Release Notes for Cisco Catalyst 8300 Series Edge Platforms, Cisco IOS XE Amsterdam 17.3.x

First Published: 2020-11-02

Last Modified: 2023-10-28

About Cisco Catalyst 8300 Series Edge Platforms

The Cisco Catalyst 8300 Series Edge Platforms are best-of-breed, 5G-ready, cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

Cisco Catalyst 8300 Series Edge Platforms with Cisco IOS XE SD-WAN Software deliver Cisco's secure, cloud-scale SD-WAN solution for the branch. The Cisco Catalyst 8300 Series Edge Platforms is built for high performance and integrated SD-WAN Services along with flexibility to deliver security and networking services together from the cloud or on premises. It provides higher WAN port density and a redundant power supply capability. The Cisco Catalyst 8300 Series Edge Platforms have a wide variety of interface options to choose from—ranging from lower and higher module density with backward compatibility to a variety of existing WAN, LAN, voice, and compute modules. Powered by Cisco IOS XE, fully programmable software architecture, and API support, these platforms can facilitate automation at scale to achieve zero-touch IT capability while migrating workloads to the cloud. The Cisco Catalyst 8300 Series Edge Platforms also come with Trustworthy Solutions 2.0 infrastructure that secures the platforms against threats and vulnerabilities with integrity verification and remediation of threats.

The Cisco Catalyst 8300 Series Edge Platforms are well suited for medium-sized and large enterprise branch offices for high WAN IPSec performance with integrated SD-WAN services.

For more information on the features and specifications of Cisco Catalyst 8300 Series Edge Platforms, refer to the Cisco Catalyst 8300 Series Edge platforms datasheet.

Note Sections in this documentation apply to all models of Cisco Catalyst 8300 Series Edge Platforms unless a reference to a specific model is made explicitly.

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the software features, platform, and software image support on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.

Note To access CFN, you do not require an account on cisco.com.

New and Changed Hardware and Software Features

New and Changed Hardware Features

New Hardware Features

- Cisco Catalyst 8300 Series Edge Platforms are available in these models:
- C8300-1N1S-4T2X
- C8300-1N1S-6T
- C8300-2N2S-4T2X
- C8300-2N2S-6T

Note N=Network Interface Modue, S=Services Module, and T=Gigabit Ethernet, X=Ten Gigabit

For information on the hardware features supported on the Cisco Catalyst 8300 Series Edge Platforms, refer to the Cisco Catalyst 8300 Series Edge Platforms datasheet.

- NIM-PVDM is the next-generation digital signal processor (DSP) module to utilize a PVDM4 chip for IP media services. This module enables the Catalyst 8300 Series Edge platforms to provide rich-media capabilities, such as high-density voice connectivity, conferencing, transcoding, media optimization, transrating, and secure voice for Cisco Unified Communications solutions

For information on the hardware features supported on the NIM-PVDM, refer to the Cisco Packet Voice Digital Signal Processor Modules for Cisco Unified Communications Solutions datasheet.

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

Table 1: New Software Features in Release Cisco IOS XE Amsterdam 17.3.3

Feature	Description
Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy	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 *push* the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to *pull* 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. Minimum Required SSM On-Prem Version: Version 8, Release 202102 Minimum Required Cisco IOS XE Version: Cisco IOS XE Amsterdam 17.3.3 For more information, see Smart Licensing Using Policy for Cisco Enterprise Routing Platforms.

Table 2: New Software Features in Release Cisco IOS XE Amsterdam 17.3.2

Feature	Description
Smart Licensing Using Policy	

Feature	Description
	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. 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. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date. 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. Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy. For conceptual, configuration, migration, and troubleshooting information for Smart Licensing Using Policy, see Cisco 8300 Series Software Configuration guide. For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide. **Note** Starting with Cisco IOS XE Amsterdam 17.3.2, 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

Feature	Description
	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)
Cisco DNA Center Support for Smart Licensing Using Policy	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 Cisco IOS XE Amsterdam 17.3.2. 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). 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. **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.

