

# Release Notes for Cisco ISR 1100 Series, Cisco IOS XE Fuji 16.9.x

**First Published:** 2020-07-14

**Last Modified:** 2021-10-21

## Overview of Cisco 1100 Series Integrated Services Routers

The Cisco 1100 Series Integrated Services Routers (ISR) are powerful fixed branch routers based on the Cisco IOS XE operating system. They are multi-core routers with separate core for data plane and control plane. There are two primary models with 8 LAN ports and 4 LAN ports. Features such as Smart Licensing, VDSL2 and ADSL2/2+, 802.11ac with Wave 2, 4G LTE-Advanced and 3G/4G LTE and LTEA Omnidirectional Dipole Antenna (LTE-ANTM-SMA-D) are supported on Cisco 1100 Series ISRs.



**Note** Explore the [Content Hub](#), the all new portal that offers an enhanced product documentation experience.

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

Get started with the Content Hub at [content.cisco.com](https://content.cisco.com) to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

The following table lists the router models that belong to the Cisco 1100 Series ISRs.

Cisco 1100 Series ISRs	
C1111-8P	C1111-4P
C1111-8PLTEEA	C1111-4PLTEEA
C1111-8PLTELA	C1111-4PLTELA
C1111-8PWE	C1111-4PWE
C1111-8PWB	C1111-4PWB
C1111-8PWA	C1111-4PWA
C1111-8PWZ	C1111-4PWZ
C1111-8PWQ	C1111-4PWN
C1111-8PWN	C1111-4PWQ

Cisco 1100 Series ISRs	
C1111-8PWH	C1111-4PWH
C1111-8PWR	C1111-4PWR
C1111-8PWF	C1111-4PWF
C1111-8PLTEEAWE	C1111-4PWD
C1111-8PLTEEAWB	
C1111-8PLTEEAWA	
C1111-8PLTEEAWR	
C1111-8PLTELAWZ	
C1111-8PLTELAWN	
C1111-8PLTELAWQ	
C1111-8PLTELAWH	
C1111-8PLTELAWF	
C1111-8PLTELAWD	

C1101-4P
C1101-4PLTEP
C1101-4PLTEPWX

C1116-4P
C1116-4PLTEEA
C1116-4PWE
C1116-4PLTEEAWE

C1117-4P
C1117-4PLTEEA
C1117-4PLTELA
C1117-4PWE
C1117-4PWA
C1117-4PWZ

C1117-4PM
C1117-4PMLTEEA
C1117-4PMWE
C1117-4PLTEEAWE
C1117-4PLTEEAWA
C1117-4PLTELAWZ
C1117-4PMLTEEAWE

## System Requirements

The following are the minimum system requirements:



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

- Memory: 4GB DDR3 up to 16GB
- Hard Drive: 200GB or higher (Optional). (The hard drive is only required for running services such as Cisco ISR-WAAS.)
- Flash Storage: 4GB to 32GB



**Note** There is no change in the flash storage size from the earlier releases. The flash storage size must be equal to the system memory size.

- 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

## Installing a New Software Release

To install, obtain a Cisco IOS XE 16.x 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 need to first download the consolidated package and extract the individual sub-packages from a consolidated package.

For information about upgrading software, see the “Installing the Software” section in the Software Configuration Guide for the Cisco 1100 Series ISRs.

## Upgrading the ROMMON Version on the Cisco 1100 Series ISR

For information about ROMMON and upgrading procedure, see the "ROMMON Overview and Basic Procedures" section in the [Hardware Installation Guide for the Cisco 1100 Series Integrated Services Routers](#).

## 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.

## Using the Cisco Bug Search Tool

### About the Cisco Bug Search Tool

Use the [Cisco Bug Search Tool](#) to access open and resolved bugs for a release.

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

The screenshot shows the Cisco Bug Search Tool interface. At the top, there are buttons for 'Save Search', 'Load Saved Search', 'Clear Search', and 'Email Current Search'. Below this is a search bar labeled 'Search For:' with a text input field and a search icon. A callout box points to the search bar with the text 'If you have a specific bug ID, enter it here'. Below the search bar are three dropdown menus: 'Product:' with a 'Series/Model' dropdown, 'Releases:' with an 'Affecting or Fixed in these Release:' dropdown, and a 'Select from list' button. A callout box points to the 'Product:' dropdown with the text 'Start typing product name to view suggestions or expand list to choose your product'. Another callout box points to the 'Releases:' dropdown with the text 'Enter release number'. The number '368025' is visible in the bottom right corner of the screenshot.

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

Save Search Load Saved Search Clear Search Email Current Search

Search For:  Examples: CSCId10124, router crash, etc...

Product:  Series/Model  Select from list

Releases:  Affecting or Fixed in these Releat

Filter:  Modified Date:  Status:  Severity:  Rating:  Support Cases:  Bug Type:  Customer Visible

Viewing 1 - 25 of 132 results Sort by  Export Results to Excel

368026

## New Features and Important Notes for Cisco ISR 1000 Series, Cisco IOS XE Fuji 16.9.1

This section describes new features in Cisco IOS XE Fuji 16.9.1 that are supported on the Cisco 1000 Series ISRs

### New Hardware Features in Cisco 1100 Series ISR Release 16.9.1

There are no hardware features on Cisco 1100 Series Integrated Service Routers for the Cisco IOS XE Fuji 16.9.1 release:

### New Software Features in Cisco ISR 1000 Series, Cisco IOS XE Fuji 16.9.1

The following are the new software features introduced in Cisco 1000 Series Integrated Service Routers for Cisco IOS XE Fuji 16.9.1 release:

#### Application Awareness capability to ZBFW

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_zbf/configuration/xe-16-9/sec-data-zbf-xe-16-9-book/app-firewall-app-fw.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-16-9/sec-data-zbf-xe-16-9-book/app-firewall-app-fw.html)

#### Candidate Configuration

A temporary configuration that can be modified without changing running configuration. You can then choose when to update the device's configuration with the candidate configuration, by committing and confirming the candidate configuration.

