Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Amsterdam 17.3.x

First Published: 2020-07-22

Last Modified: 2023-10-28

Cisco 4000 Series Integrated Services Routers Overview

The Cisco 4000 Series ISRs are modular routers with LAN and WAN connections that can be configured by means of interface modules, including Cisco Enhanced Service Modules (SM-Xs), and Network Interface Modules (NIMs).

The following table lists the router models that belong to the Cisco 4000 Series ISRs.

Cisco 4400 Series ISR	Cisco 4300 Series ISR	Cisco 4200 Series ISR
Cisco 4431 ISR	Cisco 4321 ISR	Cisco 4221 ISR
Cisco 4451-X ISR	Cisco 4331 ISR	
Cisco 4461 ISR	Cisco 4351 ISR	

System Requirements

The following are the minimum system requirements:

Note There is no change in the system requirements from the earlier releases.

- Memory: 4 GB DDR3 up to 32 GB
- Hard Drive: 200 GB or higher (Optional). The hard drive is only required for running services such as Cisco ISR-WAAS.
- Flash Storage: 4 GB to 32 GB
- NIMs and SM-Xs: Modules (Optional)
- NIM SSD (Optional)

For more information, see the Cisco 4000 Series ISRs Data Sheet.

Note For more information on the Cisco WAAS IOS-XE interoperability, refer to the WAAS release notes: https://www.cisco.com/c/en/us/support/routers/wide-area-application-services-waas-software/products-release-notes-list.html.

Determining the Software Version

You can use the following commands to verify your software version:

- For a consolidated package, use the **show version** command
- For individual sub-packages, use the **show version installed** command

Upgrading to a New Software Release

To install or upgrade, obtain a Cisco IOS XE Amsterdam 17.3.1 consolidated package (image) from Cisco.com. You can find software images at http://software.cisco.com/download/navigator.html. To run the router using individual sub-packages, you also must first download the consolidated package and extract the individual sub-packages from a consolidated package.

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

For more information on upgrading the software, see the How to Install and Upgrade the Software section of the Software Configuration Guide for the Cisco 4000 Series ISRs.

Recommended Firmware Versions

The following table lists the recommended ROMMON and CPLD versions for Cisco IOS XE 17.2.x onwards releases.

Table 1: Recommended Firmware Versions

Cisco 4000 Series ISRs	Existing ROMMON	Cisco Field-Programmable Devices	CCO URL for the CPLD Image
Cisco 4461 ISR	16.12(2r)	21102941	isr_4400v2_cpld_update_v2.0.SPA.bin isr4400v2hwprogrammbb040100.SPA.pkg
Cisco 4451-X ISR	16.12(2r)	19042950	isr4400_cpld_update_v2.0.SPA.bin
Cisco 4431 ISR	16.12(2r)	19042950	isr4400_cpld_update_v2.0.SPA.bin
Cisco 4351 ISR	16.12(2r)	19040541	isr4300_cpld_update_v2.0.SPA.bin
Cisco 4331 ISR	16.12(2r)	19040541	isr4300_cpld_update_v2.0.SPA.bin

Cisco 4000 Series ISRs	Existing ROMMON	Cisco Field-Programmable Devices	CCO URL for the CPLD Image
Cisco 4321 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4221 ISR	16.12(2r)	19042420	isr4200_cpld_update_v20.SPA.bin

Note Cisco 4461 ISR may require two upgrade packages to upgrade to 21102941. See CPLD-4-1 Release Notes.

Upgrading Field-Programmable Hardware Devices

The hardware-programmable firmware is upgraded when Cisco 4000 Series ISR contains an incompatible version of the hardware-programmable firmware. To do this upgrade, a hardware-programmable firmware package is released to customers.

Generally, an upgrade is necessary only when a system message indicates one of the field-programmable devices on the Cisco 4000 Series ISR needs an upgrade, or a Cisco technical support representative suggests an upgrade.

From Cisco IOS XE Release 3.10S onwards, you must upgrade the CPLD firmware to support the incompatible versions of the firmware on the Cisco 4000 Series ISR. For upgrade procedures, see the Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs.

Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.

New and Changed Information

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 Hardware Features in Cisco IOS XE Amsterdam 17.3.3

There are no new hardware features for this release.

New and Changed Software Features in Cisco IOS XE 17.3.3

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Amsterdam 17.3.3:

- 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.

New Hardware Features in Cisco IOS XE Amsterdam 17.3.2

The following hardware is supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Amsterdam 17.3.2.

- NIM-PVDM is the next-generation digital signal processor (DSP) module to utilize a PVDM4 chip for IP media services. This module enables the Cisco 4000 Series Integrated Services Routers 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 17.3.2

- Smart Licensing Using Policy—An enhanced version of Smart Licensing with the overall objective of providing a licensing solution that does not interrupt the operations of your network but also 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. 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 which 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.

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

- Cisco DNA 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 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.

Note Starting with Cisco IOS XE Amsterdam 17.3.2 release, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

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

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

New Hardware Features in Cisco IOS XE Amsterdam 17.3.1a

There are no new hardware features for this release.

New and Changed Software Features in Cisco IOS XE 17.3.1a

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Amsterdam 17.3.1a:

Note Cisco IOS XE Amsterdam 17.3.1a is the first release for Cisco 4000 Series ISRs in the Cisco IOS XE Amsterdam 17.3.1 release series.

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 does not impact the YANG model functionality.

