Release Notes for Cisco Catalyst 8000V Edge Software, Cisco IOS XE Dublin Release 17.12.x

First Published: 2023-08-22

Last Modified: 2026-08-05

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Cisco Catalyst 8000V Edge Software Overview

About Cisco Catalyst 8000V

Cisco Catalyst 8000V Edge Software or Cisco Catalyst 8000V is a software-based, virtual router that combines the functionalities of Cisco Cloud Services Router (Cisco CSR1000V) and Cisco Integrated Services Virtual Router (Cisco ISRv) into a single image that is intended for deployment in on-prem branches, data centers, colocation data centers, and public clouds.

Cisco Catalyst 8000V supports NIM modules on Cisco ENCS platforms, runs on any x86 platform, and is supported on ESXi, KVM, and Cisco NFVIS hypervisors. Further, you can deploy this router on public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba Cloud.

When you deploy Cisco Catalyst 8000V as a VM, the Cisco IOS XE software behaves similar to a traditional Cisco router (hardware platform). You can configure different features depending on the Cisco IOS XE software version.

Features

- **Hardware independence**: The Cisco Catalyst 8000V router uses the benefits of virtualization in the cloud to provide hardware independence. Since the Cisco Catalyst 8000V runs as a virtual machine, you can use this router on any x86 hardware that the virtualization platform supports.
- **Sharing of host hardware resources**: The host server hardware resources such as CPU cores, memory, and disk are managed by the hypervisor, and these resources are shared among the guest VMs. You can regulate the amount of hardware resources assigned to a specific Cisco Catalyst 8000V VM instance.
- **Flexibility in deployment**: You can easily move a VM from one server to another. Thus, you can move a Cisco Catalyst 8000V instance from a server in one physical location to a server in another physical location without moving any hardware resources.
- **Enhanced software security - Secure Object Store**: In Cisco Catalyst 8000V, storage partitions for NVRAM, licensing, and other data are created as object stores. The individual object stores are encrypted to ensure data security, and this product is Cisco Secure Development life cycle (CSDL) compliant. Further, Cisco Catalyst 8000V supports a 16G disk profile.

Hardware Requirements

For hardware requirements and installation instructions, see the Cisco Catalyst 8000V Edge Software Installation And Configuration Guide.

Software Images and Licenses

The following sections describe the licensing and software images for Cisco Catalyst 8000V.

Cisco Catalyst 8000V Software Licenses

The Cisco Catalyst 8000V is licensed based on throughput, feature-set, and the licensing term. This product supports Cisco Smart Licensing Usage Policy as well as Cisco DNA Licensing. Based on whether you want to opt for purchased licenses that go with the Cisco Catalyst 8000V instance, or a subscription-based license, choose one of the following options:

Subscription-Based Licensing via Cisco DNA

You can purchase a subscription license for Cisco Catalyst 8000V through the following licenses that are available via Cisco DNA:

- Cisco Catalyst 8000V - Network-Advantage
- Cisco Catalyst 8000V - Network-Essentials

For more information on Cisco Catalyst 8000V DNA licensing, see Cisco DNA Software for SD-Wan and Routing Ordering Guide.

Bring-Your-Own-Licensing

You also have an option to purchase and use licenses with Cisco Catalyst 8000V as a Bring-Your-Own-License (BYOL) instance or as a Pay-As-You-Go (PAYG) instance.

To use a Cisco Catalyst 8000V - BYOL license, see Licenses and Licensing Models to know to how install and configure your license.

If you have upgraded to Cisco Catalyst 8000V from a Cisco CSR 1000V or a Cisco ISRV, you must use Smart Licensing Using Policy (SLP). Traditional licenses do not work after the upgrade.

Pay-As-You-Go Licensing

Cisco Catalyst 8000V supports the PAYG Licensing model with Amazon Web Services (AWS) and Microsoft Azure Marketplace. Cisco Catalyst 8000V hourly-billed AMI or Pay As You Go licensing model allows you to consume an instance for a defined period of time. In this licensing model, you can directly launch the instance from the AWS or Azure Marketplace and start using the instances. The licenses are embedded in the image.

Note For demo or evaluation licenses, contact your Cisco Account Team if you have a direct purchase agreement with Cisco, or your Cisco Partner or Reseller.

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

Software Image Nomenclature for Installation Files

The Cisco Catalyst 8000V installation file nomenclature indicates properties supported by the router in a given release.

For example, these are filename examples for the Cisco IOS XE Dublin 17.12.1a release:

- c8000v-universalk9.17.12.01a.ova

- c8000v-universalk9.17.12.01a.iso
- c8000v-universalk9.17.12.01a.qcow2

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

Table 1: Installation Filename Attributes

Filename Attribute	Properties
universalk9	Specifies the package that you are installing. Images with the universalk9 designation in the image name refers to a universal image that offers all the Cisco IOS features including strong payload cryptography features such as IPSec VPN, SSL VPN, and Secure Unified Communications. This image also supports security features like Zone-Based Firewall, and intrusion prevention.
17.12.01a	Indicates that the software image is mapped to the Cisco IOS XE Dublin 17.12.1a release.

Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

New and Enhanced Features for Cisco IOS XE Dublin 17.12.x

New and Changed Software Features in Cisco IOS XE 17.12.8

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.7b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.6

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5d

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5c

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5b

There are no new software features in this release.

New and Changed Features in Cisco IOS XE 17.12.5a

There are no new features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.4b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.4a

Table 2: Software Features

Feature	Description
Support for RHEL 9.2	From Cisco IOS XE 17.12.4a, you can deploy Cisco Catalyst 8000V on RedHat RHEL 9.2 operating system with KVM hypervisor.
Support for VMware ESXi 8.0	From Cisco IOS XE 17.12.4a, you can deploy Cisco Catalyst 8000V on VMware ESXi 8.0 Update 2 hypervisor operating system.
Support for N2 instances for Google Cloud Platform deployments	Cisco IOS XE 17.12.4a supports n2-standard-8, n2-standard-4 instance types for Cisco Catalyst 8000V deployments in Google Cloud Platform.