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/169/b\\_169\\_programmability\\_cg/NETCONG\\_YANG.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/169/b_169_programmability_cg/NETCONG_YANG.html)

#### Cellular Profile Configuration

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/routers/access/1100/software/configuration/xe-16-9/cisco\\_1100\\_series\\_swcfg\\_xe\\_16\\_9\\_x.html](https://www.cisco.com/c/en/us/td/docs/routers/access/1100/software/configuration/xe-16-9/cisco_1100_series_swcfg_xe_16_9_x.html)

#### Setting Up Secure Device Provisioning for Enrollment in a PKI

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_pki/configuration/xc-16-9/sec-pki-xe-16-9-book/sec-pki-xe-16-8-book\\_chapter\\_01101.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xc-16-9/sec-pki-xe-16-9-book/sec-pki-xe-16-8-book_chapter_01101.html)

### **IOS-XE: IPSec VPN with DDNS**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_vpnav/configuration/xc-16-9/sec-vpn-availability-xe-16-9-book/sec-realtime-ipsec.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/xc-16-9/sec-vpn-availability-xe-16-9-book/sec-realtime-ipsec.html)

### **Runtime Defense: ASLR -kASLR**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mob\\_pmip6/configuration/xc-16-9/mob-pmip6-xe-16-9-book/imo-pmip6-multipath-support.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mob_pmip6/configuration/xc-16-9/mob-pmip6-xe-16-9-book/imo-pmip6-multipath-support.html)

### **VXLAN support on IOS-XE**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xc-16-9/ce-xe-16-9-book/ce-vxlan-support.html#ref\\_1060834](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xc-16-9/ce-xe-16-9-book/ce-vxlan-support.html#ref_1060834)

### **Web User Interface**

Supports an embedded Graphical User Interface based device-management tool that provides the ability to provision the device, simplifies device deployment and manageability, and enhances user experience. The following features are supported on Web User Interface:

- Day Zero Enhancement
- Open Shortest Path First (OSPF)
- Snort IPS Enhancement

## **Open and Resolved Caveats in Cisco IOS XE Fuji 16.9.x**

All open and resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

This section contains the following topics:

### **Resolved Caveats-Cisco IOS XE Fuji 16.9.8**

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvt53563</a>	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability
<a href="#">CSCvv12527</a>	Crash in SNMP Engine process while polling chassis id in LLDP
<a href="#">CSCvv78028</a>	Cisco IOS XE Software Zone-Based Policy Firewall ICMP and UDP Inspection Vulnerability
<a href="#">CSCvw25564</a>	Cisco IOS and IOS XE Software IKEv2 AutoReconnect Feature Denial of Service Vulnerability
<a href="#">CSCvx16081</a>	Cisco IOS XE Software H.323 Application Level Gateway Bypass Vulnerability

Caveat ID Number	Description
<a href="#">CSCvx37176</a>	Cisco IOS XE Software Rate Limiting Network Address Translation Denial of Service Vulnerability
<a href="#">CSCvx41294</a>	High CPU usage caused by TCP Timer process

## Open Caveats - Cisco IOS XE Fuji 16.9.8

There are no open caveats for this release.

## Resolved Caveats-Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
<a href="#">CSCuv97577</a>	Mishandling of dsmpSession pointer causes a crash
<a href="#">CSCvr50406</a>	Cisco IOS XE IOx GuestShell USB SSD Namespace Protection Privilege Escalation Vulnerability
<a href="#">CSCvr93458</a>	Hub router crashed when run test_mpol_policy_qos_policy_template testcase
<a href="#">CSCvt70639</a>	Device reload due to tunnel flapping
<a href="#">CSCvt74346</a>	Router may unexpectedly be reloaded when collecting data from the interface using telemetry/Netconf.
<a href="#">CSCvu19733</a>	Evaluation of CVE-2020-11868 for IOS
<a href="#">CSCvv02486</a>	Random MPLS-TE tunnels with explicit-path stay down after egress interface is bounced.
<a href="#">CSCvv26538</a>	Crash due to a NULL pointer while bringing down PPPoE sessions.
<a href="#">CSCvv51048</a>	Memory leak "AAA SESS ATTR"
<a href="#">CSCvv58056</a>	ACLs may be partially loaded into hardware resulting in unexpected drop or permit
<a href="#">CSCvv84345</a>	Cisco ASR 1000 Crash on configuring IP NAT inside source list under VRF
<a href="#">CSCvv88621</a>	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage
<a href="#">CSCvw06719</a>	"platform ipsec reassemble transit" tail-drops unencrypted IPv4 Fragments with specific payload
<a href="#">CSCvw11902</a>	Passive FTP doesn't work with NAT
<a href="#">CSCvw14836</a>	Cisco ISR router running 16.9.6 crashes authenticating crypto certificate
<a href="#">CSCvw34157</a>	APPNAV CFT Crashes
<a href="#">CSCvw48800</a>	unable to transfer 1500 byte IP packet when using BRI bundled Multilink

Caveat ID Number	Description
<a href="#">CSCvw56517</a>	LMR Unable to hear first seconds of audio
<a href="#">CSCvw57860</a>	Duplicate entries seen in MAC filter table.

## Open Caveats - Cisco IOS XE Fuji 16.9.7

Caveat ID Number	Description
<a href="#">CSCvm05934</a>	RSA Keysize > 2048 may cause crash
<a href="#">CSCvt66541</a>	DNAC Wolverine - Crypto PKI-CRL-IO_1 process crashed in crypto_send_pki_request,crypto_crl_io_proc
<a href="#">CSCvu57706</a>	CUBE fails to send calls with below error after updating IOS to 16.9.5 Error (Resource busy)
<a href="#">CSCvu65369</a>	Link auto-negotiation fails between Cisco 1111-4P ES-4 switch module and Meraki MX100
<a href="#">CSCvv36247</a>	Memory Leak in MallocLite / Crypto IKMP
<a href="#">CSCvw96723</a>	CP process crashed while I95 driver was adding an IPC response to the receive ring