Cisco Catalyst 8300 Series Edge Platforms ROMmon Compatibility Matrix

The following table lists the ROMmon releases supported in Cisco IOS XE 17.3.x releases

Table 3: Minimum and Recommended ROMmon Releases Supported on C8300-1N1S-4T2X|6T

Cisco IOS XE Release	Minimum ROMmon Release Supported for IOS XE	Recommended ROMmon Release Supported for IOS XE
17.3.1	17.3(1r)	17.3(5r)

Table 4: Minimum and Recommended ROMmon Releases Supported on C8300-2N2S-4T2X|6T

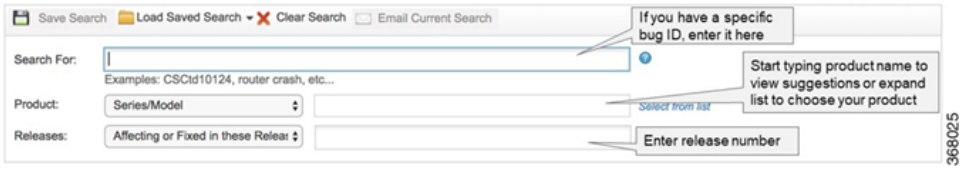
Cisco IOS XE Release	Minimum ROMmon Release Supported for IOS XE	Recommended ROMmon Release Supported for IOS XE
17.3.1	17.3(1.2r)	17.3(1.2r)

Resolved and Open Caveats

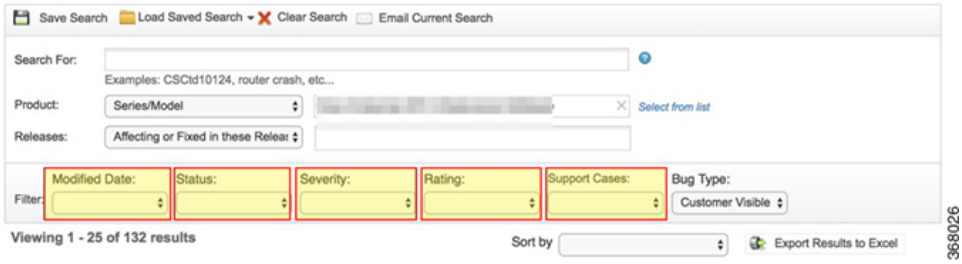
About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.



You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.



Resolved Caveats in Cisco IOS XE Amsterdam 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 Caveats in Cisco IOS XE Amsterdam 17.3.8a

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.8

There are no resolved caveats in this release.

Open Caveats in Cisco IOS XE Amsterdam 17.3.8

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.7

There are no resolved caveats in this release.

Open Caveats in Cisco IOS XE Amsterdam 17.3.7

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.6

Identifier	Headline
CSCwb23043	MACsec not working on subinterfaces using dot1q > 255 between devices.
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	Device rebooted de to watchdogs after issuing the commands s**how crypto mib ipsec** commands.
CSCwb85046	Device reloads when group-range is configured under an interface Group-Async.
CSCwb91026	Traffic is hitting wrong sequence in the data policy.
CSCwb25913	After configuring match input-interface on class-map, device 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 to 17.3.4.
CSCwb25137	NAT: Source address translation for multicast traffic fails with route-map.
CSCvy69405	Device Appnav-XE connections are going as passthrough unsupported .
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored.
CSCwa67398	NAT translations do not work for FTP traffic in the device.

Identifier	Headline
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.
CSCwb15331	Keyman memory leak using public keys.
CSCvy30606	catalyst 9800 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 Caveats in Cisco IOS XE Amsterdam 17.3.6

Identifier	Headline
CSCwb72336	ICMP traceroute return packet not classified based on forward override port information.
CSCwa76570	Device 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 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.
CSCvy79601	Device gets rebooted when Tunnel move across two egress interfaces with QoS MPoL policy configuration.
CSCwa69101	ISG: initiator unclassified ip-address LQipv4 command has no effect.
CSCvz53819	ZBFW : AR standby drops seen on Nnw active during RG switchover.
CSCvz63684	EWC Ha pair Expereincing IOS Tracebacks, followed by KEYMAN crash.
CSCwb17282	Router crashing when clearing a VPDN session.

Identifier	Headline
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	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.
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 the device.
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.
CSCvx28426	Router may crash due to Crypto IKMP process.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.5

Caveat ID Number	Description
CSCvw20026	Evaluation of curie-2RU for Intel 2020.2 IPU.

