Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Bengaluru 17.4.x

First Published: 2020-12-18

Last Modified: 2020-12-01

Cisco 4000 Series Integrated Services Routers Overview

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

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

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

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

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

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

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

Upgrading to a New Software Release

To install or upgrade, obtain a Cisco IOS XE Begaluru 17.4.1a consolidated package (image) from Cisco.com. You can find software images at http://software.cisco.com/download/navigator.html. To run the router using individual sub-packages, you also must first download the consolidated package and extract the individual sub-packages from a consolidated package.

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

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

Recommended Firmware Versions

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

Table 1: Recommended Firmware Versions

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices	CCO URL for the CPLD Image
Cisco 4461 ISR	16.12(2r)	21102941	isr_4400v2_cpld_update_v20.SPA.bin isr4400v2hwprogrammable040100.SPA.pkg
Cisco 4451 ISR	16.12(2r)	19042950	isr4400_cpld_update_v20.SPA.bin
Cisco 4431 ISR	16.12(2r)	19042950	isr4400_cpld_update_v20.SPA.bin
Cisco 4351 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4331 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4321 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4221 ISR	16.12(2r)	19042420	isr4200_cpld_update_v20.SPA.bin

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

Upgrading Field-Programmable Hardware Devices

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

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

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

Feature Navigator

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

New and Changed Information

New Hardware Features in Cisco IOS XE Bengaluru 17.4

There are no new hardware features for this release.

New Software Features in Cisco 4000 Series ISRs Release Cisco IOS XE Bengaluru 17.4.1a

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Bengaluru 17.4.1a:

- BGP Large Community—The BGP large communities are similar attributes to BGP communities. The BGP large communities attribute provides the capability for tagging routes and modifying BGP routing policy on routers. BGP large communities can be appended or removed selectively on the large community attribute as the route travels from router to router.
- Consent Token Authorization Process for Dev Key Access—With the introduction of the dev-key install functionality, a subset of Cisco IOS XE platforms which support dev-key install functionality are shipped only with release public key without a dev public key. With this change in the functionality, an image that is signed with a dev private key will not boot due to the absence of dev public key for image verification.
- CUBE: Hunt Stop for Server Groups—Server groups allow you to create simpler configurations by specifying a list of destination SIP servers for a single dial peer. When a call matches a dial peer that is configured with a server group, the destination is selected from the list of candidates based on a configured policy. If it is not possible to complete that call, the next candidate is selected. Alternatively, you can also choose to stop hunting through the group if a specified response code is received. If the call cannot be placed to any of the servers in the group, or hunting is stopped, call processing continues to the next preferred dial-peer.
- CUBE: VoIP Trace Serviceability Framework—VoIP Trace is a Cisco Unified Border Element (CUBE) serviceability framework, which provides a binary trace facility for persistently monitoring and troubleshooting SIP call issues. The VoIP Trace framework records both successful and failed calls. All call trace data is stored in system memory. In addition, data for calls with IEC errors is written to the logging buffer.
- CUBE: Smart License Using Policy—Smart Licensing using Policy reports license usage periodically based on an account policy, rather than requesting licenses based on past usage as in previous releases. Evaluation mode and license reservation are not supported. Frequent license requests used to go out from a device to CSSM in earlier versions. In the changed scenario, minimum reporting license usage is 8 hours. Now all the devices within a network follow the uniform approach of reporting their license usage to Smart Agent. The Smart Agent in turn creates a Resource Utilization Monitoring (RUM) report and dispatches to CSSM based on the Smart Agent reporting policy

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.
- CUBE: Clear Hung RTP Ports—When establishing a call, CUBE allocates several RTP ports that are based on the media that are negotiated for the session. Some ports remain assigned even after the call ends. In the current behavior, **show voip rtp stats**command displays only the ports allocated from the global table, even if the ports are allocated from all the three tables (Global port, media IP address-based, and media VRF-based). Now this command is enhanced to display the ports allocated from all the three tables. The command also displays the hung ports and allows you to release those ports. Releasing the hung ports increases the efficiency of the routers as more ports are available to receive calls.
- Change of Authorization and Trustsec—Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication,authorization, and accounting (AAA) session after it is authenticated. Identity-Based Networking Services supports change of authorization (CoA) commands for session query,reauthentication, and termination, port bounce and port shutdown, and service template activation and deactivation.