## Resolved Caveats-Cisco IOS XE Fuji 16.9.6

Caveat ID Number	Description
<a href="#">CSCvh24730</a>	PfRv3: Crash while Printing the Same TCA Message
<a href="#">CSCvi22263</a>	Crash when IOS is adapting shaping with Adaptive QoS over DMVPN configured
<a href="#">CSCvi67613</a>	Protocol type for GRE header doesn't work consistently with "cts sgt inline" enable over auto-tunnel
<a href="#">CSCvm40582</a>	Crash when entering username with aaa common-criteria policy password
<a href="#">CSCvm82184</a>	Memory leak under Key Manager (keyman) process
<a href="#">CSCvn02456</a>	Router crashes when the calls doesn't establish after making 2 calls when we set "max-conn 2"
<a href="#">CSCvn33902</a>	CPU Spike seen due to "VTEMPLATE BKG OW Process" when disconnecting PPP users 100 session/sec rate
<a href="#">CSCvp46937</a>	Sync failure and hung calls observed on standby
<a href="#">CSCvp88044</a>	Performance Monitor crash
<a href="#">CSCvq39840</a>	CiscoFlashFile - Get-Next request takes longer time for last file on directory.



Caveat ID Number	Description
<a href="#">CSCvq43004</a>	Need to check qfp ucode crash with RTCP traffic - chunk memory corruption in RTCP path
<a href="#">CSCvr10592</a>	After putting caller on hold - caller call leg tx packets are increasing in CUBE
<a href="#">CSCvr28935</a>	IOS crash in DHCPd Receive with Unnumbered interfaces
<a href="#">CSCvr66463</a>	With CRL fetch failed, stuck at Failed to send the request. There is another request in progress
<a href="#">CSCvr75640</a>	LNS crash with Segmentation fault(11) in L2TP mgmt daemon
<a href="#">CSCvr76593</a>	Memory leak in CC-API_VCM and CCSIP_SPI_CONTROL
<a href="#">CSCvr89957</a>	CFT crashed frequently
<a href="#">CSCvs00961</a>	Memory leak under CCSIP_UDP_SOCKET / MallocLite
<a href="#">CSCvs04194</a>	Process = Exec crash seen on dmap longevity testbed with clear cry sa peer several times
<a href="#">CSCvs08368</a>	FlexVPN Hub Memory Leak in AAA process when IKEv2 sessions are being established
<a href="#">CSCvs12349</a>	NeMo tunnel is down after cellular interface config is overwritten
<a href="#">CSCvs28073</a>	IOS-XE device has memory leak in linux_iosd-imag
<a href="#">CSCvs29412</a>	x509 SSH authentication incorrect UPN value selected
<a href="#">CSCvs42075</a>	crash with shared-line command
<a href="#">CSCvs46847</a>	RTP/SRTP interworking fails when 180 and 183 have different to-tag
<a href="#">CSCvs70206</a>	CUBE DNS cache clear should be limited only to the matched connection id
<a href="#">CSCvs86573</a>	Connect message is never forwarded to the calling side
<a href="#">CSCvs92848</a>	Crash due to DHCP relay
<a href="#">CSCvt04814</a>	CPP crash due to a long QoS Policy and Class name
<a href="#">CSCvt05460</a>	IOS-XE: NAT not work for Active FTP
<a href="#">CSCvt06707</a>	C1111-LTE Observe data stalling after cellular interface has been loaded with data traffic for while
<a href="#">CSCvt08178</a>	CUBE crashes when SIP call is forked with active SIP KPML subscription
<a href="#">CSCvt10151</a>	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability UTD
<a href="#">CSCvt21373</a>	unexpected reload in CPP ucode forced by nat 514 .

Caveat ID Number	Description
<a href="#">CSCvt33018</a>	MACsec 128/256 XPN on 40g/100g, stop passing traffic for one of AN and interface link flap seen
<a href="#">CSCvt48480</a>	Flow monitor is removed from interface configuration on reload
<a href="#">CSCvt49705</a>	Device Crash observed with NAT and once there is traffic from outside
<a href="#">CSCvt51433</a>	Process sessmgrd crash due to clear radius sg-stats command.
<a href="#">CSCvt52825</a>	Memory leak in SCCP TLS Client on unexpected deregister event
<a href="#">CSCvt54305</a>	Device crashed after Boost license expire
<a href="#">CSCvt61876</a>	IOS-XE FW feature crashes while inspecting TCP packet with incorrect session packet state.
<a href="#">CSCvt65588</a>	FlexVPN IKEv2 Tunnel route removed after establishing new IKEv2 SA to another peer
<a href="#">CSCvt73592</a>	missing/corrupt IOS-XE PKSC10 format
<a href="#">CSCvt89337</a>	Incorrect Source IP when resolving DNS
<a href="#">CSCvt91720</a>	router see http wsma request as coming from 192.168.1.5
<a href="#">CSCvt99552</a>	CUBE/LGW: Certificate Unknown Error is observed when cn-san-validate server is configured
<a href="#">CSCvu01690</a>	CPUHOGS produced while executing the command - client fireall access-list ?
<a href="#">CSCvu04426</a>	ISR1K/4K reloads with erroneous reload cause code
<a href="#">CSCvu04665</a>	CUBE keeps sending REINVITES to peer legs leading to high CPU and eventually crashes.
<a href="#">CSCvu11115</a>	IOS-XE MTP Fails to Interwork DTMF RFC2833 from Payload 100 to Payload 101
<a href="#">CSCvu11993</a>	ZBFW drops selfzone generated packets from CPU to host with invalid reason in 16.12.x routers
<a href="#">CSCvu14823</a>	Crash on IOS-XE router when authenticating expired IPsec peer certificate
<a href="#">CSCvu20470</a>	Memory leak in STUN/MallocLite on ISRG2 CUBE/SIP GW routers leading to memory exhaustion over time.
<a href="#">CSCvu27953</a>	Crash due to a segmentation fault in the "IPsec background proc" process
<a href="#">CSCvu34009</a>	Calls going through T1 are rejected with "no dsps found" Analog/TDM Hairpin calls
<a href="#">CSCvu40093</a>	Crash when tearing down a PPPoE client session
<a href="#">CSCvu50302</a>	Survivability.tcl recovery procedure fails on Ingress GW of CCE call flow
<a href="#">CSCvu52218</a>	Router crashes frequently on NBAR