New and Changed Software Features in Cisco IOS XE 17.12.3

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.2

This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see the Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

Table 3: Software Features

Feature	Description
Support for SUSE SLES 15 SP5	From Cisco IOS XE 17.12.2, you can deploy Cisco Catalyst 8000V on SUSE SLES 15 SP5 operating system with KVM hypervisor.

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

New and Enhanced Features for Cisco IOS XE 17.12.1a

Note Cisco IOS XE Dublin 17.12.1a is the first release for Cisco Catalyst 8000V in the Cisco IOS XE Dublin 17.12.x release series.

Table 4: Software Features

Feature	Description
Support for Intel Atom® C3000 Processor Series (Denverton)	From Cisco IOS XE 17.12.1a onwards, Cisco Catalyst 8000V is supported on Intel Atom® C3000 processor (Denverton) CPU-based servers with Intel x550 NIC on the following hypervisors: • Redhat Enterprise Linux (RHEL) 8.4 KVM • VMware ESXi 7.0.x You can run Cisco Catalyst 8000V on other x86 CPUs with different NICs and different versions of operating systems. However, support is support is available only for the versions that have been listed in the versions mentioned above.

Feature	Description
Support for Intel i350 NICs	Cisco Catalyst 8000V includes drivers to support SR-IOV connectivity to Intel i350 NICs on Intel Xeon CPU based x86 servers with SUSE SLES 15 SP3 KVM hypervisor. You can run Cisco Catalyst 8000V on other x86 CPUs with different versions of operating systems. However, support is available only for the versions that have been listed in the Cisco Catalyst 8000V Installation and Configuration Guide.
Support for D16_v5 instance in Microsoft Azure environment	Cisco Catalyst 8000V supports the D16_v5 instance type with 8 NICs (maximum) in the Microsoft Azure Marketplace for increased throughput.
Cisco Catalyst 8000V Performance Enhancements	Cisco Catalyst 8000V supports improved, 16-core performance for on-prem deployments in the KVM and ESXi environments.
IPv6 Unicast Support with DLEP	The IPv6 Unicast Support feature introduces support for IPv6 dataplane to RAR Dynamic Link Exchange Protocol.
Managing the SD-Routing Devices Using Cisco SD-WAN Manager	This feature allows you to perform management operations for SD-Routing devices using Cisco Catalyst SD-WAN Manager. You can use a single network manage system (Cisco Catalyst SD-WAN Manager) to monitor all the SD-Routing devices and therefore help in simplifying solution deployments.
Segment Routing over IPv6 Dataplane	Segment Routing (SR) can currently be applied on Multiprotocol Label Switching (MPLS) dataplane. From Cisco IOS XE 17.12.1a, SR is supported over the IPv6 dataplane for the following protocols: • Interior Gateway Protocol (IS-IS only) • Border Gateway Protocol (BGP) In addition, the following functionalities are available for Segment Routing over IPv6 dataplane: • Segment Routing Traffic Engineering Policies • Static Routes • Performance Management • Operations, Administration and Maintenance (OAM)

Feature	Description
Support for Automatic Log Deletion	This feature allows you to delete the entries from the logging buffer. You can configure the local syslog retention period after which the entries are purged from the device automatically. To enable this feature, use the **logging purge-log buffer days** command.
TrustSec and Software-Defined Access Scale Measurement	With this feature, the scale numbers for TrustSec and Software-Defined Access (SDA) are measured for the following: • Security Group Tag (SGT) or Destination Group Tag (DGT) Policies • Unidirectional IPv4 SGT Exchange Protocol (SXP) connections • Bidirectional IPv4 SXP connections • IPv4 SGT Bindings • IPv6 SGT Bindings • Security Group Access Control Entries (SG ACEs)

Table 5: Cisco Unified Border Element (CUBE) Features

Feature	Description
CUBE: GCM Ciphers for WebSocket-based Media Forking	From Cisco IOS XE Dublin 17.12.1a onwards, GCM cipher negotiation supports secure connectivity of WebSocket server.
CUBE: IPv6 Flows in High Availability	From Cisco IOS XE Dublin 17.12.1a onwards, High Availability in CUBE supports IPv6 flows.
CUBE/LGW: Cover Buffer Enhancements for VoIP Trace	From Cisco IOS XE Dublin 17.12.1a onwards, VoIP Trace for SIP messages displays cause code in the cover buffer.

Resolved and Open Bugs - Cisco IOS XE 17.12.x

Resolved Bugs in Cisco IOS XE 17.12.8

Identifier	Headline
CSCwu02602	DBAL EVENTS crash seen while trying to push config group to device in SDWAN and SD-Routing.

Identifier	Headline
CSCws75769	Netconf process doesn't start on 9130 AP in EWC mode and generates repeated dmiauthd subscription failures for invalid route-map YANG path.
CSCws80808	Loopback interface in Mgmt-intf VRF becomes unreachable via Management interface.
CSCwt87294	mDNS Cache-Flush behavior not consistent.

Open Bugs for Cisco IOS XE 17.12.8

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

Resolved Bugs - Cisco IOS XE 17.12.7b

Identifier	Headline
CSCwr27127	Azure C8000V deployment fails with provisioning timedout error
CSCwr83968	Unexpected reload on device with Static NAT when polling NAT translation data
CSCwo57783	NHRP Encap Error for Purge Request populates on spoke despite correct routing at HUB
CSCwn85623	Missing Calling-Station-ID in radius messages
CSCwp96706	Memory leak in MallocLite and Crypto IKEv2
CSCwq22471	Device unexpectedly reboots when importing CA chains
CSCwq21566	HSL entries are missing when configuration is pushed via vManage
CSCwq51358	Device might experience high memory utilization and unexpected reloads during IKEv2 operations
CSCwn18874	DMVPN spoke crashed at Process = NHRP
CSCwo14975	Memory leak in DNS Proxy/SKA triggers unexpected reloads
CSCwj88080	IOS XE device continuously crashes after configuring UTD and reboots
CSCwp40010	RP crashes while debugging IKEv2
CSCwp38609	CTS trustpoint loop triggers PKI segfault
CSCwq49981	Call Failures due to FPI resource leaks