- Configure Performance Measurement— This feature enables hardware timestamping. The Performance Measurement (PM) for link delay uses the light version of Two-Way Active Measurement Protocol (TWAMP) over IP and UDP.
- Configuring the Same Global Address for Static NAT and PAT— You can now configure the same global address within the static NAT and static PAT. This configuration is supported only on outside static NAT.
- Configuring Stateless Static NAT— Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. A new keyword stateless is introduced for Cisco IOS XE static NAT configuration and it applies only to static NAT command. When the static mapping is set to stateless, no sessions will be created for that traffic flow.
- EPC support on LTE interface and FlexVPN Interface— Embedded Packet Capture (EPC) is an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from a device. This feature facilitates troubleshooting by gathering information about packet format.
- IP-SLA-HTTPS on ISR— This feature has enhanced capabilities of IP SLA device tracking with HTTPS probes and helps to verify reachability in the network.
- NBAR Support on the EVC Service Instance—To classify the data packets, enable NBAR FIA-trace data for NBAR on the EFP interface. Quality of service (QoS) takes action on the output interface based on the NBAR traffic classification result.
- Unified SRST: Smart License Using Policy—Smart Licensing using Policy reports license usage periodically based on an account policy, rather than requesting licenses based on past usage as in previous releases. Evaluation mode and license reservation are not supported. License usage is reported to Smart Agent three minutes after the last configuration change. Now all the devices within a network follow the uniform approach of reporting their license usage to Smart Agent. The Smart Agent in turn creates a Resource Utilization Monitoring (RUM) report and dispatches to CSSM based on the Smart Agent reporting policy. For more information see the Smart License Using Policy for Unified SRST and Smart License Using Policy for Unified E-SRST guides.

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.
- Unified CME: Smart License Using Policy—Smart Licensing using Policy reports license usage periodically based on an account policy, rather than requesting licenses based on past usage as in previous releases. Evaluation mode and license reservation are not supported. License usage is reported to Smart Agent three minutes after the last configuration change. Now all the devices within a network follow the uniform approach of reporting their license usage to Smart Agent. The Smart Agent in turn creates a Resource Utilization Monitoring (RUM) report and dispatches to CSSM based on the Smart Agent reporting policy.

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.
- You can use the Web UI to configure Smart Licensing on the Cisco 4000 Series Integrated Services Routers. For more information, see *Web UI Online Help*.

Configure the Cellular Back-off Operation

For a router with 3G/4G interface, sometimes service provider network might be busy, congested, in maintenance or in fault state. In such circumstances, service provider network rejects session activation request from the router by returning reject cause code 33 as a response of the activation request. After the router receives the reject cause, the router uses the back-off operation with the pre-defined timer value which could

be carrier-specific. While back-off operation is in progress, no new session activation request is sent out from the router. After the back-off period is up, new session activation request is sent out from the router.

Note: There is no command to disable the cellular back-off feature on the router.

The following example shows how to configure the cellular back-off feature to stop continuous session activation requests back to the router:

```
Router#show cell 0/2/0 all
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
.
.
.
Success rate is 0 percent (0/5)
Router#show cell 0/2/0 c
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
RouterCall end mode = 3GPP
RouterSession disconnect reason type = 3GPP specification defined(6)
RouterSession disconnect reason = Option unsubscribed(33)
RouterEnforcing cellular interface back-off
 Period of back-off = 1 minute(s)
Profile 4, Packet Session Status = INACTIVE
...
Profile 16, Packet Session Status = INACTIVE

.
.
.
Profile 16, Packet Session Status = INACTIVE
```

Configure the Router for Web User Interface

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

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

Entering the Configuration Commands Manually

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

Before you begin

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

Procedure

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

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

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

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

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

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

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

```
Router> enable
password password
```

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

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

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

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

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

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

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

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

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

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

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

```
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# end
```

Resolved and Open Bugs

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

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

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

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

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

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

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

Using the Cisco Bug Search Tool

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

Before You Begin

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

Your search results update when you choose a filter.

Resolved and Open Bugs in Cisco 4000 Series Integrated Services Routers

Open Bugs for Cisco IOS XE Bengaluru 17.4.2

Caveat ID Number	Description
CSCvw84883	DDNS feature triggers crash on 16.X/17.X releases due to memory corruption

Resolved Bugs - Cisco IOS XE Bengaluru 17.4.2

No resolved bugs for this release.

Open Bugs-Cisco IOS XE Bengaluru 17.4.1a

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

Caveat ID Number	Description
CSCvu59952	Cisco 4461 ISR: Control Connections over sub-interface are down after upgrade, TX Channel create failure.
CSCvw14836	ISR router running 16.9.6 crashes authenticating crypto certificate.
CSCvw30791	NIM:C1111X-ES-8 on C1111X-8P with version 17.03.01a.0.354 S keeps reloading.
CSCvw44835	Cisco 4000 Series ISR: Traceback seen on cpp_sdwan_sess_stats_free
CSCvw57860	Duplicate entries seen in MAC filter table.
CSCvu32446	Cisco 4451 ISR reboots with reason_code "CPU Usage due to Memory Pressure exceeds threshold".
CSCvu59952	Cisco 4461 ISR: Control Connections over sub-interface are down after upgrade, TX Channel create failure
CSCvv33576	IGMP snooping table not populated on Cisco 4000 ISR.
CSCvv44331	AppQoe Clear Alarm is not generated from device/
CSCvv78028	No responder-bytes from cEdge when UTD is enabled
CSCvv79072	25G license tags is retained and throughput throttled after upgrade from 17.3.1 to 17.3.2.
CSCvv88621	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage.
CSCvw11902	Passive FTP doesn't work with NAT
CSCvw13048	Crash observed at NHRP while using summary-map.
CSCvw33113	Unexpected reload in NHRP when access to an invalid memory region.
CSCvw34157	APPNAV CFT crashes.
CSCvw39383	CPP ucode crash with fw_base_flow_create.