Caveat ID Number	Description
<a href="#">CSCvu87786</a>	CUBE Segmentation Fault @ sipSPIFreeOneSCB due to corrupt ccb
<a href="#">CSCvu92620</a>	Secure key agent memory leak in 16.9 and only in 16.9
<a href="#">CSCvv14026</a>	Unexpected Reload after running 'show voice dsp' command while an ISDN Call Disconnects

## Open Caveats - Cisco IOS XE Fuji 16.9.6

Caveat ID Number	Description
<a href="#">CSCvm94970</a>	[UniScale]Crash seen on csr1k during NAT44 hsl scale test when clearing max NAT translations
<a href="#">CSCvu16200</a>	Router May Crash When a SSH session is Closed After a TACACS Configuration Change (Part 2)
<a href="#">CSCvu35559</a>	Memory corruption crash when device is booting up
<a href="#">CSCvu57706</a>	CUBE fails to send calls with below error after updating IOS to 16.9.5 Error (Resource busy)
<a href="#">CSCvv21125</a>	Interface qlimit size decreases causing output / tail drops
<a href="#">CSCvv26538</a>	Crash due to a NULL pointer while bringing down PPPoE sessions.

## Resolved Caveats-Cisco IOS XE Fuji 16.9.5

Caveat ID Number	Description
<a href="#">CSCts28315</a>	DHCP-pd reflect the Advertised prefix in Request message
<a href="#">CSCvm40582</a>	Crash when entering username with aaa common-criteria policy password
<a href="#">CSCua95810</a>	IOS PKI: trustpoint doesn't rollover regenerated RSA keys.
<a href="#">CSCvh57657</a>	NAT MIB not populated when using traditional NAT
<a href="#">CSCvj00317</a>	Memory leak VOIP *MallocLite*
<a href="#">CSCvj29514</a>	CME: Toll fraud app not automatically trusting traffic from phones
<a href="#">CSCvj72294</a>	memory leak @ CCSIP_SPI_CONTR
<a href="#">CSCvk37212</a>	vEWLC:High amount of wncd memory leaks observed@crypto_encrypt_data_params_create_internal on scale
<a href="#">CSCvm25921</a>	Signaling interface inactive on "show snmp mib ifmib ifindex de" on IOS 16.6.3
<a href="#">CSCvn76837</a>	DMVPN Phase 2 shortcut triggered from a spoke behind PAT may end up in stuck DNX state

Caveat ID Number	Description
<a href="#">CSCvp27139</a>	Async lines configuration is not retrievable over netconf
<a href="#">CSCvp31779</a>	Router Running IOS-XE 16 Crashes when Stopping EPC with ACL
<a href="#">CSCvp47723</a>	ISR4K CME no way audio on calls across E1/PRI, reboot resolves for sometime
<a href="#">CSCvp68166</a>	CDETS to follow up fix "P-bit Sev Err Secs" increasing in patterns of 256 in SM-X-1T3/E3 in ISR4451
<a href="#">CSCvp69393</a>	Router crashes after snmpget to OID related to NHRP
<a href="#">CSCvp72039</a>	Ucode crash in infra with injected jumbo packet
<a href="#">CSCvp81958</a>	BGL18 Alpha: Cat9x00 hitting "No connections to Shell Manager available for processing the command"
<a href="#">CSCvp93108</a>	ISR4k Crash seen in skinny_unreserve_xcode_stream on 16.9
<a href="#">CSCvp94050</a>	cpp_bqs_srt_yoda_csr_tree_seid_initialize:1744 is not in "placed" state
<a href="#">CSCvp95156</a>	Memory leak in linux_iosd when polling mabClientIndexTest mib.
<a href="#">CSCvq07419</a>	DMVPN - Loopback interface as Tunnel source; packet not hitting NAT when egressing DMVPN device
<a href="#">CSCvq08255</a>	Neptune: 10G link does not come up after reload with GE-T SFP inserted in FPGE SFP slot
<a href="#">CSCvq10660</a>	ASR1006-X: cpp_cp_svr: QFP0.0 CPP Driver LOCKDOWN encountered due to previous fatal error
<a href="#">CSCvq20936</a>	CUBE router crashed due to memory corruption in subscription control block
<a href="#">CSCvq25297</a>	BRI leased line can't come up automatically after remove/insert one side's cable
<a href="#">CSCvq29575</a>	Voice gateway crash due to segmentation fault in process CCSIP_DNS
<a href="#">CSCvq30306</a>	IOSXE: IOMD / TDL leak seen with tdl_response_xcode_stat_side_t
<a href="#">CSCvq31129</a>	AppNav: Optimization failed with Asymmetrical traffic, VRF, FNF and NBAR
<a href="#">CSCvq33004</a>	Account logon failing for both direct and indirect lite-session in 16.9.3
<a href="#">CSCvq33563</a>	AFW_application_process triggers a crash with voice conference
<a href="#">CSCvq41777</a>	CUBE ha crash of standby unit after call hold from video endpoint
<a href="#">CSCvq43550</a>	C1111-4P doesn't restart authentication for "clear authen session" if "authen open" the port
<a href="#">CSCvq44603</a>	ISR 4k Reloads Unexpectedly, Crashing in the "IP NAT Ager" Process
<a href="#">CSCvq49000</a>	Supervisor reloaded due to cpp_cp_svr process crashing

