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

First Published: 2020-08-15

Last Modified: 2023-10-28

Cisco CSR 1000v Series Cloud Services Routers Overview

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

Virtual Router

The Cisco Cloud Services Router 1000V (CSR 1000V) is a cloud-based virtual router that is intended for deployment in cloud and virtual data centers. This router is optimized to serve as a single-tenant or a multitenant WAN gateway.

When you deploy a CSR 1000V instance on a VM, the Cisco IOS XE software functions as if it were deployed on a traditional Cisco hardware platform. You can configure different features depending on the Cisco IOS XE software image.

Secure Connectivity

CSR 1000V provides secure connectivity from an enterprise network such as a branch office or a data center, to a public or a private cloud.

Hardware Requirements

For hardware requirements and installation instructions, see the Cisco CSR 1000v Series Cloud Services Router Software Configuration Guide .

Software Images and Licenses

The following sections describe the licensing and software images for CSR 1000V.

Cisco Smart Licensing

The Cisco CSR 1000V router supports Cisco Smart Licensing. To use Cisco Smart Licensing, you must first configure the Call Home feature and obtain the Cisco Smart Call Home Services. For more information, see Installing CSR 1000V Licenses and Smart Licensing Guide for Access and Edge Routers.

For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

Cisco CSR 1000V Evaluation Licenses

Prior to Release 3.13, Cisco provided a built-in evaluation with the CSR 1000V instance, where you could use the Premium Technology Package at a maximum throughput of 50 Mbps for 60 days. With Release 3.13 and later, Cisco has moved to a self-service model to provide the flexibility of trialing additional technology packages and higher throughputs.

Evaluation licenses are valid for 60 days and are available with a valid Smart Account. To request an evaluation license, contact Cisco or a qualified Cisco partner.

The following evaluation licenses are available:

- IPBASE technology package license with 10 Gbps maximum throughput
- SEC technology package license with 5 Gbps maximum throughput
- APPX technology package license with 5 Gbps maximum throughput
- AX technology package license with 5 Gbps maximum throughput

If you need an evaluation license for the Security technology package, or for an AX technology package with higher throughput, contact your Cisco service representative.

For instructions on obtaining and installing evaluation licenses, see the *Installing CSL Evaluation Licenses for Cisco IOS XE 3.13S and Later* section in the Cisco CSR 1000v Software Configuration Guide .

Cisco CSR 1000V Software Licenses

Cisco CSR 1000V software licenses are divided into feature set licenses. The supported feature licenses depend on the release.

Current License Types

The following are the license types that are supported in Cisco IOS XE Everest 16.4.1 and later:

- IPBASE: Basic Networking Routing (Routing, HSRP, NAT, ACL, VRF, GRE, QoS)
- SEC (Security): IPBase package + Security features (IP Security VPN, Firewall, MPLS, Multicast)
- AX: IPBase package + Security features + Advanced Networking features (AppNav, AVC, OTV and LISP)
- APPX Package: IPBase package + Advanced Networking features - Security features (IP security features are not supported in this package)

Legacy License Types

The three legacy technology packages - Standard, Advanced, and Premium - were replaced in Cisco IOS XE Release 3.13 with the **IPBAsE**, **SEC**, and **AX** technology packages.

Features Supported by License Packages

For more information about the Cisco IOS XE technologies supported in the feature set packages, see the overview chapter of the Cisco CSR 1000v Series Cloud Services Router Software Configuration Guide.

Throughput

The Cisco CSR 1000V router provides term subscription licenses that support the feature set packages for the following maximum throughput levels:

- 10 Mbps
- 50 Mbps
- 100 Mbps
- 250 Mbps
- 500 Mbps
- 1 G bps
- 2.5 Gaps
- 5 Gbps
- 10 Gbps (IPBASE only)

The throughput levels are supported for different feature set packages in each version. For more information about how the maximum throughput levels are regulated on the router, see the Cisco CSR 1000v Cloud Services Router Software Configuration Guide.

