Cross Platform Release Notes for Cisco IOS Release 15.9(3)M

First Published: 2019-08-15

Last Modified: 2026-04-09

Cross Platform Release Notes for Cisco IOS Release 15.9(3)M

These release notes support Cisco IOS Release 15.9(3)M and describe new features and related documents.

Cisco IOS Release 15.9(3)M provides the latest innovations for the world's most demanding networks and is designed to provide a unified network architecture that is stable, reliable, and secure. New features are fully integrated with extensive capabilities already available in Cisco IOS software to provide solutions for enterprise, service provider, and smart grid.

System Requirements

This section describes the system requirements for Cisco IOS Release 15.9(3)M and includes the following sections:

Supported Hardware Platforms

- Cisco 800 and Cisco 800M series routers
- Cisco 900 series routers
- Cisco Analog Voice Gateways (VG202XM and VG204XM)
- Cisco Connected Grid Router (CGR) 2000 series (CGR 2010)
- Cisco Connected Grid Router (CGR) 1000 series (CGR1240,CGR1120)
- Cisco Industrial Integrated Services Routers IR8XX (809,829,807)

For more information about the platforms supported in Cisco IOS Release 15.9(3)M, see the "Platform-Specific Information" section.

Determining Your Software Version

To determine the version of Cisco IOS software that is currently running on your Cisco network device, log in to the device and enter the **show version** user EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software IOS (tm)
15.9 Software (c880data-universalk9-mz.), Version 15.9(3)M, RELEASE SOFTWARE
Upgrading to a new Release
MIBS
```

```
Field Notices and Software-Related Tools and Information
Troubleshooting
```

Upgrading to a New Release

For information about selecting a new Cisco IOS software release, see How to Choose a Cisco IOS Software Release at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml

For information about updating or upgrading Cisco IOS software, see *How to Update/Upgrade Cisco IOS Software* at the following URL:

http://www.cisco.com/en/US/prod/iosswrel/networking_solutions_products_genericcontent0900aecd806ea5be.html

Platform-specific documents may also provide information about upgrading to a new software release:

- Cisco 800 Series Industrial Integrated Services Routers: http://www-author.cisco.com/c/en/us/support/routers/800-series-industrial-routers/products-installation-guides-list.html
- Cisco 800 series routers:http://www.cisco.com/en/US/products/hw/routers/ps380/prod_installation_guides_list.html
- Cisco IR 800 series routers: https://www.cisco.com/c/en/us/support/routers/800-series-industrial-routers/products-installation-guides-list.html

  https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-9-3M-Release-Note.html
- Cisco 900 Integrated Services Routershttps://www.cisco.com/c/en/us/td/docs/routers/access/900/hardware/installation/guide/b-cisco-ISR900-series-hig.html
- Cisco 1000 CGR series routers http://www.cisco.com/c/en/us/support/routers/1000-series-connected-grid-routers/products-installation-and-configuration-guides-list.html

  https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-9-3M-Release-Note.html
- Cisco 2000 CGR series routers:https://www.cisco.com/site/us/en/products/networking/industrial-routers-gateways/2000-series-connected-grid/index.html

  https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-9-3M-Release-Note.html
- Cisco 2900 and 3900 series routers: https://www.cisco.com/c/en/us/td/docs/routers/access/2900/hardware/installation/guide/Hardware_Installation_Guide/Overview.html
- Cisco 5900 Embedded Services Routers: http://www.cisco.com/c/en/us/support/routers/5900-series-embedded-services-routers/products-installation-guides-list.html
- Cisco VG202XM and Cisco VG204XM Voice Gateways: https://www.cisco.com/c/en/us/products/collateral/unified-communications/vg-series-gateways/select-vg202xm-analog-voice-gateway-eol.html

For instructions on ordering a Cisco IOS upgrade, see the document at the following location: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.html.

To choose a new Cisco IOS software release by comparing feature support or memory requirements, use Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

To choose a new Cisco IOS software release based on information about defects that affect that software, use Bug Toolkit at the following URL: https://bst.cloudapps.cisco.com/bugsearch.

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

https://cfnng.cisco.com/mibs

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page .

https://www.cisco.com/c/en/us/support/web/tools/snmp/help/index.html?linkclickid=aisrch

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

Field Notices and Software-Related Tools and Information

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. You can find Field Notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Visit the Download Software page on Cisco.com to subscribe to Cisco software notifications, locate MIBs, access the Software Advisor, and find other Cisco software-related information and tools. Access the Download Software page at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm.

Troubleshooting

The following documents and websites provide assistance with troubleshooting your Cisco hardware and software:

- *Troubleshoot and Alerts* Product or Technology Selection Page

http://www.cisco.com/cisco/web/psa/troubleshoot.html?mode=prod&level0=268437899

- *Cisco 800 Series Routers Troubleshooting Guides*

https://www.cisco.com/c/en/us/support/routers/800-series-routers/products-troubleshooting-guides-list.html

- Cisco 1240 and 1120 Connected Grid Router Installation Guides

http://www.cisco.com/c/en/us/support/routers/1000-series-connected-grid-routers/products-installation-guides-list.html

- *Cisco 1600 Series Routers Hardware Troubleshooting Index Page*

https://www.cisco.com/c/en/us/obsolete/routers/cisco-1600-series-routers.html

- *Troubleshooting Cisco 3900 Series, 2900 Series, and 1900 Series ISRs*

https://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/oveview.html

- *Cisco Unified Communications 500 Series Install and Upgrade Tech Notes*

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-install-and-upgrade-technotes-list.html

Cisco Error Message Decoder

Refer to *Cisco System Messages*.

- Cisco Support Community

https://supportforums.cisco.com/index.jspa

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains specific Cisco IOS features.