Caveat ID Number	Description
<a href="#">CSCvq57205</a>	Recording failures with XMF media forking and SIP preservation timer
<a href="#">CSCvq58144</a>	cpp_cp_svr crash in cpp_bqs_rm_yoda_select_sch_exponent
<a href="#">CSCvq58237</a>	Supervisor reload due to cpp_cp_svr crash.
<a href="#">CSCvq61590</a>	ESP reload due to cpp_cp_svr exception at cpp_bqs_exponent_cnt_validate
<a href="#">CSCvq65366</a>	Cube might crash when sending a SIP message over TLS
<a href="#">CSCvq71094</a>	Core seen in ISR when removing the service-insertion config and committing it back
<a href="#">CSCvq71864</a>	Crash after executing "show archive config differences"
<a href="#">CSCvq72298</a>	Router crashed on running show policy-map interface <> output command
<a href="#">CSCvq74418</a>	connectivity is broken on ingress-replication L2DP/VXLAN
<a href="#">CSCvq80928</a>	CME/BE4K SNR: Crash when config changes are made while SNR call is active
<a href="#">CSCvq81620</a>	Router crashes with ZBF HA sync.
<a href="#">CSCvq85556</a>	QoS configuration download failed when device reloading
<a href="#">CSCvq90361</a>	NHRP process crash on using same tunnel address on multiple spokes
<a href="#">CSCvq97906</a>	"DHCPD Receive" process crash
<a href="#">CSCvq98999</a>	ISR4451-X / 16.09.01 / Crash when IPSEC SA installation fails
<a href="#">CSCvq99498</a>	Crashes when trying to bring-up / bring-down IPsec crypto session for OSPFv3
<a href="#">CSCvr00983</a>	Unrecoverable Error with PVDM in 0/4 and Thule+dreamliner in 1/0 on ISR4300
<a href="#">CSCvr01327</a>	incorrect Total number of translations on show ip nat translations
<a href="#">CSCvr01454</a>	Punt fragment crash when receive EoGRE packets which have many fragments
<a href="#">CSCvr05213</a>	Smart licensing PID and SN logs filling up the IOSRP tracelogs
<a href="#">CSCvr06666</a>	ISR4K Router CPP ucode Crash due IPv4 Fragmented packets
<a href="#">CSCvr12455</a>	KPML dialing fails after CSCvq20936 commit
<a href="#">CSCvr13213</a>	Session unauthorized as Redirect ACL Failure. Failed attribute name POSTURE_REDIRECT.
<a href="#">CSCvr17169</a>	qfp ucode crash with media monitor
<a href="#">CSCvr17670</a>	ISR G3, ASR1K crash after VoIP AAA test
<a href="#">CSCvr24316</a>	Router crashes due to Segmentation Fault when 'ccb' gives a NULL Pointer
<a href="#">CSCvr26524</a>	Crash due to NBAR classification

Caveat ID Number	Description
<a href="#">CSCvr27777</a>	ASR1k - Egress byte count is inaccurate
<a href="#">CSCvr33415</a>	Router may crash unexpectedly with Segmentation fault(11), Process = DSMP
<a href="#">CSCvr42310</a>	Removing and adding ACL to ASR1K is causing Tracebacks and download to DP failed errors
<a href="#">CSCvr48349</a>	ESP ucode crashed when running NAT with bpa (CGN)
<a href="#">CSCvr51860</a>	Observed Traceback with SRTP-RTP call after hold/resume
<a href="#">CSCvr58230</a>	While signalling forking the CUBE is not Sending Re-INVITE for T.38 with the Authorized header.
<a href="#">CSCvr58352</a>	Prince: Keepalive pkts dropped when serial link congested with data traffic
<a href="#">CSCvr66754</a>	CME-ISR4K: BLF working Inconsistently on 16.09.03 [Bad code fix was done in CSCvk49797]
<a href="#">CSCvr76534</a>	ISR4k : Crash seen at Process Exec
<a href="#">CSCvr80706</a>	ASR1006 tunnels are flapping CPP crash
<a href="#">CSCvr90926</a>	CUBE is updating the resolved IP only after the REGISTER expires
<a href="#">CSCvr96597</a>	IOS-XE crash after doing a SCEP enrollment
<a href="#">CSCvr99034</a>	ISR 4K router crash during updating the OpenDNS bypass whitelist
<a href="#">CSCvs13960</a>	IWAN High CPU and Memory
<a href="#">CSCvs29535</a>	IWAN crash related to DCA channel
<a href="#">CSCvs47682</a>	Router crashed on removing trustpoint on dspfarm profile

## Open Caveats - Cisco IOS XE Fuji 16.9.5

Caveat ID Number	Description
<a href="#">CSCve89377</a>	RFGW-10 Sup Moka CRC Causes Slot 3-10 Linecard Restarts
<a href="#">CSCvm94970</a>	[UniScale]Crash seen on csr1k during NAT44 hsl scale test when clearing max NAT translations
<a href="#">CSCvn02456</a>	Router crashes when the calls doesn't establish after making 2 calls when we set "max-conn 2"
<a href="#">CSCvp45666</a>	Kernel crash in netfilter
<a href="#">CSCvq84990</a>	Remove show ip/ipv6 access-list from syncfd-<ewlc-SIT>17.1-Observed Traceback followed by IOSD crash
<a href="#">CSCvq91046</a>	ASR1k crash in NAT code when processing PPTP traffic

Caveat ID Number	Description
<a href="#">CSCvq93850</a>	Passive FTP will fail when going over NAT and either client or server are off a SM-X-ES3
<a href="#">CSCvr28935</a>	IOS crash in DHCPd Receive with Unnumbered interfaces
<a href="#">CSCvr75640</a>	LNS crash with Segmentation fault(11) in L2TP mgmt daemon
<a href="#">CSCvr76593</a>	Memory leak in CC-API_VCM and CCSIP_SPI_CONTROL
<a href="#">CSCvs00961</a>	Memory leak under CCSIP_UDP_SOCKET / MallocLite
<a href="#">CSCvs04194</a>	Process = Exec crash seen on dmap longevity testbed with clear cry sa peer several times
<a href="#">CSCvs10497</a>	cpp_cp_svr fast memory leak when nbar custom protocol is configured
<a href="#">CSCvs60195</a>	ASR1K ucode crash after too many locks in ZBF pair setup

