

# Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Everest 16.6

---

**First Published:** 2017-07-27

**Last Modified:** 2019-06-10

## About Cisco ASR 1000 Series Aggregation Services Routers



**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](http://content.cisco.com) to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

---

Cisco ASR 1000 Series Aggregation Services Routers are Cisco routers deployed as managed service provider routers, enterprise edge routers, and service provider edge routers. These routers use an innovative and powerful hardware processor technology known as the Cisco QuantumFlow Processor.

Cisco ASR 1000 Series Aggregation Services Routers run the Cisco IOS XE software and introduce a distributed software architecture that moves many operating system responsibilities out of the IOS process. In this architecture, Cisco IOS, which was previously responsible for almost all of the internal software processes, now runs as one of many Cisco IOS XE processes while allowing other Cisco IOS XE processes to share responsibility for running the router.

## New Features and Important Notes

### New and Changed Information

The following sections list the new hardware and software features that are supported on the Cisco ASR 1000 Series Aggregation Services Routers.

#### New Hardware Features in Cisco IOS XE Everest 16.6.2

No new hardware features were introduced for Cisco ASR 1000 Series in Cisco IOS XE Everest 16.6.2.

#### New Software Features in Cisco IOS XE Everest 16.6.2

The following are the new software features introduced in Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Everest 16.6.2.

**ASR1000: EPA 2x40G Support**

Effective Cisco IOS XE Everest 16.6.2, Cisco ASR 1000 2x40GE Ethernet Port Adapter (EPA-2X40GE) is supported on the following Cisco ASR 1000 Series Aggregation Services Routers:

- ASR 1006-X
- ASR 1009-X
- ASR 1013
- ASR 1002-HX

**Encrypted Traffic Analytics**

For detailed information, see the following Cisco documents:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/xe-16-6/nf-xe-16-6-book/encrypted-traffic-analytics.html>

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf>

**New Hardware Features in Cisco IOS XE Everest 16.6.1**

No new hardware features were introduced for Cisco ASR 1000 Series in Cisco IOS XE Everest 16.6.1.

**New Software Features in Cisco IOS XE Everest 16.6.1**

The following are the new software features introduced in Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Everest 16.6.1.

**10GBase AOC SFP+ Cable support**

Effective with Cisco IOS XE Everest 16.6.1, the following transceiver models are supported on Cisco 1001-X Router, Cisco ASR 1001-HX Router, and Cisco ASR 1002-HX Router:

- SFP-10G-AOC1M
- SFP-10G-AOC1M
- SFP-10G-AOC2M
- SFP-10G-AOC3M
- SFP-10G-AOC5M
- SFP-10G-AOC7M
- SFP-10G-AOC10M
- SFP-10G-SR-S
- SFP-10G-LR-S

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/interfaces\\_modules/transceiver\\_modules/compatibility/matrix/10GE\\_Tx\\_Matrix.html#\\_Toc487104295](https://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/10GE_Tx_Matrix.html#_Toc487104295)

**BGP - SR: BGP Prefix SID Redistribution**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg\\_routing/configuration/xs-16-6/segrt-xe-16-6-book/sr-bgp-prefix-sid-redis.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xs-16-6/segrt-xe-16-6-book/sr-bgp-prefix-sid-redis.html)

**BGP Feature Monitoring**

Effective with Cisco IOS XE Everest 16.6.1, the Cisco IOS XE YANG models are supported for Border Gateway Protocol (BGP).

**Broadband Smart Licensing**

For detailed information, see the following Cisco document:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bbds/ios/bbds/configuration/xs-16-6/bba-xe-16-6-book/bba-smrt-lnse.html>

**CPAK-100G-SR4 Transceiver Support**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/100g/ios/100g/install/guide/100IHx\\_1002HXb\\_ASR100IHx-1002HX\\_HIGb\\_ASR100IHx-1002HX\\_HIG\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/100g/ios/100g/install/guide/100IHx_1002HXb_ASR100IHx-1002HX_HIGb_ASR100IHx-1002HX_HIG_chapter_010.html)

**Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) method support for MACsec Key Agreement (MKA)**

The Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) method support for MACsec Key Agreement (MKA) feature uses 802.1X port-based authentication with Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) to carry certificates for router ports where MACsec encryption is required. EAP-TLS mechanism is used to do the mutual authentication and to get the master session key (MSK) from which the connectivity association key (CAK) is derived for the MACsec Key Agreement (MKA) protocol.

For detailed information, see the following Cisco document:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xs-16-6/macsec-xe-16-6-book/macsec-cert-based-encrypt.html>

**Gx Monitoring**

For detailed information, see the following Cisco document:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/configuration/xs-16-6/isg-xe-16-6-book/isg-gx-dia-report-monitor.html>

**IPSec Anti-Replay Should Work When QoS is Enabled**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_dplane/configuration/xs-16-6/sec-ipsec-data-plane-xe-16-6-book/sec-ipsec-antireplay.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dplane/configuration/xs-16-6/sec-ipsec-data-plane-xe-16-6-book/sec-ipsec-antireplay.html)

**ISIS - SR OAM: ISIS FEC**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg\\_routing/configuration/xs-16-6/segrt-xe-16-6-book/oam-entropy-label-support.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xs-16-6/segrt-xe-16-6-book/oam-entropy-label-support.html)

**ISIS - SR: uLoop Avoidance**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg\\_routing/configuration/xs-16-6/segrt-xe-16-6-book/sr-is-is-uloop-avoidance.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xs-16-6/segrt-xe-16-6-book/sr-is-is-uloop-avoidance.html)

### **IWAN Application Group IWAN Harmonization**

An attribute “application-set” is added, which shares the existing features of all other attributes. This attribute can be used in QoS/PfR configurations and protocol customizations. The limitation of this attribute is that the “application-set” and “application-group” attributes must not be configured simultaneously with match protocol attribute statements.