- 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.
- Configuring Client-Initiated Dial-In VPDN Tunneling—Starting from release 17.3, IPv6 and dual-stack enabling is supported over Virtual-PPP and L2TPv2.
- 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.
- CUBE: Up to 100 VRF Instances—With this feature enhancement, CUBE supports up to 100 VRFs. Each of the VRFs supports up to 10 different RTP port ranges.
- 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.
- CUBE: Consumption of INVITE with Replaces—With this feature, new behavior is introduced for INVITE with REPLACES header consume scenario in CUBE.
- MACsec Encryption on Cisco SM-X-16G4M2X or SM-X-40G8M2X EtherSwitch Service Module—MACsec encryption on Cisco SM-X-16G4M2X or SM-X-40G8M2X EtherSwitch Service Module: The Cisco SM-X-16G4M2X or SM-X-40G8M2X EtherSwitch Service module supports 802.1AE

encryption with MACsec KeyAgreement (MKA) on switch-to-host links and helps in encryption of traffic between the switch and host device.

- Min-flow-rate CommandSet the minimum flow rate bandwidth threshold for the Dynamic Application Policy Routing instance.
- 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.
- Show IP CEF Command—To display all information of CEF, run the show ip cef command. This command in turn displays the output of the following commands therefore avoiding the need to run each of these commands individually.
- Show Platform Resources Command—The existing show platform recourses 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 that originate from IOSd or have destination marked for IOSd or other BinOS processes.
- Show Platform Hardware QFP Active Datapath Utilization Command—The output of the show platform hardware qfp active datapath utilization command now includes crypto and I/O utilization of the device.

Configure the Router for Web User Interface

This section explains how to configure the router to access Web User Interface. Web User Interface requires the following basic configuration to connect to the router and manage it.

- An HTTP or HTTPs server must be enabled with local authentication.
- A local user account with privilege level 15 and accompanying password must be configured.
- Vty line with protocol SSH/Telnet must be enabled with local authentication. This is needed for interactive commands.
- For more information on how to configure the router for Web User Interface, see Cisco 4000 Series ISRs Software Configuration Guide, Cisco IOS XE 17.

Entering the Configuration Commands Manually

To enter the Cisco IOS commands manually, complete the following steps:

Before you begin

If you do not want to use the factory default configuration because the router already has a configuration, or for any other reason, you can use the procedure in this section to add each required command to the configuration.

Procedure

Step 1 Log on to the router through the Console port or through an Ethernet port.

Step 2 If you use the Console port, and no running configuration is present in the router, the Setup command Facility starts automatically, and displays the following text:

```
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

Enter no so that you can enter Cisco IOS CLI commands directly.

If the Setup Command Facility does not start automatically, a running configuration is present, and you should go to the next step.

Step 3 When the router displays the user EXEC mode prompt, enter the **enable** command, and the enable password, if one is configured, as shown in the following example:

```
Router> enable
password password
```

Step 4 Enter config mode by entering the **configure terminal** command, as shown in the following example.

```
Router> config terminal
Router(config)#
```

Step 5 Using the command syntax shown, create a user account with privilege level 15.

Step 6 If no router interface is configured with an IP address, configure one so that you can access the router over the network. The following example shows the interface GigabitEthernet 0/0/0 configured.

```
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip address 10.10.10.1 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)# exit
```

Step 7 Configure the router as an http server for nonsecure communication, or as an https server for secure communication. To configure the router as an http server, enter the **ip http server** command shown in the example:

```
Router(config)# ip http secure-server
```

Step 8 Configure the router for local authentication, by entering the ip http authentication local command, as shown in the example:

```
Router(config)# ip http authentication local
```

Step 9 Configure the vty lines for privilege level 15. For nonsecure access, enter the transport input telnet command. For secure access, enter the transport input telnet ssh command. An example of these commands follows:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# exit
Router(config)# line vty 5 15
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# end
```

Resolved and Open Bugs

This section provides information about the bugs in Cisco 4000 Series Integrated Services Routers and describe unexpected behavior. Severity 1 bugs are the most serious bugs. Severity 2 bugs are less serious. Severity 3 bugs are moderate bugs. This section includes severity 1, severity 2, and selected severity 3 bugs.

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the bug that you have requested cannot be displayed, this may be due to one or more of the following reasons: the bug ID does not exist, the bug does not have a customer-visible description yet, or the bug has been marked Cisco Confidential.

Using the Cisco Bug Search Tool

For more information about how to use the Cisco Bug Search Tool , including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ .

Before You Begin

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool . If you do not have one, you can register for an account.

Procedure

Step 1 In your browser, navigate to the Cisco Bug Search Tool .

Step 2 If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press Enter.

Step 4 To search for bugs related to a specific software release, do the following:

a) In the Product field, choose Series/Model from the drop-down list and then enter the product name in the text field. If you begin to type the product name, the Cisco Bug Search Tool provides you with a drop-down list of the top ten matches. If you do not see this product listed, continue typing to narrow the search results.

b) In the Releases field, enter the release for which you want to see bugs.

The Cisco Bug Search Tool displays a preview of the results of your search below your search criteria.

Step 5 To see more content about a specific bug, you can do the following:

- Mouse over a bug in the preview to display a pop-up with more information about that bug.
- Click on the hyperlinked bug headline to open a page with the detailed bug information.

