command visible in running config after reload of device.
CSCwc59598	Device statistics collection causing service-side BFD to flap on every collection interval.
CSCvw13048	Crash observed at NHRP while using summary-map.
CSCwb76976	NETFLOW SIP destination/source field contains garbage value.
CSCwa30988	CoS preservation not working for the services EVPL and EPL tunnel.
CSCwc26669	TLB miss for lock address during FNF cache lookup.
CSCwa97171	PRP frames not transparent transmitted over L2TPv3 or EoMPLS tunnel.
CSCwb03893	When MACSEC dot1q-in-clear 1 is enabled on interfaces there is traffic drop.
CSCwb51238	Router reload unexpectedly two times when enter NETFLOW show command.
CSCvz59621	MKA Session not coming up on EVC.
CSCwa98617	Memory leak in AEM chunks related to firewall.
CSCwc20286	Octeon processor hang followed by ESP100 crash.
CSCwb73395	Need CLI option to disable ALG.
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes.
CSCvy90763	PYON: Adjusting new text segment to address L2i rejections issues with SDWAN profiles.

Caveat ID Number	Description
CSCvz65545	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535.
CSCwa52627	Incorrect Tx/Rx optical power values reported for QSFP transceivers.
CSCwc20171	Fragmented packets crashes while allocating memory.
CSCvx00230	Device may show input/output rate values even if the interface is in admin down state.
CSCwb72336	ICMP traceroute return packet not classified based on FW override port info.
CSCwa76570	ISG / Crashes due to %IDMGR-3-INVALID_ID: bad id in id_delete during session roaming.
CSCvx94323	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut.
CSCwa43562	Device link goes err-disabled due to link-flap after reloading Catalyst 8300 peer device.
CSCwb66749	When configuration ip nat inside/outside on VASI interface,ack/seq number abnormal.
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map.
CSCwa13553	Device QFP core due to NAT scaling issue.
CSCvy79601	Device gets rebooted when Tunnel move across two egress interfaces with QoS MPoL policy config.
CSCwa69101	ISG: initiator unclassified ip-address LQIPv4 command has no effect.
CSCvz53819	ZBFW : AR Standby drops seen on New Active during RG switchover.
CSCvz63684	EWC HA pair experiencing IOS tracebacks, followed by KEYMAN crash.
CSCwc22314	RTSP Traffic not being rewritten by NAT.
CSCwb17282	Router crashing when clearing a VPDN session.
CSCvx74212	IKEv1 IPsec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ.
CSCwb08057	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
CSCwc25291	[Verizon CAP]NIM-LTE-EA No data - requires subslot reload to recover.
CSCwb14888	Unable to remove "switchport mode access" and "switchport nonegotiate" at the same time.
CSCwb12647	Device crash for stuck threads in cpp on packet processing.
CSCwc39865	Subscriber session getting stuck and needs clearing it manually.
CSCwa57462	The router reload unexpectedly due to Cellular CNM process.
CSCvt62123	DMVPN - after removing IPsec, traffic is dropped on a tunnel interface.

Caveat ID Number	Description
CSCwb41907	CPP uCode crash due to IPC congestion from DP to CP.
CSCwb46968	Device template attachment causes pppoe commands to be removed from ethernet interface.
CSCvy54048	CPP unexpected reboot while freeing CVLA chunk.
CSCwa76260	IKEv2 deprecated ciphers denied by crypto engine CDSL - PSB security compliance - DES, 3DES, DH1/2/5.
CSCvu77711	Missing mandatory transform type (ESN) in IKEv2 ESP Protocol.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCvv55742	GETVPN-ipv6 & LISP support on device platforms.
CSCwc30050	UTD: Exception in utd_logger.py due to missing extra-data in AMP alert.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCvx73750	Hightower 5G light is blue when 4G LTE is in use.
CSCvx28426	Router may crash due to Crypto IKMP process.

Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.7

Resolved Bugs for Cisco IOS XE Amsterdam 17.3.7

Bug ID	Description
CSCwd06372	Unconditional excessive logging in EoGRE tunnel error handling case.
CSCwc26669	TLB miss for lock address during FNF cache lookup.
CSCwd25107	Interface VLAN 1 placed in shutdown state when configured with ip address pool .
CSCwc84967	Intermittent double DTMF due to changing timestamp on a DTMF event.
CSCwd30578	Wired guest client stuck at IP_LEARN with DHCP packets not forwarded out of the foreign to anchor.
CSCwc82140	QFP crash when ZBFW configuration features log dropped-packets configuration.
CSCwa57462	The router reload unexpectedly due to Cellular CNM process.
CSCwb41907	ezPM(performance monitor) error logs may cause uCode crash due to congestion of IPC from DP to CP.
CSCwd81357	QoS Classification not working for DSCP or ACL + MPLS EXP.
CSCwc72923	ERROR info: Router configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt.
CSCwc70511	Router reloads unexpectedly during NHRP processing.