Open Bugs - Cisco IOS XE 17.12.7b

Identifier	Headline
CSCwr60310	SDWAN Template push or CLI config update fails due to the duplication of VTY or Async lines in the configuration

Identifier	Headline
CSCwr00088	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP
CSCwn29062	Device might see Cosmetic DATACORRUPTION logs during IPSec tunnel up/down events
CSCwk55051	polaris_vconfd_cfgpull_t logging denials observed during configuration push trigger
CSCwr31999	Using the Azure Portal GUI stop button initiates reload before forcefully shutting down in 10 minutes
CSCwm54978	polaris_iosd_t denials 2024-09-16 06:43:22 errors seen during system boot or **dir bootflash:** command

Resolved Bugs - Cisco IOS XE 17.12.6

Identifier	Headline
CSCwo60972	C8000V: Device shows high memory usage and cpp_ha_top_leve keeps increasing
CSCwp03641	Multiple inside local addreses are translated to the same inside global IP address and port
CSCwo91955	Endpoint tracker remains in the Up state when DNS is reachable from the other interface
CSCwn99822	Large number of BFD sessions stuck due to out of window drops reported with control connections NAT flaps
CSCwp28915	SNMP walk fails to consistently return tunnel names due to incomplete tunnel setup
CSCwo89784	Unexpected reload of standby occurs during PKI trustpoint removal
CSCwn99723	The **request platform software package expand** commands are deprecated for upgrades
CSCwp12923	IKEv2 fails to parse certain route-set prefix Cisco VSA attributes from the Radius server
CSCwo47118	Crash occurs when clearing L2TP tunnels with the clear VPDN tunnel L2TP <ID> command
CSCwb24403	BFD flap on public IP change on a private color TLOC
CSCwo66822	Router reboots due to ucode core dump
CSCwo90396	Serial interface configuration lost after reload
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned
CSCwo12453	The login block-for xx attempts xx within xx? does not function when you set ?access-class xx in vrf Mgmt-vrf? on the line vty
CSCwn57838	Startup configuration is lost for NIM interfaces

Identifier	Headline
CSCwo51627	Unexpected reload occurs due to Critical process linux_iosd_image fault
CSCwn39832	vDSP fails to go into running state or install hangs with no state in **show app-hosting list**
CSCwo03915	Unexpected reload occurs due to performance monitor with packet service insertion from spoke
CSCwp81333	Cache coherency rare timing race condition
CSCwo15543	Standby device reloads after upgrade
CSCwk56650	Unexpected reboot occurs during dialer initialization
CSCwj27134	IP VRF receive command adds connected route to VRF table even though interface admin down
CSCwo34430	Terminal server drops protocol sessions upon executing **Show Memory** command
CSCwo05166	Memory leak on chunk manager via DBAL EVENTS process
CSCwo99641	Out of CGM (Class-Group Manager) memory intermittently with scaled ZBFW policy
CSCwn53302	Administrative distance of IPv6 static route to cellular interface overwrite with 254
CSCwn37412	NTP does not authenticate with open source NTP servers using 32B cmac-aes-128
CSCwk05523	Device crashes with bad magic number in chunk header, with ACL logging hash-generation
CSCwm01063	Unexpected reload occurs due to segmentation fault on IP SLA DynHostName process
CSCwp59954	Crash reported after multicast PIMv2 State-Refresh packet is processed and causes a segmentation fault
CSCwo70548	Ping failure from VRRP backup to VRRP primary virtual address when enabling security policy
CSCwp35552	Missing Calling-Station-ID (31) in Radius Accounting
CSCwn24036	Tx/Rx optical power values diffrent for **show int** and **show hw-module**
CSCwn18584	Traecbacks seen on device while applying configuration on a clean router
CSCwn54648	High CPU on Virtual EXEC and TTY background
CSCwj60804	ACL delete and reapply removes PBR mapping but TCAM is populated
CSCwo22585	Device crashes when running a NWPI trace initiated from vManage
CSCwi59338	Enable strict-kex support in IOS-SSH to address CVE-2023-48795 (Terrapin Attack)
CSCwn92976	PPP is not establishing when L2TP over IPsec

Identifier	Headline
CSCwn59814	FLOWDB_OOM condition can lead to packet loss with GRE non-IPSEC tunnel
CSCwn60286	Memory leak is observed in IPSEC/IKE session bringup with Cert-based authentication
CSCwp15054	Memory leak is seen in nbar-sdavc-scheduler
CSCwo84747	Tunnel delete/create flaps unexpectedly for PWK case for private control NAT changes
CSCwn15850	Device crashes when **show running-config full | format** begins to print QoS Policy-map config
CSCwn50935	Crash occurs during haripin call
CSCwo98465	Crash occurs when receiving BGP MVPN update/withdraw with BGP MVPN update debug enabled
CSCwq01226	Device running with RP3 and ESP200-X crashes every few hrs with nbar /fnf /APM config and high load and QFP utilization
CSCwn93483	Device reports high CPU utilization, in some cases reaching 100% utilization
CSCwq31287	Cisco IOS and IOS XE software SNMP denial of service and remote code execution vulnerability
CSCwn98779	Multihome DC publication has inconsistent domain and mh id