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit [3DES] data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Cisco Feature Navigator

Feature-to-image mapping is available through Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). You can compare Cisco IOS software releases side-by-side to display both the features unique to each software release and the features that the releases have in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

www.cisco.com/go/cfn

For help with Cisco Feature Navigator, see the help information at the following URL:

http://www.cisco.com/web/applicat/CFNTOOLS/Help_Docs/help/cfn_support.html

Determining the Software Images (Feature Sets) That Support a Specific Feature

To determine which software images (feature sets) in a Cisco IOS release support a specific feature, go to the Cisco Feature Navigator home page and perform the following steps.

Procedure

Step 1 From the Cisco Feature Navigator home page, click **Research Features.**

Step 2 Select your software type or leave the field as "All".

Step 3 To find a feature, you can search by either Feature or Technology (select the appropriate button). If you select Search by Feature, you can further filter your search by using the Filter By text box.

Step 4 Choose a feature from the Available Features text box, and click the **Add** button to add the feature to the Selected Features text box.

Note
To learn more about a feature in the list, click the **View Desc** button in the Available Features text box.

Repeat this step to add features. A maximum of 20 features can be chosen for a single search.

Step 5 Click **Continue** when you are finished choosing features.

Step 6 In the Release/Platform Tree area, select either your release (from the Train-Release list) or your platform (from the Platform list).

Step 7 The "Search Result" table will list all the software images (feature sets) that support the features that you chose.

Note
You can download your results into an Excel spreadsheet by clicking on the **Download Excel** button.

Determining the Features Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set), go to the Cisco Feature Navigator home page and perform the following steps.

Procedure

Step 1 From the Cisco Feature Navigator home page, click **Research Software.**

Step 2 Select your software type from the drop-down list and chose the **Release** button in the "Search By" area.

Step 3 From the Major Release drop-down list, chose the appropriate major release.

Step 4 From the Release drop-down list, choose the appropriate maintenance release.

Step 5 From the Platform drop-down list, choose the appropriate hardware platform.

Step 6 From the Feature Set drop-down list, choose the appropriate feature set. The Image Details area will provide details on the specific image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.

Note
To learn more about a feature in the list, click the **View Desc** button in the Available Features text box.

Memory Recommendations

To determine memory recommendations for software images (feature sets) in your Cisco IOS release, go to the Cisco Feature Navigator home page and perform the following steps.

Procedure

Step 1 From the Cisco Feature Navigator home page, click **Research Software.**

Step 2 Select your software type from the drop-down list and choose the **Release** button in the "Search By" area.

Step 3 From the Major Release drop-down list, choose the appropriate major release.

Step 4 From the Release drop-down list, choose the appropriate maintenance release.

Step 5 From the Platform drop-down list, choose the appropriate hardware platform.

Step 6 From the Feature Set drop-down list, choose the appropriate feature set.

Step 7 The Image Details area will provide details on the specific image including the DRAM and flash memory recommendations for each image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.

Features and Important Notes

These release notes describe the following topics:

New and Changed Information

Important Notes

- Nested encryption is not supported on classic IOS devices.
- The H.323 functionality is not supported from Cisco IOS 15.7(3)M onwards. This might potentially have an impact on the NAT H.323 ALG functionality. Note that Cisco technical support will not be available for any NAT H.323 ALG issues related to this change. If you are impacted by this change, we recommend that you consider Session Initiation Protocol (SIP) as an alternative solution.

New Hardware Features Supported in Cisco IOS Release 15.9(3)M

There are no new hardware features supported in this release.

New Software Features Supported in Cisco IOS Release 15.9(3)M

There are no new software features supported in this release.

Bugs for Cisco IOS Release 15.9(3)M

Open and Resolved 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.

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

Using the Bug Search Tool

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

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.

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.

To use the Cisco Bug Search Tool:

1. In your browser, navigate to the Cisco Bug Search Tool.
2. If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.
3. To search for a specific bug, enter the bug ID in the Search For field and press Enter.
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. You can mouse over bugs to see more content about a specific bug.

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.
- 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 Bugs—Cisco IOS Release 15.9(3)M13

Identifier	Headline
CSCwq01495	Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 denial of service vulnerability.
CSCwq14981	Cisco IOS Software and IOS XE Software Release 3E HTTP Server denial of service vulnerability.

Open Bugs—Cisco IOS Release 15.9(3)M13

There are no open bugs for this release.

Resolved Bugs—Cisco IOS Release 15.9(3)M12

Identifier	Headline
CSCvi23158	The trustpoint feature now supports the acceptance of asymmetric certificates.
CSCwn83263	A denial of service vulnerability affecting IKEv2 has been identified in Cisco IOS and IOS XE Software on routers and devices.
CSCwp13843	Certain devices may experience dropped GRE/IPSec traffic under specific conditions.
CSCwo20388	Cisco IOS and IOS XE Software are affected by an IKEv2 denial of service vulnerability.
CSCwo49948	Cisco IOS and IOS XE Software are affected by an IKEv2 denial of service vulnerability.
CSCwq31287	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability.

Open Bugs—Cisco IOS Release 15.9(3)M12

There are no open bugs for this release.

Resolved Bugs—Cisco IOS Release 15.9(3)M11

Table 1: Resolved Bugs—Cisco IOS Release 15.9(3)M11

Caveat ID Number	Description
CSCwm79577	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwn01892	SVI (Vlan50) automatically loses **ip address dhcp** config on IR829 and will not recover.
CSCwn01409	Crashes in NAT64 Translation during IP Forwarding.
CSCwm79570	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm89600	Cisco IOS, IOS XE, and IOS XR SNMP Denial of Service Vulnerabilities.
CSCwm79554	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwo33553	The feature code for forward-to-voicemail on VG320 does not take affect.
CSCwm79590	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm56522	C921 may crash when sending multicast packets.
CSCwm79581	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm79596	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm79564	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities

Open Bugs—Cisco IOS Release 15.9(3)M11

There are no Open bugs for this release.

Resolved Bugs—Cisco IOS Release 15.9(3)M10

Table 2: Resolved Bugs—Cisco IOS Release 15.9(3)M10

Caveat ID Number	Description
CSCwh82831	c900: Unexpected reload while using telnet with NAT overload configured.