Step 6 To restrict the results of a search, choose from one or more of the following filters:

Filter	Description
Modified Date	A predefined date range, such as last week or last six months.
Status	A specific type of bug, such as open or fixed.
Severity	The bug severity level as defined by Cisco. For definitions of the bug severity levels, see Bug Search Tool Help & FAQ .
Rating	The rating assigned to the bug by users of the Cisco Bug Search Tool .
Support Cases	Whether a support case has been opened or not.

Your search results update when you choose a filter.

Resolved and Open Bugs in Cisco 4000 Series Integrated Services Routers

Open Caveats - Cisco IOS XE 17.3.8a

All open caveats for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvx77024	IPv6 DMVPN - NBMA address not getting preserved.
CSCwf48808	FlexVPN: Stale client routes stuck in RIB on FlexServer.
CSCvy38743	CISCO-CLASS-BASED-QOS-MIB does not work with LTE Cellular interface on device after reload.
CSCwa76570	Device crashes due to %IDMGR-3-INVALID_ID: bad id in id_delete during session roaming.

Caveat ID Number	Description
CSCwf03193	Device crash with crashinfo files were generated with Segmentation fault, Process IPSEC key engine.
CSCwf80400	IOS XE router may experience unexpected reset while executing **show utd engine standard statistics**.
CSCwa69101	ISG: initiator unclassified ip-address LQipv4 command has no effect.
CSCvz63684	EWC HA pair expereincing IOS tracebacks, followed by KEYMAN crash.
CSCwb03455	Inter-VRFroute leaking not working and packet drop seen due to Ipv4Unclassified.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwe60059	Crash when using dial-peer groups with STCAPP.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwc39865	Subscriber session getting stuck and needs clearing it manually.
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface.
CSCvy54048	CPP unexpected reboot while freeing CVLA chunk.
CSCwb78173	CSDL failure: IPSec QM use of DES by encrypt process is denied.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwe41234	VMWI race condition causes no ringing for analog phones.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCwd03931	Device crashes due to cpp_cp_svr fault on fp_0_0 (rc=134) when applying umbrella dnscrypt to profile.
CSCwa67851	Router traceback and reload when different encapsulation used on xconnect interfaces.
CSCwf55830	No dial tone on analog phones due to DSP going into Power Denial state.

Resolved Caveats - 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 Caveats - Cisco IOS XE Amsterdam 17.3.8

All open caveats for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvx77024	IPv6 DMVPN - NBMA address not getting preserved.
CSCwf48808	FlexVPN: Stale client routes stuck in RIB on FlexServer.
CSCvy38743	CISCO-CLASS-BASED-QOS-MIB does not work with LTE Cellular interface on device after reload.
CSCwa76570	Device crashes due to %IDMGR-3-INVALID_ID: bad id in id_delete during session roaming.
CSCwf03193	Device crash with crashinfo files were generated with Segmentation fault, Process IPSEC key engine.
CSCwf80400	IOS XE router may experience unexpected reset while executing **show utd engine standard statistics**.
CSCwa69101	ISG: initiator unclassified ip-address LQipv4 command has no effect.
CSCvz63684	EWC HA pair expereincing IOS tracebacks, followed by KEYMAN crash.
CSCwb03455	Inter-VRFroute leaking not working and packet drop seen due to Ipv4Unclassified.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwe60059	Crash when using dial-peer groups with STCAPP.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwc39865	Subscriber session getting stuck and needs clearing it manually.
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface.
CSCvy54048	CPP unexpected reboot while freeing CVLA chunk.
CSCwb78173	CSDL failure: IPSec QM use of DES by encrypt process is denied.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwe41234	VMWI race condition causes no ringing for analog phones.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCwd03931	Device crashes due to cpp_cp_svr fault on fp_0_0 (rc=134) when applying umbrella dnscrypt to profile.
CSCwa67851	Router traceback and reload when different encapsulation used on xconnect interfaces.
CSCwf55830	No dial tone on analog phones due to DSP going into Power Denial state.

Resolved Caveats - Cisco IOS XE Amsterdam 17.3.8

There are no resolved caveats in this release.

Open Caveats - Cisco IOS XE Amsterdam 17.3.7

All open caveats for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCwa69101	ISG: **initiator unclassified ip-address LQipv4** command has no effect.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCvx77024	IPv6 DMVPN - NBMA address not getting preserved.
CSCvy38743	CISCO-CLASS-BASED-QOS-MIB doesn't work with LTE Cellular interface 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.
CSCvz89354	Router crashes due to CPUHOG when walking ciscoFlashMIB.
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.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwb78173	CSDL failure: IPSec QM use of DES by encrypt proc is denied.
CSCwe41234	VMWI race condition causes no ringing for analog phones.

Resolved Caveats - Cisco IOS XE Amsterdam 17.3.7

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

Caveat ID Number	Description
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.
CSCwc77663	Device frequent reloads due to stuck thread in CPP.
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.

Caveat ID Number	Description
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 55.1.6 Release targeting v173_throttle.
CSCwe37184	Device seeing out of service on Switch modules with new DC power supply.