Memory Upgrade

A memory upgrade license is available to add memory to the Cisco CSR 1000V router (Cisco IOS XE 3.11S or later). This license is available only for selected technology packages.

Additional Information about Licenses and Activation

For more information about each software license, including part numbers, see the Cisco CSR 1000v Router Datasheet. For more information about the standard Cisco IOS XE software activation procedure, see the Software Activation Configuration Guide, Cisco IOS XE Release 3S.

Software Image Nomenclature for Installation Files

The Cisco CSR 1000V installation file nomenclature indicates properties supported by the router in a given release.

For example, these are filename examples for the Cisco IOS XE Amsterdam 17.2.1 release:

- csr1000v-universalk9.17.02.01.ova

- csr1000v-universalk9.17.02.01.iso
- csr1000v-universalk9.17.02.01.qcow2

The following table lists the filename attributes along with its properties:

Table 1: OVA Installation Filename Attributes

Filename Attribute	Properties
universalk9	Specifies the package that you are installing.
17.02.01	Indicates that the software image is mapped to the Cisco IOS XE Amsterdam 17.2.1 release.

New and Enhanced Features for Cisco IOS XE Amsterdam 17.3.x

New and Changed Software Features in Cisco IOS XE 17.3.8a

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

New and Changed Software Features in Cisco IOS XE 17.3.8

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.7

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.6

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.5

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.4

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.3

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.2

There are no new software features in this release.

New and Changed Software Features for Cisco IOS XE 17.3.1a

The following are the new CSR 1000V software features for Cisco IOS XE Amsterdam 17.3.1a release:

Note Cisco IOS XE Amsterdam 17.3.1a is the first release for Cisco CSR 1000V in the Cisco IOS XE Amsterdam 17.3.1 release series.

- Support for Azure-PMD (Poll Mode Driver): You can now enable the Azure-PMD functionality for Cisco CSR 1000V instances running on Microsoft Azure. This functionality offers a faster, user-space packet processing framework that bypasses the VM's kernel network stack to increase the speed of network traffic. In a typical packet processing that uses the kernel network stack, the process is interrupt-driven, which involves context switching from the kernel space to the user space. Azure-PMD eliminates this context switching and the interrupt-driven method in favor of a user-space implementation that uses poll mode drivers for faster packet processing.
- Configure IP Multicast over Unidirectional links for PIM: Unicast and multicast routing protocols forward data on interfaces from which they have received routing control information- this requires 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, you need to enable the IP multicast over UDL functionality. To enable this functionality, you can now configure a UDL routing tunnel as a unidirectional generic routing encapsulation (GRE) tunnel and map this to a one-way satellite link, which in turn enables the associated unicast and multicast routing protocols to treat the UDL as a bidirectional link.
- Support for KVM (RHEL) 7.5 and 7.7 and ESXi 6.5 and 6.7.
- Support for openconfig-lldp 0.2.1: From the Cisco IOS XE Amsterdam 17.3.1 release, the openconfig-lldp 0.2.1 is supported. No additional configuration is required.
- Show platform resources command: The existing show platform resourses command now includes the following extension keywords to help you gather more information on platform resource utilization: R0, R0 cpu, R0 memory, exmem, datapath, and datapath oversubscriptions.
- 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.
- Enable debug information for Multicast: The following debug commands are introduced to enable the debugging information for Multicast via CONFD/NetConf:
  - 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
- New cipher suites for IP ssh Client and Server Algorithm: You can configure the HMAC algorithm of HMAC-SHA2-256-ETM@openssh.com or HMAC-SHA2-512-ETM@openssh.com as a cryptographic algorithm. These cipher suites can be used with the ip ssh client algorithm mac and ip ssh server algorithm mac commands.