CSCwj71021	Porting SCADA fixes from IOS-XE to Classic IOS (IR8x9).
CSCwj79682	BBUs In CGR running 15.9(3)M5 showing 4 instead of 3 BBUs.
CSCwi83306	"tx-ring-limit 240" is configured as default when QOS is applied under an interface.
CSCwj79682	BBUs in CGR running 15.9(3)M5 showing 4 instead of 3 BBUs.
CSCwj29678	C888 VRRP IP address not reachable for some VRRP ID or backup.
CSCwe24431	Cisco IOS and IOS XE software SNMP extended named Access Control List bypass vulnerability.

Open Bugs—Cisco IOS Release 15.9(3)M10

Table 3: Open Bugs—Cisco IOS Release 15.9(3)M10

Caveat ID Number	Description
CSCwk79078	C921 dead memory leak on SSH process.
CSCwk97831	TACACS type 6 encrypted keys lost on bootup when AES key not configured.

Resolved Bugs—Cisco IOS Release 15.9(3)M9

Table 4: Resolved Bugs—Cisco IOS Release 15.9(3)M9

Caveat ID Number	Description
CSCwh93289	Traps are not sent when temperature returns to the normal range.
CSCwi31181	CWMP is unexpectedly triggering DHCP discovery on the router every CWMP process run.
CSCwd59564	Cellular modem is getting rebooted constantly.

Open Bugs—Cisco IOS Release 15.9(3)M9

Table 5: Open Bugs—Cisco IOS Release 15.9(3)M9

Caveat ID Number	Description
CSCwh82831	Unexpected reload while using telnet with NAT overload configured.
CSCwi83306	tx-ring-limit 240 is configured as default when QOS is applied under an interface.
CSCvq04828	VRF aware reverse DNS lookup is not working.

Resolved Bugs—Cisco IOS Release 15.9(3)M8

Caveat ID Number	Description
CSCwe30292	PnP reset will erase the BOOT variable if images present on flash:/managed/images.
CSCwf22363	IOS upgrade causes modem to reset resulting in a crash.
CSCwe50487	C900 crypto policer causes low TCP throughput over VPN.
CSCwf54264	BGP VPNv4 MPLS over DMVPN does not work - Address family VPNv4 unicast capability not accepted.
CSCwf42797	Ignition off-timer values gets auto changed to random values.

Open Bugs—Cisco IOS Release 15.9(3)M8

Caveat ID Number	Description
CSCvq04828	VRF aware reverse DNS lookup not working.
CSCvq13832	Whenever acct-terminate-cause is 24 the duplicate set of traffic counts is sent as 0.

Open Bugs—Cisco IOS Release 15.9(3)M7

Caveat ID Number	Description
CSCvq13832	Whenever Acct-terminate-cause is 24 the duplicate set of traffic counts is sent as 0.
CSCvq04828	VRF aware reverse DNS lookup not working.
CSCuv36677	IOS allows RC4-MD5 and RC4-SHA1 SSL ciphers to be negotiated by default.

Resolved Bugs—Cisco IOS Release 15.9(3)M7

Caveat ID Number	Description
CSCwc37142	CGR2010 crashes when issuing the command 'sh interface transceiver'.
CSCwd06936	Issue with automatic tcp-mss configuration based on negotiated MTU.
CSCwd00197	Persistently high CPU seen with IR809 upgrade with FND using patch option enabled.
CSCwc46811	C927 Controller going down when using port-tagging.
CSCwd66461	Nat outside local ip address disappears in "show ip arp" when pppoe reconnection.
CSCwc36325	IOS device crashes after issuing the command "logging persistent".
CSCwd59562	C927 drops packets with MTU size > 1500.
CSCwd58885	CGR2010 crashes when issuing the command 'sh interface transceiver' with port-channel.

Resolved Bugs—Cisco IOS Release 15.9(3)M6

Caveat ID Number	Description
CSCwc20845	CWMP : Port mapping does not add VRF name to NAT rule.
CSCwb62452	Low flash error when CGR has plenty of space.
CSCwb80986	DNS servers learned via DHCP with interface in VRF do not get associated with VRF.
CSCwb33442	Dialer callback cannot trigger on device.
CSCwa89746	Configure replace crashes device with unexpected exception to CPU.
CSCvz96346	Device- STP fails to register BPDU and block the ports creating broadcast storm.

Caveat ID Number	Description
CSCwb25340	SNMP OID for SINR giving wrong (static) value of zero
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCwa87878	Rollback (config replace) failed for non default line vty configurations on classic IOS device.
CSCvz92994	Lack of MAC address in inform event message.
CSCwc20006	Backoff algorithm not working as expected with dual stack for reject code 33.

Open Bugs—Cisco IOS Release 15.9(3)M6

Caveat ID Number	Description
CSCvz96346	Router STP fails to register BPDU and block the ports creating broadcast storm.
CSCvq04828	VRF aware reverse DNS lookup not working.
CSCwc36325	IOS device crashes after issuing the command logging persistent.
CSCwc46811	Device controller going down when using port-tagging.
CSCvw45714	Secret sent in clear-text via TACACS+ command accounting/authorization with algorithm hashing config.
CSCvq13832	Whenever acct-terminate-cause is 24 the duplicate set of traffic counts is sent as 0.

Resolved Bugs—Cisco IOS Release 15.9(3)M6

Caveat ID Number	Description
CSCwc20845	CWMP : Port mapping does not add VRF name to NAT rule.
CSCwb62452	Low flash error when CGR has plenty of space.
CSCwb80986	DNS servers learned via DHCP with interface in VRF do not get associated with VRF.
CSCwb33442	Dialer callback cannot trigger on device.
CSCwa89746	Configure replace crashes device with unexpected exception to CPU.
CSCvz96346	Device- STP fails to register BPDU and block the ports creating broadcast storm.
CSCwb25340	SNMP OID for SINR giving wrong (static) value of zero
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCwa87878	Rollback (config replace) failed for non default line vty configurations on classic IOS device.
CSCvz92994	Lack of MAC address in inform event message.

Caveat ID Number	Description
CSCwc20006	Backoff algorithm not working as expected with dual stack for reject code 33.