Open Caveats - Cisco IOS XE Amsterdam 17.3.6

All open caveats for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvx77024	IPv6 DMVPN - NBMA address not getting preserved.
CSCwb72336	ICMP traceroute return packet not classified based on FW override port info.
CSCvy38743	CISCO-CLASS-BASED-QOS-MIB doesn't work with LTE Cellular interface on device after reload.
CSCwa76570	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.
CSCwc30050	UTD: Exception in utd_logger.py due to missing extra-data in AMP alert.
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map.
CSCwb66749	When configration ip nat inside/outside on VASI intereface,ack/seq number abnormal.
CSCwb78228	Platform rebooted unexpectedly with reason "LocalSoft".
CSCwa13553	Platform 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.
CSCvz07542	Device with NIM-ES2 "no igmp snooping vlan x" is not preserved after reload.
CSCvz63684	EWC Ha pair expereincing IOS Tracebacks, followed by KEYMAN crash.
CSCvy94954	LA LED turns green when just inserted SFP-10G-LR without cable connecting.
CSCvx64449	%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: mac verify failed due to ip rtp header-compression iphc-format.
CSCwc22314	IR1101-K9 - RTSP Traffic not being rewritten by NAT.

Caveat ID Number	Description
CSCwb17282	Router crashing when clearing a VPDN session.
CSCvx74212	IKEv1 IPSec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ.
CSCwb08057	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
CSCwc25291	NIM-LTE-EA No Data - requires subslot reload to recover.
CSCvw34956	HSRP and VRRP Virtual IP address is not reachable.
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.
CSCwb35303	X25 FRMR seen when switching from XOT to low speed serial.
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.
CSCvx71735	IOS-XE Device may experience an unexpected reset in "SNMP ENGINE" when polling cEigrpInterfaceEntry.
CSCwb46968	Device template attachment causes pppoe commands to be removed from ethernet interface.
CSCvy54048	CPP unexpected reboot while freeing CVLA chunk.
CSCwc56033	Not triggering any alarms when RPM of a fan is 0.
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.
CSCwc39865	Subscriber Session getting stuck and needs clearing manually.
CSCwa43562	Link goes err-disabled due to link-flap after reloading peer device.
CSCvv55742	GETVPN-ipv6 & LISP support.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCvx73750	Device 5G light is blue when 4G LTE is in use.
CSCvz53819	ZBFW : ARStandby drops seen on New Active during RG switchover.

Caveat ID Number	Description
CSCvx28426	Router may crash due to Crypto IKMP process.
CSCwc70468	CPA fail to send SIP update for AsmT before "maxTermToneAnalysis" expiration.

Resolved Caveats - Cisco IOS XE Amsterdam 17.3.6

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

Caveat ID Number	Description
CSCwb23043	MACsec not working on subinterfaces using dot1q >255.
CSCwb76988	IKEv2 fragmentation causes wrong message ID used for EAP authentication.
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 de to watchdogs after issuing the commands sh crypto mib ipsec commands.
CSCwb03662	CDP/LLDP not working when 10GE interface enabled with MACsec.
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	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwa49902	MGCP automatic configuration fails after IOS-XE upgrade.
CSCwb22552	Platform abnormal Kerlog log is produced when port in shutdown state.
CSCwb04815	NHRP process taking more CPU with ip nhrp redirect configured.
CSCwa72273	ZBFW dropping return packets from tunnel post upgrade.
CSCwb38501	Support IGMP on voice vlan.
CSCwa51582	IP Device-tracking not functional with voice VLAN configured.
CSCwb25137	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: C11xx platforms running 17.x - crypto ipsec policy installation fails.
CSCwa67398	NAT translations do not work for FTP traffic.

Caveat ID Number	Description
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.
CSCwb65455	Renewing hardware wan edge cert shows old cert serial/valid date in control local-properties.
CSCwb77202	Interface comes up with only an SFP inserted.
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 with 17.3.1prd10 image.
CSCwb15331	Keyman memory leak using public keys.
CSCvy30606	Device fails to update sdn-network-infra-iwan key after 1 year.
CSCvz00054	Nested IPSec tunnels encryption does not work as expected on platforms with crypto offload enabled.
CSCwa82825	Sub-interface may not forward traffic after a reload.
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 - Cisco IOS XE Amsterdam 17.3.5

All open caveats for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvx77024	IPv6 DMVPN - NBMA address not getting preserved
CSCwa92734	CUBE DTMF interworking fails from rtp-nte to OOB SIP methods
CSCvv81296	Protocol specific change for base path
CSCwa10809	Kernel crash with last reload reason "LocalSoftADR"
CSCvx94323	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut
CSCwa58911	Removing service-policy from the Zone-pair causes device crash

Caveat ID Number	Description
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
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
CSCvy26572	[SWI : #01080538] LTE is not reestablishing after reset of the modem
CSCvz07542	ISR4K with NIM-ES2 "no igmp snooping vlan x" is not preserved after reload.
CSCwa34648	Incorrect OMP Labels in On-Demand Tunnel H/S Topology
CSCwa49902	MGCP automatic configuration fails after IOS-XE upgrade on ISR4k
CSCvy94954	LA LED turns green when just inserted SFP-10G-LR on ISR4k without cable connecting
CSCvx64449	%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: mac verify failed due to ip rtp header-compression iphc-format
CSCvw13048	crash observed at NHRP while using summary-map
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
CSCwa59824	ngiolite: core generated after oir of SFP-10G-SR on ISR4461
CSCwa51732	Getting "%IOSXE_QFP-2-LOAD_EXCEED" on ISR4K by using code version "17.03.04a.0.5574"
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)
CSCvx71735	IOS-XE Device may experience an unexpected reset in "SNMP ENGINE" when polling cEigrpInterfaceEntry
CSCvx93477	ISR4431 PWR-GE-POE-4400 looses VID and SN after upgrade
CSCvx28426	Router may crash due to Crypto IKMP process
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
CSCvy41947	EIO: Packets getting reassembled and are forwarded as it is to the Gigabit interface