- CUBE: Up to 100 VRF Instances: 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 that need to support greater number of tenants per box, the limit of VRF instances is enhanced to 100 with this feature. Also, support is introduced for this feature in CUBE Enterprise with this release.
- CUBE: 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.
- CUBE: Media Proxy Multi-forking using SIPREC: With this feature, the SIPREC-based CUBE Media Proxy solution supports forking to multiple recorders.
- CUBE: OPUS Codec Negotiation: With this feature, support is introduced for OPUS audio codec with CUBE.
- CUBE: TLS Server Name Indication (SNI) - RFC6066: With this feature, 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.

Note If you're using a Cisco CSR1000V 17.3.x instance, and you switch to controller mode, you might not be able to log in to the device or enter the CLI prompt. To overcome this issue, upload the ciscosdwan_cloud_init.cfg bootstrap file with the **aaa authorization exec default local** command to the router. For more information, see Switching Between Autonomous and Controller Modes.

Note When you execute the **show tech-support** command multiple times in an oversubscribed environment, it might cause the device to lose ssh connectivity. If this occurs, reload the device and ensure that the environment is not oversubscribed.

Note When you upgrade from one Cisco IOS XE release to another, you may see a *%Invalid IPV6 address* error in the console log file. To rectify this error, enter the global configuration mode, re-enter the missing IPv6 alias commands, and save the configuration. The commands are persistent on subsequent reloads.

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 doesn't impact the YANG model functionality.

Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.x

Resolved Bugs for Cisco IOS XE 17.3.8a

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

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

Open Bugs - Cisco IOS XE 17.3.8a

Bug ID	Description
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature.
CSCwe38296	Procyon packets drop due to MACSEC post-encryption padding behavior.
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 expereincing 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.

Bug ID	Description
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 Bugs for Cisco IOS XE Amsterdam 17.3.7

Bug ID	Description
CSCwc95218	Device with 5G module P-5GS6-GL is losing cellular configuration at each boot after upgrading.
CSCwc77981	Device crashed - track the fman-fp's memory leak caused by cond-debug.
CSCwd25107	Interface VLAN1 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.
CSCwd76176	DSPware targeting v173_throttle.

Open Bugs for Cisco IOS XE Amsterdam 17.3.7

Bug ID	Description
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature.

Bug ID	Description
CSCwe38296	Procyon packets drop due to MACSEC post-encryption padding behavior.
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 expereincing 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 Bugs for Cisco IOS XE Amsterdam 17.3.6

Bug ID	Description
CSCwa33174	'show interfaces' counters are incorrect and display extremely large values.

Bug ID	Description
CSCwb45811	Device crashes during boot with configuration of 10 or more vCPUs.
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.
CSCwc13013	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	SCCP auto-configuration issues with multiple protocols.
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 Zscalar 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	IOS-XE: Device platforms running 17.x - crypto ipsec policy installation fails.
CSCwa67398	NAT translations do not work for FTP traffic on device.
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.

Bug ID	Description
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

Bug ID	Description
CSCvy52270	Console Port Access change CLI does not work in CONTROLLER mode.
CSCwc71989	Device dropping all dataplane traffic on Gig3 interface.
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 peer device.
CSCwb66749	When configration IP NAT inside/outside on VASI intereface, ack/seq number abnormal.
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map.
CSCwa13553	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 : ARStandby drops seen on New Active during RG switchover.
CSCvz63684	Alpha: EWC Ha pair Expereincing 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.

Bug ID	Description
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
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 Bugs for Cisco IOS XE Amsterdam 17.3.5

Caveat ID Number	Description
CSCvy74799	Ucode crash observed at tw_bad_timer_bucket () at ../../../infra/tw_timer.c:918
CSCvz43205	CSR1Kv Packets above size of 2050 being dropped in subinterface by BadUidbSubIdx
CSCvz07972	Wrong config: attach 2 same perf-monitors on same direct of 1 interface may lead reboot unexpectedly
CSCvx84786	NAT ALG breaks(Drops) ICMP control messages (ICMP Fragmentation Needed) for PMTUD