Open Bugs—Cisco IOS Release 15.9(3)M5

Caveat ID Number	Description
CSCvv63779	CCP shows loading or 404 Not Found when using IOS 15.9.3M2
CSCvw94711	UDP Checksum could not be disabled for IPV4 packets on ISR4000 routers
CSCvz96346	IR829- STP fails to register BPDU and block the ports creating broadcast storm
CSCvq04828	VRF aware reverse DNS lookup not working
CSCwa65765	CGR1120 port flaps seen
CSCvw16468	CUBE media issue with signaling forking for disable-early-media 180
CSCvw45714	Secret sent in clear-text via TACACS+ command accounting/authorization with algorithm hashing config
CSCvq13832	Whenever Acct-terminate-cause is 24 the duplicate set of traffic counts is sent as 0.
CSCuv36677	IOS allows RC4-MD5 and RC4-SHA1 SSL ciphers to be negotiated by default

Resolved Bugs—Cisco IOS Release 15.9(3)M5

Caveat ID Number	Description
CSCvz12150	Flow Record shows not configured even defined flow monitor
CSCvz84217	HSRP standby switch unable to reach the VIP
CSCvy87472	C921J-4P restart because of bus error
CSCwa52960	[IR829]: Disabling dot1x command “authentication port-control force-auth” there is no MAC learned
CSCvz84269	Incorrect temp from MCU causing false over temp alerts
CSCvx55126	C9K - Encrypted preshared key not set when configured through PnP service
CSCvy73411	during stateful ipsec failover, the standby node is crashing when becoming active
CSCwa22863	c900 Series 'storm-control shutdown' unexpectedly configured on the interface after "clear counters"
CSCvy98864	Crash due to DNS server

Open Bugs—Cisco IOS Release 15.9(3)M4

Caveat ID Number	Description
CSCuv36677	IOS allows RC4-MD5 and RC4-SHA1 SSL ciphers to be negotiated by default
CSCvj96950	NHRP should register network CIEs as part of registration
CSCvq04828	VRF aware reverse DNS lookup not working
CSCvq13832	Whenever Acct-terminate-cause is 24 the duplicate set of traffic counts is sent as 0
CSCvs56559	show crypto pki server shows wrong expire certificate date
CSCvv63779	CCP shows loading or 404 Not Found when using IOS 15.9.3M2
CSCvw16468	CUBE media issue with signaling forking for disable-early-media 180
CSCvw45714	Secret sent in clear-text via TACACS+ command accounting/authorization with algorithm hashing config
CSCvw94711	UDP Checksum could not be disabled for IPV4 packets on ISR4k routers
CSCvx62459	On C5921, tunnel MTU not getting dynamically changed as per PMTUD process
CSCvx89735	CISCO1921-SEC/K9 || Router crashing frequently
CSCvy60718	4G LTE: IPV6 profile is not active after a modem reset
CSCvy73411	during stateful ipsec failover, the standby node is crashing when becoming active
CSCvy87472	C921J-4P restart because of bus error
CSCvy91191	IOS Router cannot assign IP to Tunnel interface using DHCP Tunnel Support feature
CSCvy97399	Thinks registered but FND still thinks it is configuring. Fails config DL
CSCvz10552	Last reload reason: VDS communication failure

Resolved Bugs—Cisco IOS Release 15.9(3)M4

Caveat ID Number	Description
CSCuv97577	Mishandling of dsmpSession pointer causes a crash
CSCvg28350	Upon successful login, the network device must notify the administrator
CSCvq43731	Router running IOS might have a crash with EEM and QoS configuration
CSCvr04223	RootCA intermittently does not grant SubCA renewal request even with grant auto roll ca-cert
CSCvs45107	AnyConnect fails to reconnect when original session expires
CSCvu85572	Dynamic neighbor does not form when peer-group is shutdown in different vrf

Caveat ID Number	Description
CSCvv64633	BGP: advertised community list is malformed due to GSHUT community
CSCvw81805	WPAN interface missing
CSCvw82556	Router hangs and reload with reload reason: error - FPGA IOS watchdog timer expired
CSCvw84782	[CGR1K]: TAM/ACT2 Write Object Corruption (WPAN and IOS GTK keys mismatch)
CSCvw95836	C888 VRRP IP address not reachable for some VRRP ID
CSCvw97528	DNS info received via Cellular link in VRF goes into default DNS view instead VRF Specific DNS view
CSCvx08423	Log option cannot remove at 2nd time by override existing entry
CSCvx19503	[SHELL:] Rx side changes Tracking Bug for Commit
CSCvx21776	Cisco IOx Application Environment Path Traversal Vulnerability
CSCvx82752	Evaluation of all for OpenSSL March 2021 vulnerabilities
CSCvx85117	Communication by SVI does not recover even after the loop is resolved.