Caveat ID Number	Description
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
CSCvz53819	ZBFW : ARStandby drops seen on New Active during RG switchover
CSCwa58437	intermittent SSH TCP checksum miscalculation while decrypting and processing the FlexVPN traffic
CSCvz00054	CAT8300 nested IPSec tunnels encryption does not work as expected
CSCwa52807	Router ISR unexpectedly rebooted due to local soft QFP0 Fatal Fault: Ucode process fault

Resolved Caveats - Cisco IOS XE Amsterdam 17.3.5

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

Caveat ID Number	Description
CSCvz21267	ISR 4K running in sdwan controller mode experiencing module reload due to NGIO control packet loss
CSCvz41766	VG450 Crashes Repeatedly in IOSd due to HTSP
CSCvy95586	SCCP gateway auto configuration download results in an incomplete configuration.
CSCvx11389	NAT TCP Load Balancing not working on IOS XE
CSCvo41609	GETVPN: Clearing members on Key Server causing rekey processing failure on GMs
CSCvz47421	VLAN IP config missing on bootup due to missing startup configs
CSCvy67657	crypto ipsec security-association dummy leads to packet loss
CSCwa36699	Prefetch CRL Download Fails
CSCvy74799	Ucode crash observed at tw_bad_timer_bucket () at ../../../infra/tw_timer.c:918
CSCwa15132	DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum
CSCvx77674	A router may crash when processing an NHRP packet
CSCvx97490	ISR4321 | After enabling "cts manual" the interfaces start flapping
CSCvy54606	CVLA need to reserve at least 50M memory for low-end DRAM platform

Caveat ID Number	Description
CSCvy34102	CPP ucode crash with route-map and overload at ipv4_nat_rmap_walk_find.
CSCvz71436	Call Placing issue from SCCP phones
CSCvy31577	PDP Type error on isr4k using Cellular 4G
CSCvx39529	IKEv1/IKEv2 "show crypto session brief" output empty
CSCvy24571	Static NAT conflicts/overwrites with Port-forwarding
CSCvt35331	Console port goes unresponsive, reboot required to restore it.
CSCvw84042	IOS-xe does not correlate indices properly with cellular radio band output
CSCvz07134	Router does not boot on recent 16.X releases with large service policy applied on the interface.
CSCvz76277	Hostname not allowed beginning with numbers
CSCvz73780	memory leak with fman_cc process when SM-X-G4M2X module installed
CSCvz63029	Poor DMVPN performance when used with IPSEC (Transport Mode) and GRE options are enabled
CSCvy01097	Router may crash under ZBF configuration (cpp_cp_svr)
CSCvy98230	ISR4461 crashed in SSLVPN stress test
CSCvt66541	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted
CSCvy89461	Crash when getting cdspCardStatusEntry OID
CSCwa11150	E1 configurations (under Serial interface) lost after reload.
CSCvz50081	Curie: posix_printf does not work on COFF core in calo testbed
CSCvz58895	IOS-XE unable to export elliptic curve key
CSCvy89785	OSPFv3 adjacency won't come up after "ospfv3 authentication ipsec" is applied on Tunnel interface
CSCvx76924	Crash seen on executing 'no ccm-manager sccp'
CSCvw91361	Crash when issuing "show crypto isakmp peers config"
CSCvy85141	tdm-group timeslot 31 failed to create/connect
CSCvw48943	crypto ikev2 proposals are not processed separately
CSCvv38438	Watchdog timeout due to Crypto IKMP

Open Caveats - Cisco IOS XE Amsterdam 17.3.4a

All open caveats for this release are available in the Cisco Bug Search Tool.

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
CSCvx71735	"SNMP ENGINE" Crashes When Polling cEigrpInterfaceEntry MIB
CSCvx74212	IKEv1 IPSec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
CSCvy54314	Data-policy local-tloc with app-route is dropping packets when SLA is not met
CSCvy58115	Cedge : Cloudexpress Office 365 probes are hitting 100% loss
CSCvy67301	URL Filtering regex pattern match not working on large pattern
CSCvy73818	cEdge QFP starts dropping traffic - UTD Service Node not healthy ident
CSCvy78123	cEdge: High CPU usage due to Multicast and Data Policy configuration.
CSCvy78943	Cisco 4451 ISR: Startup config lost for NIM-2GE-CU-SFP after upgrade to Amsterdam
CSCvy82696	cEdge dropping packets [combination /16, /17 data prefix with multiple ports in policy]
CSCvy69555	Unable to fetch eigrp prefix, nexthop, omptag, and route origin

Resolved Caveats - Cisco IOS XE Amsterdam 17.3.4a

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

Caveat ID Number	Description
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