Open Bugs - Cisco IOS XE 17.12.6

Identifier	Headline
CSCwn85623	Missing Calling-Station-ID in radius messages
CSCwq22471	Device unexpectedly reloads after importing subca chain
CSCwq08151	Unexpected reload occurs while running a speed test from and leaves the page before it completes
CSCwo57783	A NHRP Encap Error for Purge Request error message populates on the spoke despite correct routing at HUB
CSCwm54978	The following alert is seen when you boot the device or when you run the **dir bootflash:** command `%SELINUX-1-VIOLATION: Chassis 1 R0/0: audispd: type=AVC msg=audit(1724681880.369:235): avc: denied { getattr } for pid=4585 comm=417578696C69617279205468726561 path="/bootflash/pd_info" dev="sda1" ino=1444321 scontext=system_u:system_r:polaris_iosd_t:s0 tcontext=system_u:object_r:polaris_pd_info_t:s0 tclass=dir permissive=0.`
CSCwp40010	RP crashes while debugging IKEv2
CSCwp38609	CTS trustpoint loop triggers PKI segfault

Identifier	Headline
CSCwq49981	Call failures due to FPI resource leaks

Open Bugs - Cisco IOS XE 17.12.5d

Identifier	Headline
CSCwo38924	Cisco IOS XE software secure boot bypass vulnerability
CSCwo38903	Cisco IOS XE software secure boot bypass vulnerability
CSCwn48408	Cisco IOS XE software HTTP API command injection vulnerability
CSCwm57073	Cisco IOS XE software WebUI reflected cross-site scripting vulnerability
CSCwm41327	Cisco IOS XE software CLI argument injection vulnerability
CSCwm99306	Cisco IOS and IOS XE software TACACS+ authentication bypass vulnerability
CSCwp03900	Cisco IOS XE software Simple Network Management Protocol Denial of Service vulnerability
CSCwq31287	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution vulnerability

Open Bugs - Cisco IOS XE 17.12.5d

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

Resolved Bugs - Cisco IOS XE 17.12.5c

Identifier	Headline
CSCwp66926	FNF AOR might have double-free risk

Open Bugs - Cisco IOS XE 17.12.5c

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

Resolved Bugs - Cisco IOS XE 17.12.5b

Identifier	Headline
CSCwo67161	IPsec-related crash on an IOS-XE device.

Open Bugs - Cisco IOS XE 17.12.5b

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

Resolved Bugs - Cisco IOS XE 17.12.5a

Identifier	Headline
CSCwn07540	C8000V crashes due to LSMPI interface getting stuck
CSCwj85529	C8000V license boot level configuration done via customdata is lost after reload
CSCwk69597	C8000V running config write memory does not persist after reload
CSCwn22830	vDSP container network mask mismatch seen with the VPG interface
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration
CSCwk42190	Config and dp show command don’t match the dp oper output
CSCwj06950	DSL module gets stuck in a booting state
CSCwf79399	Port-channel sub-interface overload. Port-channel interface must be created first and then deleted.
CSCwj80411	Deleting and adding the rules in a ZBFW policy with 510 rules results in traffic drop
CSCwf77488	IOSd crash after device boot up and online
CSCwm72099	ICE PF driver reports MDD with DPDK v21.11 and higher versions
CSCwm14462	IPv6 flowspec nexthop redirect policy does not redirect the traffic on IOS XE
CSCwm05524	Unexpected reload occurs due to "cpp-mcplo-ucode" process when handling fragments with SRv6 routing
CSCwj84949	Unencrypted traffic due to non-functional IPsec tunnel in FLEXVPN hub and spoke setup
CSCwm98642	OMP redistributes summary routes in the service VPN even though the exact networks don't exist
CSCwm80356	LLDP packets dropped when it comes through active port-channel interface
CSCwk79454	Endpoint tracker does not fail if the default route is removed
CSCwk61238	RRI static does not populate route after reload if stateful IPSec is configured
CSCwk75459	MGCP GW fails to respond with 250 OK when there's a delay from dataplane in gathering stats
CSCwk87452	Device unexpectedly reboots when NWPI is run at the site
CSCwm79570	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm89600	Cisco IOS, IOS XE, and IOS XR SNMP Denial of Service Vulnerabilities
CSCwm79581	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79554	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities

Identifier	Headline
CSCwm79596	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79577	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm08791	Dial-peer never recovers an active state if it goes partial or busyout.
CSCwm01029	Calls to certain numbers are failing because the Local Gateway is forwarding the 183 Session Progress and 200 OK to Webex Calling with no crypto attribute in the SDP
CSCwn49403	CUBE incorrectly offers RTP instead of SRTP in 200OK for srtp fallback scenario
CSCwn19326	CDR file accounting creates dummy files
CSCwm03319	Optimize voip trace handling with tenants
CSCwm73825	Crash observed on device while performing the conference calls
CSCwn48914	Router crashes during SGW sync in VOICE REG BG process
CSCwm32946	CUBE doesn't relay/pass 488 Media unacceptable from one leg to another leg for FAX (T.38) Re-INVITEs
CSCwi77331	Device unexpectedly reboots after running the **show sip-ua connection** command
CSCwn09710	Memory leaks are observed for media forking calls
CSCwn60303	The cube sip-ua commands are lost after reload
CSCwn13988	CDR file accounting credentials exposure
CSCwm91190	MWI app not registering on Vcube
CSCwk44855	Cannot dial to/from phone after it reboots in survivability mode
CSCwm82247	Memory leak for SIP out-of-dialog SUBSCRIBE under CCSIP_SPI_CONTROL process
CSCwm79213	*setPthruCryptoData: mfPthruCrypto NULL* shows up excessively in the log
CSCwm91175	OOD Subscribe with event message-summary is causing memory leak
CSCwm47634	No audio issue on call transfer and conference
CSCwm39795	The DATA_RECREATE_ERR: (STBY-Modify): HA Module DSP_MSP reported CALL_MODIFY RECREATE error is seen on standby routers once moh is received with inband DTMF
CSCwm79956	Memory leak under *Dead* caused by AFW_application_proc

Open Bugs - Cisco IOS XE 17.12.5a

Identifier	Headline
CSCwn97600	BFD flapping is seen intermittently with PWK IPsec-rekey
CSCwe23188	Upgrade from vmanage declared successful even though device boots up with different version than requested
CSCwk87338	SNMPv3 user credentials to be stored as part of running-configuration with encryption.