Caveat ID Number	Description
CSCvy89785	OSPFv3 adjacency won't come up after "ospfv3 authentication ipsec" is applied on Tunnel interface
CSCvy33639	SDWAN: CSR1000v deployed in Microsoft Azure throwing continuous errors on consol.
CSCvo41609	GETVPN: Clearing members on Key Server causing rekey processing failure on GMs
CSCwa15132	DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum
CSCvy54606	CVLA need to reserve at least 50M memory for low-end DRAM platform
CSCvz69851	csr: Missing iid_certs for AWS invite-only regions
CSCvx39529	IKEv1/IKEv2 "show crypto session brief" output empty
CSCvy24571	Static NAT conflicts/overwrites with Port-forwarding
CSCwa36699	Prefetch CRL Download Fails
CSCwa17289	Memory leak when packet tracing or any other platform debug condition is enabled.
CSCvz73780	memory leak with fman_cc process when SM-X-G4M2X module installed
CSCvt66541	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted
CSCvz58895	IOS-XE unable to export elliptic curve key
CSCvz88205	CSR1000v Buffer Leak - IPSEC reply msg getting dropped
CSCvy67657	crypto ipsec security-association dummy leads to packet loss
CSCvw91361	Crash when issuing "show crypto isakmp peers config"
CSCvy23369	RAR: After Credit starvation, packets are not properly classified based on QoS.
CSCvw48943	crypto ikev2 proposals are not processed separately
CSCvv38438	Watchdog timeout due to Crypto IKMP
CSCwa37006	VXE: IOSd watchdog crash while printing to syslogs to console
CSCwa18177	Flapping bidirectional/unidirectional packet capture option with ipv4 filter for long time failed

Open Bugs for Cisco IOS XE Amsterdam 17.3.5

Caveat ID Number	Description
CSCwb45811	CSR1000V 17.3.5 crashes during boot with configuration of 10 or more vCPUs
CSCvv81296	Protocol specific change for base path

Caveat ID Number	Description
CSCvx94323	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut
CSCvy63924	Telemetry: IOS-XE Controller crashes after using 'show telemetry ietf subscription all' command.
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
CSCwa58911	Removing service-policy from the Zone-pair causes device crash
CSCvy52270	csr1kv/c8kv: Console Port Access change CLI does not work in CONTROLLER mode
CSCvy79601	ASR1001X gets rebooted when Tunnel move across two egress interfaces with QoS MPoL policy config
CSCwa17720	Router rebooted de to watchdogs after issuing the commands sh crypto mib ipsec commands
CSCvz53819	ZBFW : ARStandby drops seen on New Active during RG switchover
CSCvw13048	crash observed at NHRP while using summary-map
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
CSCwa18588	IOSd Nhrp core due to a segmentation fault when disabling PfR IWANs
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)
CSCvy54048	CPP Unexpected Reboot While Freeing CVLA Chunk
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
CSCvy30606	Device: sdn-network-infra-iwan key does not update successfully under network disruption situation
CSCvv55742	GETVPN-ipv6 & LISP support on C900 platforms
CSCwa29964	SCEP fails if AAAA DNS repy is received and source interface has no IPv6 address
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