Caveat ID Number	Description
CSCvw74609	Cisco 4000 Series ISR LACP Configuration lost: channel-group X "mode active" gets removed on reload
CSCvw81572	Multiple crashes cpp_cp_svr and qfp-ucode on 16.12.4
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.
CSCvx33043	Cisco 4400 ISR routing multicast packets out of order VASI-left in VRF RIB VASI-right in Global RIB
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
CSCvx45788	cannot apply ciscosdwan.cfg due to vpg-log-server-acl ACL on VirtualPortGroup0 for logging
CSCvx53049	Crash when TPOOL is updating and 'wr mem' is issues at same time
CSCvx57615	ZBFW blocking ACK packets for applications using cloudexpress SaaS set to use a Gateway with synsent
CSCvx59899	Cisco 4431 ISR/K9 rebooting due to CPP crashing becaue of UTD feature.
CSCvx64846	"show sdwan policy service-path/tunnel-path" command cause device crash
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
CSCvx88246	Packets dropped due to firewall + data policy interop issue
CSCvx89710	SCEP: CA server fails to rollover CA certificate with error: "Storage not accessible"

Caveat ID Number	Description
CSCvx97718	vtcp frees rx buffer when packet with expected next sequence arrives with no payload; phones reset
CSCvy14126	Cisco 4331 ISR are crashing frequently 17.4.1b
CSCvy25957	Security container is dropping legitimate FIN,ACK Packets
CSCvy30209	IOS-XE cpp ucode crash with fragmented packets
CSCvy31298	Cisco 4461 ISR NIM-2GE-CU-SFP - Sub-interfaces not transmitting traffic
CSCvy35044	Signature update failure - SSL-CERTIFICATE_VERIFY_FAILED

Open Caveats - Cisco IOS XE Amsterdam 17.3.3

All open caveats for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvw74609	Cisco 4000 Series ISR LACP Configuration lost: channel-group X "mode active" gets removed on reload
CSCvw89001	LTE interface is not getting IP address after upgrading teh router.
CSCvw89147	Crash at the moment of calculating tcp header
CSCvw92643	Netflow crash at fnf_ipv6_output_feature_final_internal with flow record on IPv6 IPsec tunnel.
CSCvw96723	CP process crashed while I95 driver was adding an IPC response to the receive ring
CSCvx14095	NETCONF ACL not working if ACL is referencing an object-group.
CSCvx17563	Cisco 4331 ISR/K9 running 16.12.04 crashed with Segmentation fault(11), Process = Cellular CNM
CSCvx18526	Clients using DHCP Server Port-Based Address Allocation not getting IP address.
CSCvx22522	cpp-mcplo-ucode crashes on Cisco 4461 ISR
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
CSCvx33043	Cisco 4400 ISR routing multicast packets out of order VASI-left in VRF RIB VASI-right in Global RIB
CSCvx35902	fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash.

Caveat ID Number	Description
CSCvx38454	ISR Crash for CENT-MC-0 process
CSCvx40030	IP PIM SPT-threshold infinity causes ICMP Echo Replies to not be generated for IP Multicast Requests

Resolved Caveats - Cisco IOS XE Amsterdam 17.3.3

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

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
CSCvu59952	Cisco 4461 ISR: Control Connections over sub-interface are down after upgrade, TX Channel create failure
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
CSCvv58312	17.4 : Dataplane Crash due to driver cpp_drv_i95_read_cb observed on Cisco 4461 ISR with traffic
CSCvv61770	Crash seen in isis_sr_uloop_lspdb_dump with 'debug isis microloop' enabled
CSCvv64633	BGP: advertised community list is malformed due to GSHUT community
CSCvv71775	Cellular interface down/up frequently occurs with DoCoMo MVNO sim
CSCvv78028	No responder-bytes from cEdge when UTD is enabled
CSCvv79273	Router may crash when using Stateful NAT64
CSCvv88621	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage
CSCvv91865	Moving PC from network causes static DHCP binding to be removed from the device.
CSCvv98528	Cisco 4000 Series ISR SER parity error checks continuing till router crashes
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

Caveat ID Number	Description
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
CSCvw14836	ISR router running 16.9.6 crashes authenticating crypto certificate
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
CSCvw23041	Crash seen on Fugazi due to %CPPHA-3-FAILURE: R0/0: cpp_ha: CPP 0 failure Stuck Thread(s)
CSCvw30128	ip-acl errors of correcting the logic of sequence id when there is an error with msg creation
CSCvw31389	pktlog functionality is broken
CSCvw32481	EVPN Type-2 IP/MAC route is created for not-connected SVI
CSCvw33113	Unexpected reload in NHRP when access to an invalid memory region
CSCvw34157	APPNAV CFT Crashes
CSCvw36514	cEdge crashes due to a large packet at vesen_ipsec_v4_input_get_vctrl_data
CSCvw37109	Pseudowire interface may be unexpectedly removed from VFI on unrelated configuration change
CSCvw38433	OMP-Agent Routes in EIGRP changes AD to 252 on non-SDWAN devices
CSCvw39383	CPP ucode crash with fw_base_flow_create
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

Caveat ID Number	Description
CSCvw57860	Duplicate entries seen in MAC filter table.
CSCvw58560	FlexVPN reactivate primary peer feature does not work with secondary peer tracking
CSCvw62805	SDWAN ZBFW CPU punted traffic mishandling -- Out2In packet looped
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
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.
CSCvx19135	ISR crashes when ZBFW ALG inspects tunneled packet
CSCvx19209	ISIS crash in isis_sr_tilfa_compute_protection
CSCvx36844	Control plane hitting EID prefix entry limit for MAC after upgrade

Open Caveats - Cisco IOS XE Amsterdam 17.3.2

All open caveats for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvu77745	PMAN-3-PROCFAIL: Chassis 1 R0/0: pman: R0/0: The process keyman has failed (rc 139).
CSCvu89597	RM crash at __be_address_cmp __be_avl_get_next while doing shut/no shut or BR.
CSCvu89599	BR crash at __be_strlen __be_fman_rtmap_create_route_map_msg.
CSCvv40206	Router may crash under ZBF configuration.
CSCvv51001	Crash during BGP VPN route import.
CSCvv79273	Router may crash when using Stateful NAT64.
CSCvv91204	SSS crashed the router at the moment of freeing AAA request.
CSCvw05211	Pre-mature session deletion leading to churn and lower TPS at scale.
CSCvw09093	Route not getting installed, need to remove and reattach the template.