CSCvy34864	[CGR1K]: Status of ACTd component stuck in Deployed state
CSCvy44382	CGR 1xxx ciscoEnvMonSupplyState SNMP object returns Warning when DC supply is less than 12 volts
CSCvy91068	Port status looped as listening - learning - blocking with enabled STP on C921J router

Resolved Bugs—Cisco IOS Release 15.9(3)M3

Table 6: Resolved Bugs—Cisco IOS Release 15.9(3)M3

Caveat ID Number	Description
CSCvn71487	CUBE fails to send outgoing SUBSCRIBE if egress dial-peer has session server-group configured
CSCvn76365	VoIP Dial-peer up/down traps sent to SNMP server every interval
CSCvo15003	CUBE - SDP version increment behavior creates cypto interworking issues
CSCvq11134	SDP version was incremented due to misplace of PT 100
CSCvs06889	IOS router crashes with Crypto PAKs unavailable error from crypto engine
CSCvs39559	Reflexive ACL does not work on PATed packets in specific situation on IOS 15.7(3)M4a
CSCvs52160	MWI does not work for all shared lines

Caveat ID Number	Description
CSCvu73840	Unexpected reboot observed while trying to relay the digit to opposite leg
CSCvu78280	Traceback seen after show cellular on CGR
CSCvv08356	AP 860VAE-W GUI does not reflect changes in WLAN Configuration
CSCvv10404	After upgade to 15.9-3M1, GOS is using secondary IP on svcbr_0 for NAT
CSCvv14026	Unexpected Reload after running show voice dsp command while an ISDN Call Disconnects
CSCvv14078	Unexpected reload during a SIP call
CSCvv28615	15.2(7)E2: PnP process hangs after rollback triggered
CSCvv41229	RTP port leak
CSCvv48060	CUBE accepts SDP with invalid port number
CSCvv57896	Empty VoiceXML Property Value breaks Audio even when validating syntax success
CSCvv78486	Traceback: Unexpected reload after IOS Zone-based Firewall configuration
CSCvv86851	TACACS not working if TACACS group server has server-private <ip> key <passw> in 15.2(7)E3/3.11.3E
CSCvv92630	PKI http client fails to handle 1xx and 2xx responses
CSCvw15842	HSRP group id 11 can't create virtual MAC
CSCvw46822	Cisco 3900 ISR fails to reset ROC on receiving new SDP parameters in SRTP hold/resume after 15 minutes

Open Bugs—Cisco IOS Release 15.9(3)M3

Table 7: Open Bugs—Cisco IOS Release 15.9(3)M3

Caveat ID Number	Description
CSCuv36677	IOS allows RC4-MD5 and RC4-SHA1 SSL ciphers to be negotiated by default
CSCvj96950	NHRP should register network CIEs as part of registration
CSCvq04828	VRF aware reverse DNS lookup not working
CSCvq13832	Whenever Acct-terminate-cause is 24 the duplicate set of traffic counts is sent as 0
CSCvq43731	IR-829 h-QOS NULL pointer deference causing a crash
CSCvv63779	CCP shows loading or 404 Not Found when using IOS 15.9.3M3
CSCvv64633	BGP: advertised community list is malformed due to GSHUT community

Caveat ID Number	Description
CSCvw16468	CUBE media issue with signaling forking for "disable-early-media 180"
CSCvw32890	NAT stopped working with multicast
CSCvw39209	IR807: GPS module does not acquire coordinates after reload (instable state SWI)
CSCvw45714	Secret sent in clear-text via TACACS+ command accounting/authorization with algorithm hashing config
CSCvw82556	Router hangs and reload with reload reason: error - FPGA IOS watchdog timer expired
CSCvw84782	[CGR1K]: TAM/ACT2 Write Object Corruption (WPAN and IOS GTK keys mismatch)
CSCvw97528	DNS info received via Cellular link in VRF goes into default DNS view instead VRF Specific DNS view
CSCvx08423	Log option cannot remove at 2nd time by override existing entry
CSCvx08664	Login prompt comes up when try to telnet even if access denied by access-class
CSCvx08994	CTS credential password will be added to local keystore even if the password is longer than 24 char

Resolved Bugs—Cisco IOS Release 15.9(3)M2

Table 8: Resolved Bugs—Cisco IOS Release 15.9(3)M2

Caveat ID Number	Description
CSCul97065	5900 Series: Running config get cleared with random power cycles
CSCvd43539	NTP crash with empty peer list
CSCve47374	Mwheel Chunk leak
CSCvf69272	SNMP ENGINE high CPU usage observed with 1.3.6.1.2.1.185.1.1.1(mgmdHostInterfaceEntry)
CSCvg19259	MPLSoFlexVPN: Hub doesn't forward resolution req when default route is advertised to spokes
CSCvh24730	PfRv3: Crash while Printing the Same TCA Message
CSCvh92659	BFD flaps everytime with dynamic tunnel creation in DMVPN
CSCvm59977	DTMF renegotiation from RFC2833 to OOB does not work
CSCvm94891	Crash caused by a “TLB Modification exception” after processing a null chunk in “IP Input” process.
CSCvo42105	IOS-XE DHCP server creates option 125 with invalid format

Caveat ID Number	Description
CSCvo47866	Crash at Process = SCCP Auto Config
CSCvo50851	HTTP defaults to IPv6 even though IPv4 is also configured
CSCvp69393	Router crashes after snmpget to OID related to NHRP
CSCvp88044	Performance Monitor crash
CSCvq57205	Recording failures with XMF media forking and SIP preservation timer
CSCvq74033	Packet drop in vdsl controller pppoe stuck in PADISNT
CSCvq79177	Router reload due to command “show control-plane host open-ports”
CSCvr27393	Crash on “BGP Router” process
CSCvr61586	Cat4K sends RA with incorrect packet format
CSCvr97977	EIGRP hello packets sourced from the tunnel ip address even the EIGRP is not enabled on interface
CSCvs01516	IR829: “lte event rssi onset mib-trap” is not recognized
CSCvs08413	Reload when applying event manager policy to the router.
CSCvs27889	NAT address is deleted from route table after FTP passive mode communication
CSCvs40081	CUBE is not able to transfer the call
CSCvs46847	RTP/SRTP interworking fails when 180 and 183 have different to-tag
CSCvs47682	Router crashed when attempting to remove a nonexistent trustpoint from dspfarm profile
CSCvs67791	491 returned on midcall INVITE when peer leg is not pending a request
CSCvs99705	PKI CLI - no warning that rsakeypair name starting from 0 (zero) is not working for cert regenerate
CSCvt02534	ISR4K Unexpectedly Reboots with CENT-BR-0
CSCvt09605	CLI parser unexpectedly interprets backslash with octal numbers
CSCvt19077	AAA configurations are missing after reload.
CSCvt21259	IPV4 Multicast packets are unexpectedly replicated to underlay interface of mGRE tunnels
CSCvt25863	After firmware upgrade to version 15.9(3)M1 , AP is not booting
CSCvt46401	CUBE does not accept channel ID for MRCPv2
CSCvt49036	C800 with multiple ‘main’ regions do not successfully write all cores via ‘exception core-file’

Caveat ID Number	Description
CSCvt53256	C3900e platform running 15.7(3)M4b experienced a crash - previous bug CSCur96943
CSCvt62123	[C891F/15.9(3)M1] DMVPN after removing IPSec, packet drops continues at tunnel int
CSCvu13983	C927/C926 “show controller vdsl 0” hangs when MAC address is confogured on Eth 0 interface
CSCvu19733	Evaluation of CVE-2020-11868 for IOS
CSCvu19869	“Error in encoded data” is shown by ip nat command
CSCvu20470	Memory leak in STUN/MallocLite on ISRG2 CUBE/SIP GW routers leading to memory exhaustion over time.