Resolved Bugs - Cisco IOS XE 17.12.4b

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

Open Bugs - Cisco IOS XE 17.12.4b

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

Resolved Bugs - Cisco IOS XE 17.12.4a

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

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

Open Bugs - Cisco IOS XE 17.12.4a

There are no open bugs in this release.

Resolved Bugs - Cisco IOS XE 17.12.4

Identifier	Headline
CSCwk54698	C8000V hosted in Azure reloaded unexpectedly, generating a system report
CSCwj70335	Crypto IKEv2 - Fragmented Authentication packets detected as malformed on 3rd party vendor device

Identifier	Headline
CSCwj44868	GETVPN COOP KS | Wrong severity for rekey acknowledgement configuration mismatch log message
CSCwi88969	FMFP-3-OBJ_DWNLD_TO_DP_FAILED observed when you delete and reconfigure zone-pair back
CSCwi34858	NETVSC VLAN sub interfaces not passing traffic after upgrade
CSCwj21653	Kernel crashes over continuous reloads
CSCwi68865	Memory leak in crypto IKEv2 due to C_NewObject
CSCwj09284	Unexpected reboot in WLC due to SSL
CSCwi40603	Memory leak in the crypto IKMP process
CSCwf87975	Device crashes when port-channel interface flaps with scale of per-tunnel qos policies
CSCwj34578	NAT46 translations are dropped when NAT64 router is also Carrier Supporting Carrier CE
CSCwi55183	**crypto pki certificate pool** in running configuration
CSCwk15127	Failure to communicate a period of time after the stp status changes
CSCwf43856	DPDK RX buffer can get corrupted on DPDK based network drivers causing crash
CSCwj45130	Segmentation Fault - Process = IPSec dummy packet process
CSCwj88872	IPsec tunnel fails to establish due to error IPSec policy invalidated proposal
CSCwj73113	MGCP GW doesn't respond with 250 OK for a DLCX leading to DLCX loop from CUCM side
CSCwi59854	The **show sdwan policy service-path** command gives inconsistent results with app name specified
CSCwj38106	Only one split-exclude subnet is pushed to client PC with IOS-XE headend for an RA VPN connection
CSCwh73320	NAT Pool doesn't work under prefix 16. Available address is zero
CSCwi89822	Unexpected reboot due to cpp ucode on a router
CSCwh86053	ENH: Config parser issue for NAT is seen with extendable and redundancy
CSCwj42249	Disabling PMTU-Discovery with MTU change and BFD flap breaks packet duplication
CSCwi78365	Trim installed certificate on upgrade
CSCwj72888	Reload in tcp_sanity due to l4 pointer not set
CSCwj33292	AnyConnect connection through IPSec fails when connecting from an RDP user to an IOS/IOS-XE headend

Identifier	Headline
CSCwj06622	Segmentation fault and core files are seen on IOS-XE due to speed test
CSCwi16111	IPv6 TCP adjust-mss not working after delete and reconfigure
CSCwj29947	AAA authorization failure during IKEv2 phase negotiation caused unexpected reboot
CSCwj23735	The RTP port range configuration is lost under voice service VOIP after reload
CSCwj26668	Wrong audio RTP packet marking is seen for SCCP SRST
CSCwj23804	Passwords created using **key config-key password-encrypt** ending with a \ are lost after reload
CSCwj59262	SIPREC Secure media forking -1 of 2 audio streams is encrypted due to the same key sent for both streams
CSCwj95128	CUBE incorrectly changes DTMP payload in asymmetric case
CSCwj93967	History-Info header compatibility seen between CUBE and MS direct routing
CSCwj05013	CUBE Media Proxy (CMP) dual forking does not work after upgrade
CSCwj82258	Device may crash during transfer call flow in SRST
CSCwi69071	Unexpected reload caused by crash in 'Skinny Msg Server' process
CSCwj98360	Media forking does not work as expected in CUBE
CSCwj54666	SIP cause code incorrect for CCAPI cause code 31
CSCwk08864	**authentication** command under dial-peer is missing **challenge**
CSCwj61168	Device experiences memory leak in ucode_pkt_PPE0 process
CSCwh81312	NO MEMORY error seen in standby router while checkpointing legs
CSCwj41553	When SGW calls TDM, AOR is not getting changed to number
CSCwj75508	SRST fails to register SCCP phones after reload

Open Bugs - Cisco IOS XE 17.12.4

Identifier	Headline
CSCwj85529	C8000V license boot level configuration done through customdata is getting lost after reload
CSCwh91039	C8000V faces high system CPU load reported due to unsupported number of vCPUs allocated
CSCwj90614	High CPU utilisation for confd_cli
CSCwk03686	Crash due to a segmentation fault because of a negative value

Identifier	Headline
CSCwi03502	IMS is hardcoded for Profile 1 preventing second PDN connection when configuring Multi-PDN
CSCwk52677	Device crashes due to %PLATFORM-3-ELEMENT_CRITICAL memory level / iomd process
CSCwk31560	NAT command is not readable after reload
CSCwk61238	RRI static does not populate route after reload if stateful IPSec is configured
CSCwi86698	No error message is seen while using multicast address as system-IP in SD-routing devices
CSCwh45389	Key manager crashes after hostname change with usage keys
CSCwk44078	GETVPN: Migrating to new KEK RSA key doesn't trigger GM re-registration
CSCwk12524	Device reloads due to ezManage mobile app service
CSCwj77594	WAN IP is allowed to be configured as SYSTEM IP
CSCwk63722	Startup configuration fails post PKI server enablement
CSCwk54544	ZBFW TCAM misprogramming after the rules are reordered on device
CSCwk30527	IKEv2 session is down after reload if identity local address is assigned to an interface on device
CSCwk58303	Watchdog crashes during IPv6 cef adjacency routines
CSCwj84949	Unencrypted traffic due to non-functional IPsec tunnel in FLEXVPN hub and spoke setup
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in the routing table
CSCwh91136	IOS XE:Traffic is not encrypted and is droped over IPSEC SVTI tunnel
CSCwk22942	Unable to build two IPSec SAs with the same source/destination where one peer is PAT'd through the other
CSCwi31110	NHRP-related tracebacks are being generated due to negative global cache count