Caveat ID Number	Description
CSCvw14836	Cisco ISR router running 16.9.6 crashes authenticating crypto certificate.
CSCvw16643	Device Template failing to attach after changing few device variables.
CSCvw16816	Cisco 4000 ISRs fails to install new IPSec SAs.
CSCvw22760	MACSEC MKA stops forwarding data after every 3rd rekey.

Resolved Caveats - Cisco IOS XE Amsterdam 17.3.2

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

Caveat ID Number	Description
CSCvj29514	CME: Toll fraud app not automatically trusting traffic from phones.
CSCvp73666	DNA - LAN Automation doe not configure link between Peer Device and PnP Agent due CDP limitation.
CSCvq65366	Cube might crash when sending a SIP message over TLS.
CSCvq73575	TCP traceroute - response ICMP TTL exceeded packet dropped by ZBFW with NAT enabled.
CSCvq90343	Secure SIP trunk between SIP-GW/CUBE and CUCM with multiple nodes not coming in to service.
CSCvq97906	DHCPD Receive process crash.
CSCvq98999	Crash when IPSEC SA installation fails @ imgr_ipsec_sa_n2_install_done.
CSCvq99498	Crashes when trying to bring-up / bring-down IPsec crypto session for OSPFv3.
CSCvr00983	Unrecoverable Error with PVDM in 0/4 and Thule+dreamliner in 1/0 on Cisco 4300 ISR
CSCvr01327	Incorrect Total number of translations on show ip nat translations.
CSCvr01454	Punt fragment crash when receive EoGRE packets which have many fragments.
CSCvr05213	Smart licensing PID and SN logs filling up the IOSRP tracelogs.
CSCvr05504	Dialer interface counter does not correlate to the counter of interfaces bounded to.
CSCvr06666	Cisco 4000 Series routers CPP ucode Crash due IPv4 Fragmented packets.
CSCvr12455	KPML dialing fails after CSCvq20936 commit.
CSCvr13358	STUN packet breaks MOH RTP packet flow.
CSCvr13385	CUBE/LGW: STUN Indication packets generated constantly for call forking flows.
CSCvr17169	QFP ucode crash with media monitor.

Caveat ID Number	Description
CSCvr24316	Router crashes due to Segmentation Fault when ccb gives a NULL Pointer.
CSCvr26524	Crash due to NBAR classification.
CSCvr31188	GETVPN gikev2 Secondary KS does not push new policy after merging split condition.
CSCvr33415	Router may crash unexpectedly with Segmentation fault(11), Process = DSMP.
CSCvr39932	IPSEC install failed IPSEC_PAL_SA shows "unexpected number of parents.
CSCvr41793	IOS PKI: CRL retrieval does not use HTTP Content-Length.
CSCvr48349	ESP ucode crashed when running NAT with bpa (CGN).
CSCvr51860	Observed Traceback with SRTP-RTP call after hold/resume.
CSCvr57565	MGCP Calls with SRTP fail to connect with Cause Value=47 due to T.38 calls.
CSCvr58230	While signalling forking the CUBE is not Sending Re-INVITE for T.38 with the Authorized header.
CSCvr61217	GetVPN in Cisco 4461ISR: Getvpn traffic is failing with Transport mode with all the versions.
CSCvr66754	CME-Cisco 4000 Series ISR: BLF working Inconsistently on IOS XE 16.09.03.
CSCvr72844	CUBE generates 400 Bad Request when INVITE contains a large SDP and sip profiles are in use.
CSCvr76534	Cisco 4000 Series ISRs: clear counters command may cause router to crash.
CSCvr80706	IOS XE - ucode crash in ZBF during flow creation for TCP subflows/.
CSCvr90926	CUBE is updating the resolved IP only after the REGISTER expires.
CSCvr96597	IOS-XE crash after doing a SCEP enrollment.
CSCvr99034	Cisco 4000 Series ISRs crash during updating the OpenDNS bypass whitelist
CSCvs01943	Login authentication VTY_authen" is missing on "line vty 0 4" only.
CSCvs13960	IWAN High CPU and Memory
CSCvs29535	IWAN crash related to DCA channel.
CSCvs47682	Router crashed when attempting to remove a nonexistent trustpoint from dspfarm profile.
CSCvs56721	Spoke-to-spoke PLR packets should not change the interface PLR status.
CSCvt20318	BGP Neighbors stuck on device.
CSCvt48480	Flow monitor is removed from interface configuration on reload.