CSCvu39805	C841-WIM-1T DTE does not raise RTS signal
CSCvu49754	Deleting a Voice Port on CUCM Shuts Down Additional Voice Ports on MGCP Gateway
CSCvu54635	SRTP key not updated to DSP on re-INVITE
CSCvu59071	I/O Memory Leak With Tunnel Config
CSCvu87814	FAC custom alias starting with #key stop working after IOS upgrade

Open Bugs—Cisco IOS Release 15.9(3)M2

Table 9: Open Bugs—Cisco IOS Release 15.9(3)M2

Caveat ID Number	Description
CSCuv36677	IOS allows RC4-MD5 and RC4-SHA1 SSL ciphers to be negotiated by default
CSCva36891	ISM-VPN: double counting of SNMP ifInOctets on sub-int with crypto map
CSCvn71487	CUBE fails to send outgoing SUBSCRIBE if egress dial-peer has "session server-group" configured
CSCvo15003	CUBE - SDP version increment behaviour creates cypto interworking issues
CSCvq04828	VRF aware reverse DNS lookup not working
CSCvq11134	SDP version was incremented due to misplace of PT 100
CSCvq13832	Whenever Acct-terminate-cause is 24 the duplicate set of traffic counts is sent as 0.
CSCvq43731	IR-829 Crashing with EEM Script Triggered
CSCvq62065	SIP phone paging party hears own voice
CSCvs06889	IOS router crashes with Crypto PAK's unavailable error from crypto engine.

Caveat ID Number	Description
CSCvs39559	Reflexive ACL does not work on PATed packets in specific situation on IOS 15.7(3)M4a.
CSCvs52160	MWI does not work for all shared lines
CSCvu73840	Crash observed while trying to relay the digit to opposite leg
CSCvu78280	Traceback seen after show celluar on CGR
CSCvu83051	WCCP ACL programming issue - denied traffic is redirected
CSCvv08356	AP 860VAE-W GUI doesn't reflect changes in WLAN Configuration.
CSCvv09009	Router is generating tracebacks after GM registration
CSCvv09517	[CGR1240] : The WIFI Interface Line State is Incorrect when compared to FSM Status
CSCvv10404	After upgade to 15.9-3M1, GOS is using secondary IP on svcbr_0 for NAT
CSCvv14078	Unexpected reload during a SIP call
CSCvu99875	Not able to boot 159-3.0o.M1 IOS on C867VAE-POE-W-A-K9 router

Resolved Bugs—Cisco IOS Release 15.9(3)M1

Table 10: Resolved Bugs—Cisco IOS Release 15.9(3)M1

Caveat ID Number	Description
CSCvd14310	IP TUNNELS: Overlapping Loopback Interface Causes Incorrect Forwarding Decision with AppNav and PfR
CSCvh09266	SNMP SMALL CHUN memory leak seen on KS while getvpn scale testing 300 group 4800 gm
CSCvh73576	config revert Rollback visible in console and locks up config from VTY
CSCvj00317	Memory leak VOIP *MallocLite*
CSCvj41876	Prefixes are stuck indefinitely in the BGP pending-prefixes list
CSCvj43156	Crash in XDR process: "fib_rp_table_broker_encode_buf.size <= FIB_RP_TABLE_BROKER_ENC_BUF_SZ"
CSCvm56592	CME/BE4K: Corrupted config file for Auto Registered IP Phones after reload
CSCvn55798	C897VAW-E-K9 // 15.7(3)M1 // Unable to disable lldp
CSCvn63087	Observing Memory leak at Sip MPA
CSCvn78113	Tunnel PMTUD not being aged out after PMTUD ager timer expires
CSCvn79227	QSIG - SIP - Connected Number Missing leading digit when decoding raw QSIG

Caveat ID Number	Description
CSCvn82489	CUBE changing the payload for content sharing packets, though it negotiate correctly
CSCvo20620	CUBE DNS SRV Query is not performed for PRACK
CSCvo90231	spurious accesses are seen in show alignment output with BGP
CSCvp22063	IR829 4G: Inserting antenna/SIM in SLOT1 disables IP connectivity on a working intf Cell 0/0
CSCvp38317	MGCP GW doesn't reset SSRC/ROC on receiving MDCX with new IP/port/SDP parameter for SRTP call.
CSCvp76434	OSPF summary-route (Type 5) redistribute into ospf via 'summary-address' cmd is not install in RIB
CSCvp79333	SSH may crash due to a corrupt MAC
CSCvp91256	BGP labels not propagated
CSCvp99569	Secondary subnets not redistributed from OSPF into BGP
CSCvp99881	BGP set wrong local preference for routes in RPKI invalid state
CSCvq01055	Replaces string not passed on CUBE REFER consumption scenario when address-hiding is configured
CSCvq06717	BGP/ expanded extcommunity regex filter is not working as expected
CSCvq18328	SSH: host_key->name is not null after reload which prevents SSH from starting up
CSCvq20936	CUBE router crashed due to memory corruption in subscription control block
CSCvq23676	CGR1000 - FE LEDs and SVI incorrect behavior
CSCvq40226	CUBE doesn't terminate the call after network failure
CSCvq41777	CUBE ha crash of standby unit after call hold from video endpoint
CSCvq46617	RLFA config causing OSPF to ignore backup path addition for NSSA prefix after primary link flap
CSCvq55604	C841M (15.8(3)M2) stuck at Splash Screen when access GUI (3.5.3) via Google Chrome & Firefox.