Open Caveats in Cisco IOS XE Amsterdam 17.3.5

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.4a

Caveat ID Number	Description
CSCvv11460	No redistibuted connected route-map command not working.
CSCvv33873	Crimson Database Memory Leak In "/tmp/rp/tdldb/0/IOS_PRIV_OPER_DB" Due to "platform_property_value"
CSCvv72067	Multicast till the scope configured is forwarded.
CSCvv92064	App-aware policy need to be honored when queuing is not set by localized policy.
CSCvv95280	The device may crash when ZBFW HSL(High Speed Logging) is configured.
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	VTCP may cause packet drop for sip packets causing phones to reset.
CSCvw45135	Mismatch in System CPU statistic -- "Real Time" and historical 1/3/6/12h.
CSCvw52574	Device configured with no ip unreachables sending ICMP Type 3 Code 13.
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCvw65439	Crash seen at chunk_lock or memcmp with ipv6 host scale.
CSCvw81572	Multiple crashes cpp_cp_svr and qfp-ucode on 16.12.4.
CSCvw82778	The device forwards own DNS request in Service VPN towards VPN0 instead of data-tunnel.
CSCvw84671	Hashed TACACS/RADIUS key displays differently in the running-config.
CSCvw86304	Registering unsupported xpaths in mapping for cEdge.
CSCvw86452	OSPF External type-1 Route in Database but missing in RIB.
CSCvx00578	Crash at boot up in isis_ip_sr_prefix_sid_notify() with flex-algo setup.
CSCvx08994	CTS credential password will be added to local keystore even if the password is longer than 24 char
CSCvx21270	SDWAN custom policy that does not looked to be programmed correctly on the cedge platform.
CSCvx23083	17.3.2: Route-map not working properly when we have multiple sequences with match/set with BGP
CSCvx23159	FW-4-ALERT_ON: (target:class)-():getting aggressive seen when no half open feature configed.
CSCvx25394	Increase In Memory Usage by pubd and confd Over Time With Telemerty

Caveat ID Number	Description
CSCvx25977	Crash is seen with 'show tech isis command.
CSCvx32670	Wrong reload reason reflected after a power outage.
CSCvx34088	[EVPN RT2-RT5] BGP crash @bgp_evpn_evi_delete_rt5_path,bgp_evpn_l2rib_path_update
CSCvx34623	SIT : IOS exception seen and ASR reboots when a netconf is issued to get interface details
CSCvx34811	The "clear pppoe all" command causes software crash.
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.
CSCvx38454	ISR Crash for CENT-MC-0 process
CSCvx41293	TCP-AO may calculate incorrect MAC on IOS XE under certain conditions.
CSCvx41294	High CPU usage caused by "TCP Timer" process.
CSCvx43798	SIT 17.5.1 02/01: Stby switch reloaded due to config mismatch during telemetry push from DNAC.
CSCvx44334	VRF stuck in deleting after updating VRF configuration with "config replace bootflash:" command
CSCvx45788	cannot apply ciscosdwan.cfg due to vpg-log-server-acl ACL on VirtualPortGroup0 for logging
CSCvx48936	Native Multicast: Underlay Groups are not pruned once source stops multicast traffic
CSCvx49943	Flex algo Sid not advertised after delete/config back of flex algo in ospf
CSCvx50511	router crashes when BMP mem usage is 100% and vrf under address-family is removed.
CSCvx51664	For-us Icmp packets are collected by cflowd which against the data-policy
CSCvx52273	Smart license registration through proxy server fails.
CSCvx53049	Crash when TPOOL is updating and 'wr mem' is issues at same time
CSCvx54540	Missing neighbor x.x.x.x update-source Loopback10 when upgrade 16.12.4 to 17.3.2 w/0 intent template.
CSCvx57615	ZBFW blocking ACK packets for applications using cloudexpress SaaS set to use a Gateway with synsent.
CSCvx59899	IRouter rebooting due to CPP crashing becaue of UTD feature.

Caveat ID Number	Description
CSCvx64640	Data plane VPLS traffic generating Control Word on all Label Switched Headers
CSCvx64756	RIP MD5 Authentication failure when authentication key length is 16 characters.
CSCvx64846	Show sdwan policy service-path/tunnel-path" command cause device crash
CSCvx65762	SISF process reloads.
CSCvx65789	Unexpected reload generating pttcd and pubd cores
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
CSCvx81030	Need to remove ordered-by user from the leaf-list dns-server-list
CSCvx85334	Port enters err-disabled state (BPDU guard) when LLDP packet with MAC DA:0180.c200.0000.
CSCvx88246	Packets dropped due to firewall + data policy interop issue.
CSCvx88383	DMI2 | ERROR_NETCONF_RPC_ERROR | application communication failure
CSCvx89710	SCEP: CA server fails to rollover CA certificate with error: "Storage not accessible"
CSCvx94722	IOS-XE version 16.12.5 does generate jumbo frames for dot1x packets.
CSCvx97465	IOS-XE Device Unexpected Reset due to Segmentation fault in IPv6 ICMP
CSCvx97718	vtcp frees rx buffer when packet with expected next sequence arrives with no payload; phones reset.
CSCvy04606	BGP BMP CPUHOG causing router reloaded with VRF scale deletion.
CSCvy06736	Config out of sync after upgrading to 17.4.1.
CSCvy08748	OSPF summary-address isn't generated though candidate exists
CSCvy12075	Binding label is not associated for the routes associated with VRF.
CSCvy14126	Devices are crashing frequently 17.4.1b.
CSCvy25957	Security container is dropping legitimate FIN,ACK Packets.
CSCvy29106	Device crashed on a Eigrp enabled device when Netconf get operation was used.
CSCvy30209	IOS-XE cpp ucode crash with fragmented packets.