Resolved Bugs - Cisco IOS XE 17.12.3a

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

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

Resolved Bugs - Cisco IOS XE 17.12.3

Identifier	Headline
CSCwi79584	Upgrade fails for SD-Routing devices via vManage due to error: System config has been modified
CSCwh71278	Appx license boot level configuration is lost in running configuration after upgrade
CSCwh84068	Device crashes after changing NAT HSL configuration
CSCwi10735	ZBF drops transit WAAS PSH/ACK packet due to 'Invalid ACK Number'
CSCwh60968	HSEC install time out, device license status displays **device-request-successful**
CSCwh73350	Device keeps crashing when processing a firewall feature
CSCwh18120	The IKEv2 Diagnose feature is taking 11% CPU during session bring up
CSCwh68508	Unexpected reboot occurs after establishing control plane of EVPN MPLS and receiving packets
CSCwi28227	NAT HSL logging VRF-filter does not work
CSCwh22414	Warning and critical CPU utilization thresholds are not recomputed when using data-plane-heavy mode
CSCwi01046	PoE module does not provide enough power to bring the ports after an unexpected reload
CSCwh77221	SNMP is unable to poll SDWAN tunnel data after a minute
CSCwh96578	SKA_PUBKEY_DB leak in TDL
CSCwh69765	Security policy w/IPS external syslog configuration generation fails for specific devices
CSCwi06843	Endpoint tracker triggers a CPU hog
CSCwh87619	ZBFW is not able to detect packets on TenGig interface
CSCwh10813	Add a detailed log to indicate grant ra-auto un configures grant auto in PKI server
CSCwi60312	Device can't boot up in full configuration
CSCwh93257	Device creates crooked NAT entry if two or more IP phones from NAT outside registers to the same server
CSCwi59121	Mobile-app causes excessive authorization attempts with a null username
CSCwi08171	Device may crash due to crypto IKMP process
CSCwi06404	PKI crashes after failing a CRL fetch
CSCwh50510	Device crashes with segmentation fault(11), Process = NHRP when processing NHRP traffic

Identifier	Headline
CSCwh75800	Device unexpectedly reloads while fetching certificate trustpool for SIP TLS
CSCwi28781	ePBR generates error when the policy is added and deleted multiple times
CSCwi49240	One-way RTP issue including DSP timeout messages (63.2.0 / 62.3.1)
CSCwh45169	Unexpected reboot occurs while dispalying information from cleared SSS session
CSCwh70449	PMTUD incorrectly converges without attempting to learn a higher MTU
CSCwh96415	Cannot disable DMVPN logging in
CSCwi25737	Device should discard IKE notification messages with incorrect DOI
CSCwh50628	Race condition crash on IOS-XE device
CSCwf86207	Frame relay DTE router crashes due to EXMEM exhaustion
CSCwh72869	cpp_mcplo_ucode crashes with port-channel and NAT
CSCwh99399	FTMD crash observed in ENCS platforms while running PWK suite
CSCwi76087	ATO : Session fails to come up with tunnel its shut no shut in loop (cable unplug-plug in customer)
CSCwi55379	IPsec traffic is dropped on Strongswan when PPK is implemented
CSCwi63042	Packet drops observed between LISP EID over GRE tunnel
CSCwi30529	AAA:Template push fails when AAA authorization is set to local

Open Bugs - Cisco IOS XE 17.12.3

Identifier	Headline
CSCwi46997	NAT command is not readable after reloaded
CSCwi67621	Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)
CSCwi16111	IPv6 tcp adjust-mss does not work after delete and reconfigure
CSCwj08744	Unexpected reload occurs when using the **show running-config full | format** command
CSCwj16808	Bootstrap fails to load
CSCwj23835	Syslog flow over TCP port 514 gets dropped under code L7 inspection returns drop

Resolved Bugs - Cisco IOS XE 17.12.2

Identifier	Headline
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP

Identifier	Headline
CSCwh20734	Crypto PKI-CRL-IO_0 process crashes when PKI trustpoint is requested and deleted
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error
CSCwf65696	Non-fabric- loads the minimal bootstrap configs again if device is rebooted without saving the configs
CSCwf49390	Device crashes@crypto_map_unlock_map_head
CSCwh30377	Device data plane crashes in Umbrella/OpenDNS processing due to incorrect UDP length
CSCwf74668	HSEC licenses incrementing
CSCwh20577	Crashed by TRACK client thread at access invalid memory location
CSCwf82676	CPU usage mismatch seen in **show sdwan system status** vs **show proc cpu platform**
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface
CSCwf80191	Flowspec on device won't revoke
CSCwf99947	Device crashes when modifying tunnel after running **show crypto** commands
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z
CSCwf67564	Device observes memory leak at process SSS Manager.
CSCwf60151	Memory leak with pubd.
CSCwh60190	**ip name-server** command not pushed
CSCwf56463	IOS process crashes during VRRP hash table lookup
CSCwh11858	Device running IOS-XE crashes when removing FQDN ACL
CSCwf99906	NTP authentication removed after reload using more than 16 bytes.
CSCwf59173	Segmentation fault at IPv6 BGP backup route notification
CSCwf67351	Cisco IOx application hosting environment privilege escalation vulnerability
CSCwf68612	WLC unexpected ueload due to segmentation fault in WNCD process
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot
CSCwf41084	Extranet multicast code improvements for better handling of data structure
CSCwh04884	VC down due to control-word negotiation
CSCwf26494	BDI + NTP configuration puts DMI process in degraded mode
CSCwh96700	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper

Open Bugs - Cisco IOS XE 17.12.2

Identifier	Headline
CSCwh84068	C8000V crashes after changing NAT HSL configuration.
CSCwh74249	C8000V IPv6 PMTUD packet is fragmented at 1494 bytes
CSCwh71278	Appx license boot level config is lost in running-config after CSR1000V release17.3.4a is upgraded to 17.9.3a
CSCwh94906	Device segmentation fault crashes with Network Mobility Services Protocol (NMSP)
CSCwh73350	Router keeps crashing when processing a firewall feature
CSCwh68508	Unexpected reboot occurs after establishing control plane of EVPN MPLS and receiving packets
CSCwi01046	PoE module is not providing enough power to bring the ports after an unexpected reload
CSCwh16901	HSEC license installation from the workflow does not complete
CSCwh77221	SNMP unable to poll SDWAN Tunnel Data after a minute
CSCwh10813	Add verbose log to indicate grant ra-auto un configures grant auto in PKI server
CSCwh57544	Silent reload due to LocalSoftADR causes crash without core file
CSCwh50510	Router crashes with Segmentation fault(11), Process = NHRP when processing NHRP traffic
CSCwh75800	CUBE router unexpectedly reloads while fetching certificate Trustpool for SIP TLS
CSCwh73320	NAT pool does not work under prefix 16. Available address = zero
CSCwh96700	Carrier grade NAT reaching max host entries and failing to translate due to gatekeeper
CSCwh45169	Unexpected reboot occurs while dispalying information from cleared SSS session
CSCwh70449	PMTUD incorrectly converging without attempting to learn a higher MTU
CSCwf91481	Device crashes unexpectedly after a successful WGB/AP config deployment from OD
CSCwf00276	Packets with L2TP headers cause router to crash
CSCwh83228	NHRP phase 3 spoke-spoke cache got purged after 5-6 hours with always on traffic running
CSCwh91136	IOS XE:Traffic not encrypted and droped over IPSEC SVTI tunnel
CSCwh96415	Can not disable DMVPN logging in IOS-XE
CSCwh12093	Enable SoS/ROC feature for DSL
CSCwf86207	Frame Relay DTE router crashes due to EXMEM exhaustion

Identifier	Headline
CSCwh98527	Device match ICMP trafdfic to VRF 65528 causing ping to not be completed
CSCwh58252	IPv6 SPD min/max defaults to values 1 and 2
CSCwh14083	High CPU due to MPLS MIB poll
CSCwh22981	WNCD process crashes
CSCwh99513	VPLS IRB does not work when traffic comes from VPNv4 and next-hop is learned over VPLS
CSCwh90851	Pubd process shows high CPU utilization
CSCwh83532	1Gig int on device using GLC-SX-MMD are down/down after changing connection
CSCwh96891	Memory leak with pubd
CSCwh91085	Convergence improvement after device reboot with mVPN profile 14
CSCwh58919	NETCONF: DMI enters degraded mode caused by BGP neighbor configured under the SCOPE command
CSCuu85298	FIB/LFIB inconsistency after BGP flap
CSCwf83684	IOS XE router may experience %FMANRP_QOS-4-MPOLCHECKDETAIL: errors
CSCwh59926	EEM is running daily instead of weekly or monthly if special strings @weekly or @monthly are used
CSCwh24280	Mismatch between resource allocation and app-resource profile custom configuration
CSCwh82668	Incorrect local MPLS label in CEF after BGP flap
CSCwh95036	Cisco IOS-XE IPv6 based subscription telemetry does not work
CSCwh99464	Guestshell connectivity does not work with NAT overload
CSCwh30928	SDA - using spt-threshold infinity and having LHR+FHR can cause the S,G to be pruned on the RP
CSCwh01738	Unexpected reload when using rsh/rcmd
CSCwh04124	Locally generated traffic received on incorrect interface inbound and dropped by ACL
CSCwh67285	WLC unable to get telemetry data due to pubd unexpected reload and fail
CSCwh96332	Device crashes due to dhcpd_binding_check
CSCwh56940	Site tag change wncd working/failing EAP-TLS
CSCwh44418	ARP incomplete in VRF Mgmt-intf - G0/0/0 - Switch -G0
CSCwh46559	LLDP location information is not sent when configured

Identifier	Headline
CSCuv36790	The **clear bgp** command does not consider AFIs when used with update-group option
CSCwh02698	Device sending incomplete SGT to ISE
CSCwh05869	Only portion of HSRP config being pushed via CLI ADDON template
CSCwf53750	match pktlen-range does not work with GRE/IPSEC GRE
CSCwh60107	In the show tech file, enable secret does not get hidden
CSCwh45579	Unexpected reload on device ucode core @l2_dst_output_goto_output_feature_ext_path
CSCwh95024	ISIS crashes in local uloop
CSCwh41155	Wrong /32 self, complete map-cache entry for fabric hosts on iBN when overlapping summary exists
CSCwh31485	Member interface config not applied with mis-match in pcakages.conf files
CSCwh72437	WLC does not send accounting start for user auth after machine auth on 9105AXW RLAN dot1x port
CSCwi00680	Router unexpectedly reloads while using DHCP for ISG
CSCwh96823	IOS-XE router not installing classless-static-routes from DHCP option 121
CSCwh77706	SVL, 10G link on the active chassis will go down after reload
CSCwh02592	Device sync fails when device prompt comes along with device banner and TACACS is used
CSCwh84850	Unexpected reboot in device due to SISF and STP initialization
CSCwh64903	Crash on device polling SPA sensor data
CSCwh53432	VLAN name mismatch when authorizing VLAN name from radius server and enable VLAN fallback
CSCwh21796	Password getting visible for the mask-secret in show logging
CSCwh50104	Upgrade failing with config check track-id-name
CSCwf59929	CTS CORE process crash after configuring role based ACL
CSCwh81471	IPv6 traffic is passing through when the client is in Webauth Pending state (CWA)
CSCwh93772	Option 121 never requested by IOS-XE client
CSCwh06087	[IPv6 BGP] multiple sourced paths present for the same prefix
CSCwh29120	IP SPD queue thresholds are out of range
CSCwh14953	CBQoS polling for the object cbQosCMPostPolicyBitRate returns incorrect value