Bug ID	Description
CSCwd76176	DSPware 55.1.6 Release targeting v173_throttle.

Open Bugs for Cisco IOS XE Amsterdam 17.3.7

Bug ID	Description
CSCvz89354	Router crashes due to CPUHOG when walking Cisco Flash MIB.
CSCvz73202	TCAM parity error - QFP crash with a scale configuration.
CSCwa69101	ISG: initiator unclassified IP-address LQIPv4 command has no effect.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCvx77024	IPv6 DMVPN - NBMA address not getting preserved.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCvy38743	CISCO-CLASS-BASED-QOS-MIB doesn't work with LTE Cellular interface on device after reload.
CSCwa76570	ISG/Crashes due to %IDMGR-3-INVALID_ID: bad id in id_delete during session roaming.
CSCwc39865	Subscriber session getting stuck and needs clearing it manually.
CSCwa98617	Memory Leak in AEM chunks related to Firewall.
CSCvz63684	EWC HA pair experiencing IOS Tracebacks, followed by KEYMAN crash.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCwa43562	Device link goes err-disabled due to link-flap after reloading peer device.
CSCwb61073	BQS Failure - Qos policy is missing in hardware for some Virtual-Access tunnels after session flaps
CSCwa67851	Router traceback and reload when different encapsulation used on xconnect interfaces.
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface.
CSCwc76044	Interface stats are not getting updated for port-channel.
CSCvx35902	fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwb78173	CSDL failure: IPSec QM use of DES by Encrypt Proc is denied.
CSCwe41234	VG450 VMWI race condition causes no ringing for analog phones.

Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.8

Resolved Bugs for Cisco IOS XE Amsterdam 17.3.8

Bug ID	Description
CSCwd73783	Observed QFP-UCode-WLC crash.
CSCwf45769	Ingress and Egress Bytes counters can suddenly increase and are not accurate for Sub-Interfaces.

Open Bugs for Cisco IOS XE Amsterdam 17.3.8

Bug ID	Description
CSCwa69101	ISG: initiator unclassified IP-address LQIPv4 command has no effect.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwf48808	FlexVPN: Stale client routes stuck in RIB on FlexServer.
CSCwe60059	Crash when using dial-peer groups with STCAPP.
CSCwa76570	ISG / Crashes due to %IDMGR-3-INVALID_ID: bad ID in id_delete during session roaming.
CSCwc39865	Subscriber Session getting stuck and needs clearing it manually.
CSCvz63684	EWC HA pair experiencing IOS Tracebacks, followed by KEYMAN Crash.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCwd03931	Device crashes due to cpp_cp_svr fault on fp_0_0 (rc=134) when applying umbrella dnsencrypt to profile.
CSCwb03455	Inter-vrf route leaking not working and packet drop seen due to Ipv4Unclassified.
CSCwf03193	Device crash with crashinfo files were generated with Segmentation fault, Process IPSEC key engine.
CSCwa43562	Device link goes err-disabled due to link-flap after reloading peer device.
CSCwf80400	IOS XE router may experience unexpected eeset while executing show utd engine standard statistics .
CSCwe12194	Auto-Update Cycle incorrectly deletes certificates.
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface.
CSCwe39011	GARP on port up/up status from router is not received by remote peer device.
CSCvy54048	CPP unexpected reboot while freeing CVLA chunk.
CSCwb78173	CSDL failure: IPsec QM Use of DES by encrypt proc is denied.
CSCwb61073	BQS Failure - QoS policy is missing in hardware for some Virtual-Access tunnels after session flaps.

Bug ID	Description
CSCvz73202	Device TCAM parity error - QFP crash with a scale configuration.
CSCwb55514	Unexpected reboot of the ESP seen after enabling platform qos port-channel-aggregate .
CSCwh26209	Router crashed with no UCode due to possible dataplane memory corruption in NAT client.
CSCwa98617	Memory Leak in AEM chunks related to Firewall.
CSCwe25815	Crash due to DTL push/pop on wait loop.
CSCvy73165	Remove auto-negotiation support on 10G dual-rate interfaces.
CSCwf80191	Flowspec on device won't revoke.
CSCwc76044	Interface stats are not getting updated for port-channel.
CSCwf99947	Crash when modifying tunnel after running show crypto commands.
CSCvx35902	fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.

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
- ASR 1000-RP3

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](#)
- [Command Reference 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](#)
- [Deferral Notices](#)
- [Cisco Bulletins](#)