CSCvq63089	cat9300 hang and generate memory error when applying "privilege interface level 15 ospfv3"
CSCvq66030	Cisco IOS and Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability
CSCvq70840	LTE failover timer resets to 5 min after reload
CSCvq75610	freed rpi_parent is hit when deleting parent route by route update event

Caveat ID Number	Description
CSCvq89607	SIP phone paging party hears own voice on T-train
CSCvq92102	VG450: SCCP crashing router while shutdown the process
CSCvr02717	CGR1K_DOT11-3-RADIO_RESET
CSCvr12015	DMVPN with shared ipsec protection profile on ipv4 and ipv6 tunnel, only one tunnel comes up
CSCvr12455	KPML dialing fails after CSCvq20936 commit
CSCvr18570	When user cancel Call Forward All from the analog phone, user can't hear the confirmation tone
CSCvr23353	Unregistered supplicant can ping every re-authentication timer with mab when Spanning is disabled
CSCvr24316	Router crashes due to Segmentation Fault when 'ccb' gives a NULL Pointer
CSCvr27854	CGR1000 has SNMP queue length on 1 by default since 15.8(3)M2
CSCvr36117	router crash and reload due to freeblock magic number corruption
CSCvr53712	c927 c926 c921 usb flash drive/memory Stick problem
CSCvr57088	C3900-SPE250/K9 // memory leak in voice gateway
CSCvr62163	IOS Firewall crash with video call
CSCvr70878	SNMP cannot poll LLDP neighbors from the device
CSCvr80585	XSVC SIP trunks are shown as DOWN
CSCvr81357	ISR c800 is not giving DHCP address when port authentication failover from MAB to guest-vlan
CSCvr82645	PoE stops working after upgrade on C881K9
CSCvr92028	C921J-4P: Layer3 port(Gi4 and Gi5) linkup failure when peer is in fixed mode(speed or duplexity)
CSCvr95825	Trackbacks observed when querying DNS to ipv6 link local address.
CSCvr96849	System power-off after removing CLI for ignition undervoltage threshold
CSCvs50445	Ping Fails after SW-port is configured on interfaced

Open Bugs—Cisco IOS Release 15.9(3)M1

Table 11: Open Bugs—Cisco IOS Release 15.9(3)M1

Caveat ID Number	Description
CSCuv36677	IOS allows RC4-MD5 and RC4-SHA1 SSL ciphers to be negotiated by default
CSCva36891	ISM-VPN: double counting of SNMP ifInOctets on sub-int with crypto map
CSCvm94891	Crash caused by a "TLB Modification exception" after processing a null chunk in "IP Input" process.
CSCvn71487	CUBE fails to send outgoing SUBSCRIBE if egress dial-peer has "session server-group" configured
CSCvo15003	CUBE - SDP version increment behaviour creates cypto interworking issues
CSCvq04828	VRF aware reverse DNS lookup not working
CSCvq11134	SDP version was incremented due to misplace of PT 100
CSCvq62065	SIP phone paging party hears own voice
CSCvq74033	Packet drop in vdsl controller pppoe stuck in PADISNT
CSCvq79177	Router reload due to command "show control-plane host open-ports"
CSCvq83601	SNMP OID giving inaccurate/no updates for Cellular and interface OIDs
CSCvr37717	Crash due to PIM process
CSCvr97977	EIGRP hello packets sourced from the tunnel ip address even the EIGRP is not enabled on interface
CSCvs16361	Block Overrun after NHRP-3-PAKERROR syslog message
CSCvs27889	NAT address is deleted from route table after FTP passive mode communication
CSCvs28277	After configuring the time based queue limit in ms complete packet drops in default class
CSCvs39559	Reflexive ACL does not work on PATed packets in specific situation on IOS 15.7(3)M4a.
CSCvs40081	CUBE is not able to transfer the call
CSCvs52160	MWI does not work for all shared lines
CSCvs64611	Dual SIM fast-switchover is not working
CSCvs67791	491 returned on midcall INVITE when peer leg is not pending a request
CSCvs79450	Crash due to memory corruption [SNA]

Resolved Bugs—Cisco IOS Release 15.9(3)M0a

Table 12: Resolved Bugs—Cisco IOS Release 15.9(3)M0a

Caveat ID Number	Description
CSCvn55798	C897VAW-E-K9 // 15.7(3)M1 // Unable to disable lldp
CSCvr27262	DHCP CLIENT not working when CWMP agent is enabled
CSCvr44605	"Not supported for this platform" errro log when "show run"
CSCvr53712	c927 c926 c921 usb flash drive/memory Stick problem

Open Bugs—Cisco IOS Release 15.9(3)M0a

Table 13: Open Bugs—Cisco IOS Release 15.9(3)M

Caveat ID Number	Description
CSCvs26493	HCD_TRANS :VERBOSE error seen with USB OIR

Resolved Bugs—Cisco IOS Release 15.9(3)M

Table 14: Resolved Bugs—Cisco IOS Release 15.9(3)M

Caveat ID Number	Description
CSCvd19860	OSPFv3 AUTH breaks IPv6 traffic intermittently
CSCve77011	SSL handshake failure when validating certification with name-constraints
CSCvi48253	Y2.02K: self-signed cert expires after 31 Dec 2019, cannot be created after 1 Jan 2020
CSCvj28921	High CPU due to Alignment Corrections - SMEF & IWAN
CSCvk17998	Rekey Timer are same for both the Server and Client
CSCvn11434	IPSEC NAT-T / transport mode: UDP checksum not updated on decryption
CSCvn18500	Certificate map does not work always with UPN in SAN field
CSCvn56017	Crash while processing ISIS updates when DiffServ-TE is enabled
CSCvn66220	Layer 2 Neighbors Have No Connectivity Despite Authentication Open Being Configured
CSCvn66390	bgp dynamic neighbor not up
CSCvn75933	IS-IS needs to filter out Adjacency-SIDs for IPv6 address-family
CSCvn98815	TCLSH: smtp_lib.tcl broken VRF support
CSCvo03458	PKI "revocation check crl none" does not fallback if CRL not reachable

Caveat ID Number	Description
CSCvo10491	PnP Agent should detect image upgrade scenario and configure dialer to bring up cellular interface
CSCvo12745	Packet drop occurs after acl permit configurations
CSCvo19623	9200L Day0 setup not working out of box.