## Resolved Caveats-Cisco IOS XE Fuji 16.9.4

Caveat ID Number	Description
<a href="#">CSCvg29037</a>	Traceback is observed during mid-call media IP and port change
<a href="#">CSCvk20560</a>	491 not sent in a multiple re-invites in DO2EO scenario
<a href="#">CSCvk62792</a>	IKE Fragmentation payload incorrectly marked as critical
<a href="#">CSCvm01420</a>	CUBE crashes at sipSPI_ipip_vcc_CheckCodecSetType
<a href="#">CSCvm19399</a>	CRL file is getting overwritten when PKI server turns up after reload
<a href="#">CSCvm39894</a>	False authorizations and authentications even without radius server for dot1x/mab
<a href="#">CSCvm42441</a>	Router crash when clearing ip nat translations
<a href="#">CSCvm45068</a>	IOS CUBE Ent does not show 'media anti-trombone' in configuration
<a href="#">CSCvm51112</a>	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys
<a href="#">CSCvm58960</a>	"VoIP dial-Peer <XX> is Busied out" printed in log every 2 minutes when destination is not reachable
<a href="#">CSCvm61279</a>	Crash under AFW_application_process with shared-line configuration
<a href="#">CSCvm62419</a>	Crash at CCB of RTPSPI at the moment of creating a disconnect timer
<a href="#">CSCvm65384</a>	SNMP PKI trap are generated with wrong OID of 6999 instead of 854 per OID assignment
<a href="#">CSCvm74894</a>	PKI authentication should proceed even if GetCACaps return any http failure
<a href="#">CSCvm76295</a>	[SAP] syncfd fails to start on reload after upgrade to new ES image

Caveat ID Number	Description
<a href="#">CSCvm76452</a>	IPSec background crash while sending SNMP trap
<a href="#">CSCvm76590</a>	CUBE doesn't forward 200 OK in SRTP-RTP scenario with TCL script on Dial-peer
<a href="#">CSCvm86397</a>	CUBE: Crash observed at rbuf_ooh_handler
<a href="#">CSCvm92019</a>	Media Ant-Trombone does not properly handle a Re-Invite utilizing a Replaces Header
<a href="#">CSCvm92061</a>	ISR1K Fails to Send Multicast Traffic When Also Receiving The Same Group From a Non-direct Source
<a href="#">CSCvm93603</a>	IP change on dialer-int does not trigger a correct "local crypto entpt" in DMVPN
<a href="#">CSCvm94112</a>	DSM-3-INTERNAL: Internal Error : No DSM handle provided traceback on TDM voice gateway
<a href="#">CSCvm94788</a>	Device reloads when applying #client <IP> vrf Mgmt-vrf server-key 062B0C09586D590B5656390E15
<a href="#">CSCvm94891</a>	Crash caused by a "TLB Modification exception" after processing a null chunk in "IP Input" process.
<a href="#">CSCvm99036</a>	CUBE Crash in CCSIP_SPI_CONTROL process
<a href="#">CSCvm99045</a>	IOS-XE PKI: Certificate with 4 dashes imported in trustpool gets lost after reboot
<a href="#">CSCvn00218</a>	CUBE Crash in sipSPIAppAddCallInfoUI
<a href="#">CSCvn01681</a>	IPv6 To/From headers malformed with TCL IVR Script and header-passing
<a href="#">CSCvn07614</a>	Out of Band DTMF Events Not Passing to CUCM via SCCP When Using IOS MTP
<a href="#">CSCvn14737</a>	Crash with SIP call
<a href="#">CSCvn15588</a>	loss of two way audio with Skinny Phone, Line instance does not work until the next reboot.
<a href="#">CSCvn18500</a>	Certificate map does not work always with UPN in SAN field
<a href="#">CSCvn18790</a>	Cube crash with %SDP-3-SDP_PTR_ERROR
<a href="#">CSCvn27497</a>	ISR1k ping fails with MTU value 1560
<a href="#">CSCvn33961</a>	SSRC-field in RTCP gets changes to 0 when going through TRP present in the media path.
<a href="#">CSCvn36359</a>	CUBE doesn't forward INVITE with "midcal-signalling passthru media-change" during a video escalation
<a href="#">CSCvn41467</a>	Recommit of CSCvm99778 - eca/ewlc/qwlc/mewlc Sanity : AP join failed.
<a href="#">CSCvn47534</a>	RTP/SRTP interworking fails when 18x w/o SDP is before 183 w/SDP
<a href="#">CSCvn53969</a>	Memory leak in SMD process due to AAA Idle-timer not being freed



Caveat ID Number	Description
<a href="#">CSCvn64296</a>	Crash when making an external call
<a href="#">CSCvn64397</a>	Incorrect syntax in CRL download URL cause crash
<a href="#">CSCvn67837</a>	TCP port takes 4 minutes to get released after it is closed
<a href="#">CSCvn71041</a>	TACACS group server is not seen, when "transport-map type console test" is configured.
<a href="#">CSCvn78349</a>	FlexVPN with password encryption - keyring aaa LIST password 6 xxxxx encrypted again upon reload
<a href="#">CSCvq60252</a>	PBR works although an interface is down.
<a href="#">CSCvn78961</a>	Subscribers cannot re-login due to CoA time-out (lite-sessions in routed mode)
<a href="#">CSCvo00968</a>	Radius attr 32 NAS-IDENTIFIIER not sending the FQDN.
<a href="#">CSCvo15141</a>	CLI "nat force-on" in voice service voip not working as expected

## Open Caveats - Cisco IOS XE Fuji 16.9.4

Caveat ID Number	Description
<a href="#">CSCvh59431</a>	Byte counters for physical interface and subinterface don't match
<a href="#">CSCvj00317</a>	Memory leak VOIP *MallocLite*
<a href="#">CSCvk39056</a>	memleak_detect script errors "can't use floating-point value as operand of -"
<a href="#">CSCvn76837</a>	DMVPN Phase 2 shortcut triggered from a spoke behind PAT may end up in stuck DNX state
<a href="#">CSCvp45666</a>	Kernel crash in netfilter
<a href="#">CSCvp65151</a>	CPP Stuck thread when processing IPv6 traffic
<a href="#">CSCvp69393</a>	Router crashes after snmpget to OID related to NHRP
<a href="#">CSCvq25297</a>	BRI leased line can't come up automatically after remove/insert one side's cable
<a href="#">CSCvq26821</a>	shaper of the internal crypto interface is incorrectly programmed
<a href="#">CSCvq30306</a>	IOSXE: IOMD / TDL leak seen with tdl_response_xcode_stat_side_t
<a href="#">CSCvq31129</a>	AppNav: Optimization failed with Asymmetrical traffic, VRF, FNF and NBAR
<a href="#">CSCvq31871</a>	Router crashes with ZBF HA sync.
<a href="#">CSCvq43004</a>	Need to check qfp ucode crash with RTCP traffic - chunk memory corruption in RTCP path
<a href="#">CSCvq50202</a>	Class-attributes duplicated after EAP reauthen. in ISG radius proxy scenario