Caveat ID Number	Description
CSCvy31298	ISR4461 NIM-2GE-CU-SFP - Sub-interfaces not transmitting traffic
CSCvy35044	Signature update failure - SSL-CERTIFICATE_VERIFY_FAILED.

Open Caveats in Cisco IOS XE Amsterdam 17.3.4a

Caveat ID Number	Description
CSCvt62123	DMVPN - after removing IPSec, traffic is dropped on a tunnel interface
CSCvt89229	VRF rd value help menu asking for string instead of ASN:nn, IP-address:nn VPN Route Distinguisher
CSCvu06483	Data consistancy errors seen on configuring mac-sec on the underlay interface with ipsec configured
CSCvu10830	route-map doesnt allow to match ipv4 access-list
CSCvu41891	Config mismtach between show run and show sdwan running-config while removing AAA config
CSCvu57475	Config sync failure when removing and adding config
CSCvu62879	Crash@bgp_perform_general_scan.
CSCvv17346	Unexpected reload due to Crypto IKEv2 process
CSCvv38438	Watchdog timeout due to Crypto IKMP
CSCvv48885	Issue with updating local-address in a crypto keyring.
CSCvv85441	match {community|large-community|extcommunity|aspath} item may NVGEN too many items in one line.
CSCvw48943	Crypto ikev2 proposals are not processed separately
CSCvw73769	17.4 ZBFW:Cpp_cp crash seen when a rule is added at beginning in automation on the device
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
CSCvx25680	IOS-XE Memory Leak in SSS Manager
CSCvx27965	cEdge ipv6 netflow with high scale flows FNF does not working
CSCvx34435	Dot1q sub-interface syntax error when configuring "encapsulation dot1Q" on C8500 HundredGigEx/y/z

Caveat ID Number	Description
CSCvx35902	Fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash.
CSCvx62167	Route-map corruption when configured using Netconf with ncclient manager
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
CSCvx89805	while polling BGP Neighbours under VRF getting all ip instead of associated ip.
CSCvy10041	Removal of set reverse-route tag xxx' removes 'reverse-route' config from crypto map.
CSCvy34805	Consecutive Multicast Crashes is seen oin the device.
CSCvy34854	17.X throttle running in sdwan mode does not have allowas in option in BGP.
CSCvy35490	Order of operation in OSPF template.
CSCvy42216	Switchport trunk native vlan xx" gets removed when upgrading from 16.12.x to 17.3.3.
CSCvy54048	CPP Crash While Freeing CVLA Chunk.
CSCvy54314	Data-policy local-tloc with app-route is dropping packets when SLA is not met
CSCvy55408	Router multiple crash. - session hash corrupted.
CSCvy58115	Cloudexpress Office 365 probes are hitting 100% loss.
CSCvy67301	URL Filtering regex pattern match not working on large pattern.
CSCvy78087	Qos download failed with FW policy when rebooting device
CSCvy78123	High CPU usage due to Multicast and Data Policy configuration.
CSCvy79601	The device gets rebooted when Tunnel move across two egress interfaces with QoS MPoL policy config
CSCvy87803	Ethernet loopback not working.
CSCvv82985	dhcpv6_relay:dhcp-client on branch not receive ipv6 address.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
CSCvw08885	Enhancement for logging systemd service failure on boot up as per CSCvp71539.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.2

Caveat ID Number	Description
CSCvb16018	C8300-1N1S: NIMX-M-1TE-SFP/SM-X-E2-20UXF bp link issue during OIR reload ping
CSCvp75924	C8300-1N1S-4T2X: "pause output" counter is not working in FPTE while sending oversubscribed traffic

Related Documentation

- Hardware Installation Guide for Catalyst 8200 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8300 Series Edge Platforms
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Cisco Catalyst 8300 and 8200 Series Edge Platforms Software Configuration Guide