CSCvo24472	SNMP querry for local BGP AS "cBgpLocalAS" is failing
CSCvo27553	PKI incorrect fingerprint calulation during CA authentication
CSCvo27961	"%IR800_SPI_FLASH-3-VERIFY_ERROR: SPI Flash verification error at block 0x900000"
CSCvo37464	CUBE picks incorrect interface for media after receiving c=IN IP4 0.0.0.0
CSCvo39963	Analog phones on VG310 play continious BEEP tone approx every 60 secs.
CSCvo45698	BGP has VxLAN RNH "show bgp l2vpn evpn rnh" but missing entries in "show nve peers"
CSCvo60302	Deleting one sip-copylist will remove all sip copy-lists from dialpeers
CSCvo66216	IPSec-Session count in "show crypto eli" reaches max causing VPN failure
CSCvo70400	Reverse SSH bringing down RTS on serial interface
CSCvo72426	Flexible NetFlow Template ID is not getting exported
CSCvo81559	Router crashes after running "show interfaces transceiver detail"
CSCvo82837	Transcoder getting invoked for SRTP-SRTP calls.
CSCvo94468	%PERF_MON_ASYNC-3-MEM: Memory cleanup failed - ssrc db cache results in PMI not created on BR
CSCvp00182	Bytes output in show policy-map is incorrect on dialer interface
CSCvp05070	Overlay BGP down when configured "ip nhrp server-only"
CSCvp08738	Router loses "transport tcp tls v1.0" on reload
CSCvp13270	"mac-address-table secure sticky <mac-add>" lost when configure "mac-address-table secure maximum"
CSCvp26876	PNP profile using hostname is not working anymore
CSCvp27220	Tail drops on IPSLA sender when using scaled udp-jitter probes
CSCvp29316	ISR8xx TCAM limitation
CSCvp30312	Async port counter doesn't increment with 'reverse telnet'
CSCvp33421	Shut down interface Wlan-GigabitEthernet0

Caveat ID Number	Description
CSCvp38876	ESR crashed with Segmentation fault on Process Rate limit load process
CSCvp46185	Source Filter and Voice RTP Source-Filter in IOS Routers should allow RTP when on Hold
CSCvp47074	BGP sends malformed EVPN MAC/IP Advertisement Route
CSCvp47792	VG3x0 - groundstart voice-port configuration removed after reload
CSCvp60608	Reload when importing certificate from nvram:
CSCvp66849	MED should be compared if the first AS number in AS-PATH is 2^16, i.e, 65536
CSCvp78236	Crash during SNMP Configuration, ospfv3_pdb_from_router_info
CSCvp81102	IPsec SA installation fails with simultaneous negotiations despite fix for CSCve08418
CSCvp81193	After receiving 491, cube is not setting the media transcoder flag at SRTP leg
CSCvp87125	Default-route is not installed in Local PE VRF if there is 0.0.0.0/X route present in routing table
CSCvp90380	C5915 - NVRAM corrupts during bootup
CSCvp92334	Crash after Media monitor look up.
CSCvq00362	ISRG2: SRTP information not passed in Outgoing 183SP's SDP in external call forward scenario
CSCvq00550	Split DNS not working in case of TCP query coming on WAN interface and destined to LAN interface
CSCvq03717	ISDN memory leak
CSCvq04830	C921 forward packets with a destination MAC address that is not the MAC Address of SVI
CSCvq09955	[C900] traffic cannot be forwarded once storm-control changed from blocking to forwarding
CSCvq22176	IR807G-LTE-GA-K9 is not recognized as Cisco genuine product
CSCvq55604	C841M (15.8(3)M2) stuck at Splash Screen when access GUI (3.5.3) via Google Chrome & Firefox.
CSCvq57345	When the traffic rate is increased , VDSL interface starts bouncing
CSCvq59529	C926 and C927 will have VDSL down when mac address on Ethernet interface is changed

Open Bugs—Cisco IOS Release 15.9(3)M

Table 15: Open Bugs—Cisco IOS Release 15.9(3)M

Caveat ID Number	Description
CSCva36891	ISM-VPN: double counting of SNMP ifInOctets on sub-int with crypto map
CSCve53112	ASR920: EC-5-MINLINKS_MET syslog is not generated
CSCvh82421	Port channels interface counters show decrement for CRC errors
CSCvj00317	Memory leak VOIP *MallocLite*
CSCvm94891	Crash caused by a "TLB Modification exception" after processing a null chunk in "IP Input" process.
CSCvn71487	CUBE fails to send outgoing SUBSCRIBE if egress dial-peer has "session server-group" configured
CSCvn79227	QSIG - SIP - Connected Number Missing leading digit when decoding raw QSIG
CSCvn82489	CUBE changing the payload for content sharing packets, though it negotiate correctly
CSCvo15003	CUBE - SDP version increment behaviour creates cypto interworking issues
CSCvo20620	CUBE DNS SRV Query is not performed for PRACK
CSCvo58774	tracebacks unqueue didn't find XX in queue XXX-Process= "MAB Framework", ipl= , pid=
CSCvo61691	Disable MOP by default
CSCvq04828	VRF aware reverse DNS lookup not working
CSCvq05185	ISDN calls being picked in round robin manner instead of all happening at the same time
CSCvq11134	SDP version was incremented due to misplace of PT 100
CSCvq18307	VRF routes disappeared after reload
CSCvq20936	3945 CUBE / 15.7(3)M3 / Subscription control block corrupted ccsipSCB_t
CSCvq40226	CUBE doesn't terminate the call after network failure
CSCvq45550	SIP Profiles not properly modifying 400 responses
CSCvq47016	Exporter Thread crash after low stack report
CSCvq56242	C888 VIP not reachable for some VRRP ID
CSCvq62065	SIP phone paging party hears own voice
CSCvq74033	Packet drop in vdsl controller pppoe stuck in PADISNT

Caveat ID Number	Description
CSCvq79643	Crash after configuring network statement under BGP
CSCvq83601	SNMP OID giving inaccurate/no updates for Cellular and interface OIDs
CSCvq87669	dACL Not Applied on Slave Switches in a stack

© 2019–2026 Cisco Systems, Inc. All rights reserved.