Caveat ID Number	Description
<a href="#">CSCvq57862</a>	cable-detect command not reflecting proper status in Analog ports on IOS-XE platforms
<a href="#">CSCvq57996</a>	RADIUS attribute 4 (NAS-IP-Address) is not honored
<a href="#">CSCvq58144</a>	cpp_cp_svr crash in cpp_bqs_rm_yoda_select_sch_exponent
<a href="#">CSCvq67003</a>	CPP microcode core file generated due to HW interrupt
<a href="#">CSCvq71864</a>	Crash after executing "show archive config differences"
<a href="#">CSCvq72298</a>	Router crashed on running show policy-map interface <> output command
<a href="#">CSCvq73575</a>	TCP traceroute - response ICMP TTL exceeded packet dropped by ZBFW with NAT enabled
<a href="#">CSCvq74418</a>	connectivity is broken on ingress-replication L2DP/VXLAN
<a href="#">CSCvq75610</a>	IWAN router crash after upgrading to 16.3.8
<a href="#">CSCvq78529</a>	IOSd Segmentation Fault on CTS enabled SDA fabric-edge switch stack
<a href="#">CSCvq81620</a>	Router crashes with ZBF HA sync.
<a href="#">CSCvq85329</a>	NEAT/CISP:authenticate SVI interface for Supplicant switch in NEAT port when spanning-tree disabled
<a href="#">CSCvq85913</a>	FlexVPN with password encryption -- after MasterKey change password in profile is not working
<a href="#">CSCvq87063</a>	getvpn suiteb:KS sends delete payload to gm's while scheduled rekey after primary KS dead/readdd
<a href="#">CSCvq90361</a>	NHRP process crash on using same tunnel address on multiple spokes
<a href="#">CSCvq91789</a>	When issuing ip helper-addresss x.x.x.x command, "sh run" and "sh run all" show differently
<a href="#">CSCvq93830</a>	IOS XE: RSA Keys randomly getting wiped out after rebooting
<a href="#">CSCvq94679</a>	[SDA] Crash due to Segmentation fault(11), Process = ARP Input
<a href="#">CSCvq95517</a>	Segmentation Fault in IP RIB Update following Virtual-Access Interface flap
<a href="#">CSCvq95756</a>	IPSec SA creation failure causes crash in fman-fp-image
<a href="#">CSCvq97365</a>	2 interfaces of client in different vrf connected to same vlan of server not able to get ip via dhcp
<a href="#">CSCvq97906</a>	"DHCPD Receive" process crash
<a href="#">CSCvq98095</a>	Gi0/0/0 interface stays up/up and LED green after cable removed

## Resolved Caveats-Cisco IOS XE Fuji 16.9.3

Caveat ID Number	Description
<a href="#">CSCvg29037</a>	Traceback is observed during mid-call media IP and port change
<a href="#">CSCvk20560</a>	491 not sent in a multiple re-invites in DO2EO scenario
<a href="#">CSCvk62792</a>	IKE Fragmentation payload incorrectly marked as critical
<a href="#">CSCvm01420</a>	CUBE crashes at sipSPI_ipip_vcc_CheckCodecSetType
<a href="#">CSCvm19399</a>	CRL file is getting overwritten when PKI server turns up after reload
<a href="#">CSCvm39894</a>	False authorizations and authentications even without radius server for dot1x/mab
<a href="#">CSCvm42441</a>	Router crash when clearing ip nat translations
<a href="#">CSCvm45068</a>	IOS CUBE Ent does not show 'media anti-trombone' in configuration
<a href="#">CSCvm51112</a>	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys
<a href="#">CSCvm58960</a>	"VoIP dial-Peer <XX> is Busied out" printed in log every 2 minutes when destination is not reachable
<a href="#">CSCvm61279</a>	Crash under AFW_application_process with shared-line configuration
<a href="#">CSCvm62419</a>	Crash at CCB of RTPSPI at the moment of creating a disconnect timer
<a href="#">CSCvm65384</a>	SNMP PKI trap are generated with wrong OID of 6999 instead of 854 per OID assignment
<a href="#">CSCvm74894</a>	PKI authentication should proceed even if GetCACaps return any http failure
<a href="#">CSCvm76295</a>	[SAP] syncfd fails to start on reload after upgrade to new ES image
<a href="#">CSCvm76452</a>	IPSec background crash while sending SNMP trap
<a href="#">CSCvm76590</a>	CUBE doesn't forward 200 OK in SRTP-RTP scenario with TCL script on Dial-peer
<a href="#">CSCvm86397</a>	CUBE: Crash observed at rbuf_ooh_handler
<a href="#">CSCvm92019</a>	Media Ant-Trombone does not properly handle a Re-Invite utilizing a Replaces Header
<a href="#">CSCvm92061</a>	ISR1K Fails to Send Multicast Traffic When Also Receiving The Same Group From a Non-direct Source
<a href="#">CSCvm93603</a>	IP change on dialer-int does not trigger a correct "local cryto entpt" in DMVPN
<a href="#">CSCvm94112</a>	DSM-3-INTERNAL: Internal Error : No DSM handle provided traceback on TDM voice gateway
<a href="#">CSCvm94788</a>	Device reloads when applying #client <IP> vrf Mgmt-vrf server-key 062B0C09586D590B5656390E15