Caveat ID Number	Description
CSCvw44835	Cisco 4000 ISR: Traceback seen on cpp_sdwan_sess_stats_free.
CSCvw47800	HSL Export over VASI Interface causes Netflow v9 Template Flooding.
CSCvw48800	Unable to transfer 1500 byte IP packet when using BRI bundled Multilink.
CSCvw48943	crypto ikev2 proposals are not processed separately.
CSCvw57860	Duplicate entries seen in MAC filter table.
CSCvw58560	FlexVPN reactivate primary peer feature does not work with secondary peer tracking.
CSCvw70461	ZBFW: Classification of traffic not happening correctly sometimes when a rule in RS is edited.
CSCvw71941	QFP crash in cpp_ess_tc_tgt_if_fm_edit_helper.
CSCvw73701	ZBFW:Stale ACL entries seen.
CSCvw74921	APPNAV CFT crash on ISR

Resolved Bugs - Cisco IOS XE Bengaluru 17.4.1a

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

Caveat ID Number	Description
CSCvt05460	IOS-XE: NAT not work for Active FTP.
CSCvu04426	Cisco 4000 Series ISR reloads with erroneous reload cause code.
CSCvv17488	Cisco 4000 Series ISR wth SM-X-ES3: Memory leak in iomd
CSCvv34057	Cisco 4351 ISR: Crash is seen with ZBFW.
CSCuv97577	Mishandling of dsmpSession pointer causes a crash.
CSCvs48300	Boot fails in ISR4221.
CSCvt05460	IOS-XE: NAT not work for Active FTP.
CSCvt75088	ISR4451: Protocol not in this image logs are seen after advertise network <prefix> config commit.
CSCvt89441	IOS-XE device crashed with CGD shared memory corruption freed by FMAN-FP.
CSCvu07639	UTD policy on global VPN does not work properly for DIA traffic.
CSCvu10006	Performance monitor caused QoS miss classification.
CSCvu11066	Umbrella custom DNS config not in sync between confd and IOS.
CSCvu11115	IOS-XE MTP Fails to Interwork DTMF RFC2833 from Payload 100 to Payload 101.

Caveat ID Number	Description
CSCvu27953	Crashes due to a segmentation fault in the "IPsec background proc" process.
CSCvu34009	Calls going through T1 are rejected with "no dsps found" Analog/TDM Hairpin calls.
CSCvu34381	Packets are not dropped as expected in selfzone to zone vpn 0 firewall configuration.
CSCvu43248	%IP-4-DUPADDR: Duplicate address issue at NAT-HSRP ISR4k router.
CSCvu65669	Traffic drop from branch overlay ping to service side without zp vpn1 to vpn1 when FW & IPS enabled.
CSCvu89033	Template push error due to NAT-MIB process helper traceback/warm restart.
CSCvu92277	Memory leak observed for FTM process leading to a device crash eventually.
CSCvu92879	Huge amount of Crypto PKI RECV memory leaks keep increasing during clients SCEP enrollments.
CSCvu99045	NIM-1GE-CU-SFP/NIM-2GE-CU-SFP: Show interface output reports incorrect bandwidth.
CSCvv03229	Crash is seen in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE tunnel.
CSCvv04236	IOS-XE: IPv6 OSPF authentication ipsec - adjacency fails
CSCvv08341	Netconf deleting wrong IKEv2 parameters
CSCvv12401	ZBFW HA redundancy stuck in STANDBY-COLK-BULK. Bulksync Traceback seen in logs.
CSCvv17488	Cisco 4000 Series with SM-X-ES3: Memory leak in iomd.
CSCvv20380	Removing and adding bulk ACL leads to tracebacks and error-Objects.
CSCvv26538	Crash due to a NULL pointer while bringing down PPPoE sessions.
CSCvv36247	Memory Leak in MallocLite / Crypto IKMP.
CSCvv47691	Reload: IOS-XE router crashing due to DN mismatch.
CSCvv58312	Dataplane crash due to driver cpp_drv_i95_read_cb observed on Cisco 4461 ISR with traffic.
CSCvv79273	Router may crash when using Stateful NAT64.
CSCvv83345	Summary/default-map routes getting ignored for p2p interface.
CSCvw06719	Platform ipsec reassemble transit" tail-drops unencrypted IPv4 Fragments with specific payload
CSCvw14836	Cisco ISR router running 16.9.6 crashes authenticating crypto certificate.
CSCvw31389	PKT log functionality is broken.

Caveat ID Number	Description
CSCvw56517	LMR Unable to hear first seconds of audio.

Related Documentation

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