Caveat ID Number	Description
CSCvt62112	Physical policy cannot be clean up with QoS policy in suspended mode on PPPoE dialer.
CSCvt91720	Ruter see http wsma request as coming from 192.168.1.5.
CSCvu09862	Call Rerouting functionality not working on 16.6/16.12/17.1 IOS-XE trains.
CSCvu18001	Segmentation fault observed in BGP -"UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scanner".
CSCvu19733	Evaluation of CVE-2020-11868 for IOS.
CSCvu26741	Punt-Keepalive crash with lsmpi_lo_drv and container app traffic.
CSCvu27953	Crash due to a segmentation fault in the "IPsec background proc" process.
CSCvu54786	Crash on configuring a highest key identifier for OSPF authentication under an interface.
CSCvu70286	L2RIB thread crashed after removing global vrf definition for evpn.
CSCvv01445	Router Crashes when advertised-routes command executed for neighbours.
CSCvv02486	Random MPLS-TE tunnels with explicit-path stay down after egress interface is bounced.
CSCvv04236	IOS-XE: IPv6 OSPF authentication ipsec - adjacency fails.
CSCvv08341	Netconf deleting wrong IKEv2 parameters.
CSCvv17488	Cisco 4000 Sereis ISR with SM-X-ES3 module: Memory leak in iomd.
CSCvv17560	BMP BGP server can lead to CPUHOG and crashes
CSCvv20380	Removing and Adding Bulk ACL leads to Tracebacks and Error-Objects.
CSCvv26042	IOS crash at l2rib_server_ios_obj_notification.
CSCvv26538	Crash due to a NULL pointer while bringing down PPPoE sessions.
CSCvv34057	Cisco 4351 ISR:Crash seen with ZBFW. Reboot reason:Critical process qfp_ucode_utah fault on fp_0_0 (rc=139).
CSCvv43279	[EVPN RT2-RT5] Routing Loop due to CGW re-originating the Type 2 MAC+IP with MAC+IP VRF details
CSCvv64319	BGP crash in bgp_show_network_detail, bgp_imp_find_imported_path_topo.
CSCvv72254	EVPN incorrect duplicate v4/v6 default routes, crash eventually.
CSCvv94834	BGP crash during IOL testbed launch.
CSCvv85766	Memory leak upon ssh/scp connections to a router.

Open Caveats - Cisco IOS XE Amsterdam 17.3.1

All open caveats for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvu59952	Cisoc 4461 ISR: Control Connections over sub-interface are down after upgrade, TX Channel create failure.
CSCvu92277	Memory leak observed for FTM process leading to a device crash eventually.
CSCvv08341	Netconf deleting wrong IKEv2 parameters.
CSCvt65588	FlexVPN IKEv2 Tunnel route removed after establishing new IKEv2 SA to another peer.
CSCvu00804	AnyConnect authentication fails when password contains "&" character.

Resolved Caveats - Cisco IOS XE Amsterdam 17.3.1

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

Caveat ID Number	Description
CSCvp24405	Router crashes after adding macsec reply-protection command on an interface.
CSCvs45107	AnyConnect fails to reconnect when original session expires.
CSCvs56559	Show crypto PKI server shows wrong expire certificate date.
CSCvs65950	IOS PKI: P12 not generated on IOS Sub CA at rollover certificate generation.
CSCvs81967	Cisco 4000 Series ISRs: %BOOT-3-BOOT_SRC: R0/0: No space on boot /dev/bootflash5 for packages, using bootflash!.
CSCvs85642	Cisco 4000 Series ISRs crash when rtp-nte DTMF packet arrives at MTP + BDI.
CSCvs88686	Cisco 4000 Series ISR crash in cpp_cp_svr due to watchdog timeout.
CSCvs98389	Packet drops in XE-SDWAN because of IN_CD_COPROC_ANTI_REPLAY_FAIL" errors.
CSCvs99705	PKI CLI - no warning that rsakeypair name starting from 0 (zero) is not working for cert regenerate.
CSCvt01186	Interface does down when "l2vpn xconnect" command is removed.
CSCvt03869	Router reloads due to crypto pki crl request <trustpoint-name> during get a fresh copy of CRL.
CSCvt21263	Crash upon delete of virtual-access when virtual-template has "no tunnel protection ipsec initiate".
CSCvt31561	TBAR is not disabled in GM when it is disabled in KS.
CSCvt35947	Duplicate ipv6 address while connecting to remote client.

Caveat ID Number	Description
CSCvt40523	GETVPN: KS 16.12.x - COOP switchover causes GMs to immediately use new TEK rekey.
CSCvt52051	IPsec tunnel is getting established for a backup NHS DMVPN hub.
CSCvt52825	Memory leak in SCCP TLS Client on unexpected deregister event.
CSCvt65588	FlexVPN IKEv2 Tunnel route removed after establishing new IKEv2 SA to another peer.
CSCvu82189	Enabling guestshell gives "float division by zero".
CSCvv05776	CXP Probe DNS packets are not exiting via correct source interface.
CSCvv05776	NAT doesnt translate SIP headers orignial source for return traffic on IOS XE 16.9.3 and 16.9.4.

Related Documentation

- Release Notes for Previous Versions of Cisco 4000 Series ISRs
- Hardware Installation Guide for Cisco 4000 Series Integrated Services Routers
- Configuration Guides for Cisco 4000 Series ISRs
- Command Reference Guides for Cisco 4000 Series ISRs
- Product Landing Page for Cisco 4000 Series ISRs
- Datasheet for Cisco 4000 Series ISRs
- Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs
- Field Notices
- Cisco Bulletins