Caveat ID Number	Description
<a href="#">CSCvm94891</a>	Crash caused by a "TLB Modification exception" after processing a null chunk in "IP Input" process.
<a href="#">CSCvm99036</a>	CUBE Crash in CCSIP_SPI_CONTROL process
<a href="#">CSCvm99045</a>	IOS-XE PKI: Certificate with 4 dashes imported in trustpool gets lost after reboot
<a href="#">CSCvn00218</a>	CUBE Crash in sipSPIAppAddCallInfoUI
<a href="#">CSCvn01681</a>	IPv6 To/From headers malformed with TCL IVR Script and header-passing
<a href="#">CSCvn07614</a>	Out of Band DTMF Events Not Passing to CUCM via SCCP When Using IOS MTP
<a href="#">CSCvn14737</a>	Crash with SIP call
<a href="#">CSCvn15588</a>	loss of two way audio with Skinny Phone, Line instance does not work until the next reboot.
<a href="#">CSCvn18500</a>	Certificate map does not work always with UPN in SAN field
<a href="#">CSCvn18790</a>	Cube crash with %SDP-3-SDP_PTR_ERROR
<a href="#">CSCvn27497</a>	ISR1k ping fails with MTU value 1560
<a href="#">CSCvn33961</a>	SSRC-field in RTCP gets changes to 0 when going through TRP present in the media path.
<a href="#">CSCvn36359</a>	CUBE doesn't forward INVITE with "midcal-signalling passthru media-change" during a video escalation
<a href="#">CSCvn41467</a>	Recommit of CSCvm99778 - eca/ewlc/qwlc/mewlc Sanity : AP join failed.
<a href="#">CSCvn47534</a>	RTP/SRTP interworking fails when 18x w/o SDP is before 183 w/SDP
<a href="#">CSCvn53969</a>	Memory leak in SMD process due to AAA Idle-timer not being freed
<a href="#">CSCvn64296</a>	Crash when making an external call
<a href="#">CSCvn64397</a>	Incorrect syntax in CRL download URL cause crash
<a href="#">CSCvn67837</a>	TCP port takes 4 minutes to get released after it is closed
<a href="#">CSCvn71041</a>	TACACS group server is not seen, when "transport-map type console test" is configured.
<a href="#">CSCvn78349</a>	FlexVPN with password encryption - keyring aaa LIST password 6 xxxxx encrypted again upon reload
<a href="#">CSCvn78961</a>	Subscribers cannot re-login due to CoA time-out (lite-sessions in routed mode)
<a href="#">CSCvo00968</a>	Radius attr 32 NAS-IDENTIFIIER not sending the FQDN.
<a href="#">CSCvo15141</a>	CLI "nat force-on" in voice service voip not working as expected

## Open Caveats - Cisco IOS XE Fuji 16.9.3

Caveat ID Number	Description
<a href="#">CSCvn56017</a>	Crash while processing ISIS updates when DiffServ-TE is enabled
<a href="#">CSCvn78203</a>	Router crashed when printing logs while constructing rekey packets (GETVPN)
<a href="#">CSCvo18177</a>	IPV4 routes on the global routing table learnt via BGP refreshes upon adding or removing a VRF
<a href="#">CSCvo24170</a>	Crash due to chunk corruption in ISIS code
<a href="#">CSCvo35606</a>	Dialer interface shutdown caused crash of router.
<a href="#">CSCvo36188</a>	Crash at NAT clear
<a href="#">CSCvo62122</a>	IOS-XE Router may crash when attempting to Fragment Corrupted IPv4 Packet
<a href="#">CSCvo62584</a>	DHCP discover packets were being dropped at firewall since UDP source port as 0.

## Resolved Caveats-Cisco IOS XE Fuji 16.9.2

Caveat ID Number	Description
<a href="#">CSCvj69654</a>	OSPF originates default route without "default-information originate"
<a href="#">CSCvj73544</a>	OSPF routing loop for external route with multiple VLINKs/ABRs
<a href="#">CSCvj92862</a>	Viptela-netconf returns 255 length byte-stream chars instead of actual length for OSPFV2 Key-string
<a href="#">CSCvj95351</a>	OSPF SR uloop : After issuing "clear ip ospf process". ospf process crashed
<a href="#">CSCvk00446</a>	BGP high CPU when config 256k vxlan static route
<a href="#">CSCvk10633</a>	BGP crash while running show command and same time bgp peer reset
<a href="#">CSCvk52512</a>	C1100 router stops forwarding traffic when doing bulk configurations on device via telnet
<a href="#">CSCvk35032</a>	TSN: Maximum HSRP Groups on FPGE interface not match the HW capability
<a href="#">CSCvj74614</a>	ISR1111-4P Ping issue between LAN inetrface and directly connected switch
<a href="#">CSCvm06270</a>	ICMP unreachables are not sent to the client on C1117 platform

## Open Caveats - Cisco IOS XE Fuji 16.9.2

Caveat ID Number	Description
<a href="#">CSCvm99745</a>	Can't configure multiple CFM IP SLA with the same source MEP on ISR1k

Caveat ID Number	Description
<a href="#">CSCvm92061</a>	ISR1K Fails to Send Multicast Traffic When Also Receiving The Same Group From a Non-direct Source
<a href="#">CSCvj12370</a>	cpp_cp_svr crash in bqs while running QMRT test tool
<a href="#">CSCvk59169</a>	Strict SID has NOT been enabled in ISIS segment-routing
<a href="#">CSCvm52543</a>	Subscriber session hangs after the upgrade and reload
<a href="#">CSCvm78822</a>	<b>config-sync failure aaa</b> authorization commands
<a href="#">CSCvn02047</a>	Configuring more than 5k NAT entries cause high CPU utilization even with no traffic

## Resolved Caveats - Cisco IOS XE Fuji 16.9.1

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Caveat ID Number	Description
<a href="#">CSCvf34608</a>	Excessive Reflector Tracelogs
<a href="#">CSCvh66642</a>	uIDB leaks at the DMVPN hub if the route to remote NBMA is not learned
<a href="#">CSCvj70308</a>	C1111 Gi0/0/1 not passing packets when autoneg is disabled

## Open Caveats - Cisco IOS XE Fuji 16.9.1

Caveat ID Number	Description
<a href="#">CSCvj47652</a>	NIM-VAB-A: Configured in ADSL2+ mode brings up the ethernet interface.
<a href="#">CSCvj56758</a>	C1101-4PLTEP-EM74xx: No free dialer causes data call fails after another SIM slot is activated.
<a href="#">CSCvj71853</a>	<b>sdave_ppdk.pack force</b> command is not accepted during boot up
<a href="#">CSCvk12152</a>	Unable to remove the <b>ip nat inside destination</b> command.