Identifier	Headline
CSCwh89096	Device unexpectedly reloads
CSCwh99597	After migration MAC/IP only MAC is advertised
CSCwh75992	BGP Router process crash
CSCwh48058	Memory leak under MallocLite/AAA proxy with NETCONF/RESTCONF
CSCwh76920	Memory leak in linux_iosd-imag due to SNMP
CSCwh75112	After a reboot, EAP-FAST/PEAP does not authenticate unless credentials are changed

Resolved Bugs - Cisco IOS XE 17.12.1a

Identifier	Headline
CSCwe82666	Not all HSL entries get pushed to the device if more than 1 HSL entries are configured
CSCwe31226	Issues/discrepancies around CPU alarms generated and sent to device
CSCwe43341	TLS control-connections down, traffic from controller dropped with SdwanImplicitAclDrop
CSCwe18124	Macsec remains marked as SECURED, but traffic stops working randomly
CSCwe18276	Route-map not getting effect when its applied in OMP for BGP routes
CSCwb74821	Unexpected behavior due to unstable power source
CSCwe63222	Certificate output does not change on renew when Cloud Certificate Authorization is automated
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail
CSCwe90501	CSR1000V upgrade fails from 17.3.4a to C8000v 17.6.5 due to advertise aggregate with VRF
CSCwe85195	AAR: BoW feature ignoring color preference from Tiered Transport preference configuration
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication
CSCwd53710	Crash seen when umbrella/zscaler template pushed to device when name_lookup takes > 30 sec
CSCwe66318	NAT entries expire on the standby router
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP
CSCwe70374	Platform punt-policer is not configurable

Identifier	Headline
CSCwe73408	For some error condition platform_properties may double free
CSCwd42523	Same label is assigned to different VRFs
CSCwe12194	Auto-Update cycle incorrectly deletes certificates
CSCwe57239	All USB internal communcation is closed when using the **platform usb disable** command
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value
CSCwe85421	BFD Session Down with interface flap
CSCwe95606	Double GR_Additional log enablement defect
CSCwe31471	Segmentation fault in PB rx when per-tunnel qos config withdraw
CSCwe89404	No way audio when using secure hardware conference with secure endpoints
CSCwd39257	IOS-XE cpp crash when entering no ip nat create flow-entries
CSCwe70642	AAR overlay actions are applied to DIA traffic
CSCwa96399	Configuring entity-information xpath filter causes syslogs to print, does not return data
CSCwe79007	Unexpected reload when doing ips test with UTD ips engine
CSCwe31281	Autotunnel IPsec tracker:Tracker does not come up at all on device
CSCwd93401	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM
CSCwd76648	Port-channel DPI load-balancing not utilizing all the member-links
CSCwe39011	GARP on port up/up status from router is not received by remote peer device

Open Bugs - Cisco IOS XE 17.12.1a

Identifier	Headline
CSCwh67812	Unable to configure crypto map on a physical interface due to which crypto map-based VPN's cannot be formed.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP
CSCwh06870	APN password in plain text when Cellular controller profile is configured
CSCwf87292	Punt keep alive failure crash on device controller managed apparently due to for us data packets
CSCwf83850	With pure IPV6, minimal bootstrap unable to onboard Non-Fabric - ipv6 config missing in WAN INT G1

Identifier	Headline
CSCwf94294	Misprograming during vpn-list change under data policy
CSCwf94052	BFD going down for newly onboarded device
CSCwh02439	Unable to add devices to Cloud on Ramp for SaaS due to timeout while loading device list
CSCwh01095	Rapid memory leak on ngiolite process
CSCwf61720	No licenses in use after upgrading from traditional to Smart Licensing IOS-XE versions
CSCwf63771	Non-Fabric:With Multiple interfaces in instance using minimal bootstrap unable to onboard C8000V
CSCwf84522	Unexpected reboot while classifying packet with CTF (Common Flow Table)
CSCwf08895	ENTROPY-0-ENTROPY_ERROR causes constant reboots
CSCwf44703	NAT64 prefix is not originated into OMP
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands
CSCwf77252	SIP calls not working on device with ZBFW enabled
CSCwf92905	C8000V / HSECK9 throughput license fails after deploying a router's snapshot AWS/KVM
CSCwf96416	Device couldn't access any **show sdwan** commands at all
CSCwf67564	Device observes memory leak at process SSS Manager
CSCwf34171	**Configure replace** command fails due to the **license udi PID XXX SN:XXXX** line on IOS-XE devices
CSCwf74668	HSEC licenses incrementing
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot
CSCwf69062	SDRA-SSLVPN : The sslvpn session closes with re-authentication error after some interval of time
CSCwf79264	Traffic forwarded to wrong VPN hence traffic gets wrong zonepair matched and gets dropped
CSCwf71557	IPv4 connectivity over PPP is not restored after reload
CSCwf45486	OMP to BGP redistribution leads to incorrect AS_Path installation on chosen next-hop
CSCwh01313	Unexpected reboot due qfp ucode due to ipsec functions
CSCwf95527	BFD entries removed
CSCwe26895	Router has LocalSoftADR crash, writes flat core, and reloads

Identifier	Headline
CSCwh01318	Multiple crashes observed on platform due to memory exhaustion
CSCwf71116	Static route keeps advertising via OMP even though there is no route
CSCwf60120	Static NAT entry is deleted from running config but remains in startup config
CSCwh00332	B2B NAT: when configration ip nat inside/outside on VASI intereface,ack/seq number abnormal

Related Documentation

Cisco Catalyst 8000V Edge Software Product Page

Cisco Catalyst 8000V Edge Software Data Sheet

Cisco Catalyst 8000V Edge Software Installation And Configuration Guide

Cisco Catalyst 8000V Edge Software High Availability Configuration Guide

Troubleshooting Guide for Cisco Catalyst 8000V Edge Software

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.