Resolved Bugs for Cisco IOS XE Amsterdam 17.3.4

Caveat ID Number	Description
CSCvv53387	cedge is sending incorrect if index values for the sub-interfaces.
CSCvv92064	App-aware policy need to be honored when queuing is not set by localized policy
CSCvw05211	Pre-mature session deletion leading to churn and lower TPS at scale
CSCvw23197	BFD sessions go down on Service VPN after UTD is enabled on cEdge
CSCvw42048	Cisco 1111 CSR vtcp may cause packet drop for sip packets causing phones to reset
CSCvw81572	Multiple crashes cpp_cp_svr and qfp-ucode on 16.12.4
CSCvw83359	AWS:Cisco 8000kv CSR crashed and reboots if shut/no shut an interface a number of times
CSCvw93490	Cisco 1000v CSR crashing frequently with Critical software exception error.
CSCvx02009	cEdge running 17.3.2 crashed - Critical software exception / IOSXE-WATCHDOG: Process = SNMP ENGINE
CSCvx21270	SDWAN custom policy that does not looked 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.
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
CSCvx43331	Cisco 1000v CSR: Crashes during reg_invoke_iosxe_license_export_controlled_enforcement_bypass
CSCvx43798	SIT 17.5.1 02/01: Stby switch reloaded due to config mismatch during telemetry push from DNAC.
CSCvx45788	cannot apply ciscosdwan.cfg due to vpg-log-server-acl ACL on VirtualPortGroup0 for logging
CSCvx51664	For-us Icmp packets are collected by cflowd which against the data-policy
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
CSCvx64640	Data plane VPLS traffic generating Control Word on all Label Switched Headers
CSCvx64846	"show sdwan policy service-path/tunnel-path" command cause device crash

Caveat ID Number	Description
CSCvx72682	[DMM/SLM test issue] CFM crash when using physical port, DMM/SLM doesn't work on EVC
CSCvx73741	custom app not getting detected after attached removed and re-attached- app-visibility is disabled
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
CSCvx87726	Cisco 1000v CSR Multicast Over OTV Not Forwarding
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
CSCvy06736	Config out of sync after upgrading to 17.4.1
CSCvy25957	Security container is dropping legitimate FIN,ACK Packets
CSCvy30209	IOS-XE cpp ucode crash with fragmented packets
CSCvy35044	Signature update failure - SSL-CERTIFICATE_VERIFY_FAILED

Open Bugs for Cisco IOS XE Amsterdam 17.3.4

Caveat ID Number	Description
CSCvt62123	DMVPN - after removing IPSec, traffic is dropped on a tunnel interface
CSCvu06483	Data consistancy 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
CSCvw48943	crypto ikev2 proposals are not processed separately
CSCvw60359	cEdge-policy: set next-hop-ipv6 is not working next-hop-ip (ipv4) is working.
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

Caveat ID Number	Description
CSCvx27965	cEdge ipv6 netflow with high scale flows FNF does not working
CSCvx35902	fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash.
CSCvx64449	%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: mac verify failed due to ip rtp header-compression iphc-format
CSCvx74212	IKEv1 IPSec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ
CSCvx90032	CSR in Azure can fail to authenticate using AAD
CSCvx94285	CSR crashes after oce_lookup_one_adj_id_handle while reading emu_mem.
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
CSCvy33639	SDWAN: Cisco 1000v Series CSR deployed in Microsoft Azure throwing continuous errors on consol.
CSCvy52270	Cisco 1000v Series CSR/Cisco 8000v Series CSR: Console Port Access change CLI does not work in CONTROLLER mode
CSCvy54048	CPP Crash While Freeing CVLA Chunk
CSCvy54314	Data-policy local-tloc with app-route is dropping packets when SLA is not met
CSCvy55408	Cisco 1121 ISR router multiple crash. - session hash corrupted
CSCvy58115	Cedge : Cloudexpress Office 365 probes are hitting 100% loss
CSCvy64180	ccedge Cisco 1121-4P CSR crahed with Localsoft error
CSCvy67301	URL Filtering regex pattern match not working on large pattern
CSCvy73818	cEdge QFP starts dropping traffic - UTD Service Node not healthy ident
CSCvy78087	Qos download failed with FW policy when rebooting device
CSCvy78123	cEdge: High CPU usage due to Multicast and Data Policy configuration.
CSCvy69555	Unable to fetch eigrp prefix, nexthop, omptag, and route origin

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

Caveat ID Number	Description
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
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
CSCvv91865	Moving PC from network causes static DHCP binding to be removed from the device.
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
CSCvw14131	Crash in TCL Bytecode When Running RA Trace in Guestshell Python
CSCvw16643	Device Template failing to attach after changing few device variables
CSCvw19171	Smart license registration through explicit mode proxy server
CSCvw19362	[EVPN RT2-RT5] After few host moves RT2-RT5 re-origination happens even when there is no Remote RT2
CSCvw22760	MACSEC MKA stops forwarding data after every 3rd rekey
CSCvw30128	ip-acl errors of correcting the logic of sequence id when there is an error with msg creation
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

Caveat ID Number	Description
CSCvw38433	OMP-Agent Routes in EIGRP changes AD to 252 on non-SDWAN devices
CSCvw39383	CPP ucode crash with fw_base_flow_create
CSCvw41482	SSH with Certificate authentication doesn't work after upgrade to 17.3.1
CSCvw47800	HSL Export over VASI Interface causes Netflow v9 Template Flooding
CSCvw48800	unable to transfer 1500 byte IP packet when using BRI bundled Multilink
CSCvw48811	RP went down due to __be_iosd_rec_malloc_free_before
CSCvw54076	[SIT]: BFD sessions not established between Edges, with UTD enabled
CSCvw55030	Dynamic Nat pool "ip aliases" are not created on the device
CSCvw56517	LMR Unable to hear first seconds of audio
CSCvw58560	FlexVPN reactivate primary peer feature does not work with secondary peer tracking
CSCvw64559	Throughput license grace period starts counting down after upgrade router software
CSCvw76715	OpenSSL vulnerability (CVE-2020-1971) evaluation for IOS-XE
CSCvw77485	Router may not send PIM Register message if RP is reachabile 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 wile configuring l2vpn evpn instance for VXLAN
CSCvw97748	Decouple mac aging from ARP aging on vlans not using the centralized gw feature
CSCvx02515	BGP IPv6 link-local session doesn't come up
CSCvx08852	Not able to create VFI instances
CSCvx12686	Memory Lock and system crashed while clearing ip access-list stats.
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
CSCvw89147	Crash at the moment of calculating tcp header

Caveat ID Number	Description
CSCvw92643	Netflow crash at fnf_ipv6_output_feature_final_internal with flow record on IPv6 IPsec tunnel
CSCvx14095	NETCONF ACL not working if ACL is referencing an object-group
CSCvx18526	Clients using DHCP Server Port-Based Address Allocation not getting IP address
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
CSCvx35902	FMAN_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash
CSCvx40030	IP PIM SPT-threshold infinity causes ICMP Echo Replies to not be generated for IP Multicast Requests

Resolved Bugs for Cisco IOS XE Amsterdam 17.3.2

Caveat ID Number	Description
CSCvv03800	ASR1002X lost all configuration after upgrade from 16.12 to 17.3.
CSCvv04959	GRUB2 Arbitrary Code Execution Vulnerability.
CSCvv85766	Memory leak upon ssh/scp connections to a router.

Resolved Bugs for Cisco IOS XE Amsterdam 17.3.1

Caveat ID Number	Description
CSCvs81791	Fix for kernel driver issue causing wake up for empty block, packet too large to process
CSCvt16915	CSR Gig3 Interface not created even after ENI is attached to VM instance in AWS
CSCvt31588	CSR on AWS - PAYG Broken in 17.1, 17.2, and Polaris
CSCvt50394	Custom Data: bash/python scripts in Scripts section does not execute
CSCvu34653	CSR stuck in Bootloop while upgrading to 17.2.1r on Azure.
CSCvt94976	vmxnet3 vnics need ability to set MTU

Open Bugs for Cisco IOS XE Amsterdam 17.3.1

Caveat ID Number	Description
CSCvu52185	CSR1000v may unexpectedly reload (or hang) due to keepalive failures
CSCvv38068	C8000v not booting up in Azure if assigned IPaddr 10.0.1.0 to Gig1 Interface

Related Documentation

- Release Notes for previous versions of Cisco Cloud Services Router 1000V Series
- Configuration Guides for Cisco Cloud Services Router 1000V Series
- Product Landing page for Cisco Cloud Services Router 1000V Series
- Datasheet for Cisco Cloud Services Router 1000V Series
- Field Notices
- Deferral 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.