### **Multiple HSL (N44 & N64) destinations over IPv6**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr\\_nat/configuration/xs-16-6/nat-xe-16-6-book/iadnat-hsl-vrf.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xs-16-6/nat-xe-16-6-book/iadnat-hsl-vrf.html)

### **NAT-Serviceability**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr\\_nat/configuration/xs-16-6/nat-xe-16-6-book/iadnet-int-overload-ports.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xs-16-6/nat-xe-16-6-book/iadnet-int-overload-ports.html)

### **OSPFv2: SR-OAM LSP Support**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg\\_routing/configuration/xs-16-6/segrt-xe-16-6-book/oam-entropy-label-support.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xs-16-6/segrt-xe-16-6-book/oam-entropy-label-support.html)

### **Patch for x86**

For detailed information, see the following Cisco document:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xs-16-6/config-mgmt-xe-16-6-book/cm-smu.html>

### **PBR Named Ordering Rules Support for Yang**

For detailed information, see the following Cisco document:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_pi/configuration/xs-16-6/iri-xe-16-6-book/iri-iprouting.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/xs-16-6/iri-xe-16-6-book/iri-iprouting.html)

### **PfRv3 Remote Prefix Tracking**

For detailed information, see the following Cisco document:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xs-16-6/pfrv3-xe-16-6-book/pfrv3-remote-prefix.html>

### **PfRv3 Per Interface Probe Tuning**

For detailed information, see the following Cisco document:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xs-16-6/pfrv3-xe-16-6-book/pfrv3-int-probe.html>

### **PfRv3-Inter-DC-Optimization**

For detailed information, see the following Cisco document:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xs-16-6/pfrv3-xe-16-6-book/pfrv3-inter-dc.html>

**PnP:SMU/Patching Support**

For detailed information, see the following Cisco document:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pnp/configuration/xe-16-6/pnp-xe-16-6-book.html>

**RESTconf Programmable Interface**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b\\_166\\_programmability\\_cg/restconf\\_prog\\_int.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b_166_programmability_cg/restconf_prog_int.html)

**SCP Performance Improvement**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_ssh/configuration/xe-16-6/sec-usr-ssh-xe-16-6-book.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-16-6/sec-usr-ssh-xe-16-6-book.html)

**SD-Access Phase 2**

For detailed information, see the following Cisco document:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sdaccess/configuration/xe-16-6/sda-xe-16-6-book.html>

**SD-AVC Auto-update Capability**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos\\_nbar/configuration/xe-16-6/qos-nbar-xe-16-6-book.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/xe-16-6/qos-nbar-xe-16-6-book.html)

**SD-AVC NBAR Export Capability**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos\\_nbar/configuration/xe-16-6/qos-nbar-xe-16-6-book.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/xe-16-6/qos-nbar-xe-16-6-book.html)

**Software Maintenance Upgrade**

For detailed information, see the following Cisco document:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xe-16-6/config-mgmt-xe-16-6-book/cm-smu.html>

**SR TE OAM**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg\\_routing/configuration/xe-16-6/segrt-xe-16-6-book/oam-entropy-label-support.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16-6/segrt-xe-16-6-book/oam-entropy-label-support.html)

**SR:OAMIGPFEC, BGP FEC**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg\\_routing/configuration/xe-16-6/segrt-xe-16-6-book/oam-entropy-label-support.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16-6/segrt-xe-16-6-book/oam-entropy-label-support.html)

**SXP Enhancements for Filtering (IP prefix and SGT) and Fail-open**

For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_cts/configuration/xe-16-6/sec-usr-cts-xe-16-6-book/cts-sxp-sgt.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-16-6/sec-usr-cts-xe-16-6-book/cts-sxp-sgt.html)

### UDF ACL Enhancement

For detailed information, see the following Cisco document:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xr-16-6/lanswitch-xe-16-6-book/lansw-conf-erspan.html>

### Web Server Enhancements

For detailed information, see the following Cisco document:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/configuration/xr-16-6/https-xe-16-6-book.html>

### WEB User Interface

Supports an embedded GUI-based device-management tool that provides the ability to provision the router, simplifies device deployment and manageability, and enhances user experience. The following features are supported on Web User Interface from Cisco IOS XE Everest 16.6.1:

- Cisco Umbrella Branch—The Cisco Umbrella Branch feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the enterprise DNS server through the Cisco 4000 Series Integrated Services Routers (ISR). The security administrator configures policies on the Cisco Umbrella Branch cloud to either allow or deny traffic towards the fully qualified domain name (FQDN). Cisco 4000 Series ISR acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Cisco Umbrella Branch cloud.
- Dynamic Multipoint VPN—The Dynamic Multipoint VPN feature allows users to better scale large and small IP Security (IPsec) Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).
- Snort IPS/IDS—The Snort IPS feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on Cisco 4000 Series Integrated Services Routers and Cisco Cloud Services Router 1000v Series. This feature uses the open source Snort solution to enable IPS and IDS.
- Zone-Based Firewall—Allows you to easily manage Cisco IOS unidirectional firewall policy between groups of interfaces known as zones.

### YANG Data Models

For the list of Cisco IOS XE YANG models available with this release, navigate to <https://github.com/YangModels/yang/tree/master/vendor/cisco/xr/1661>. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same github location highlights changes that have been made in the release

### Zero Touch Provisioning

Supports HTTP file download with TFTP file download. For detailed information, see the following Cisco document:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b\\_166\\_programmability\\_cg/zero\\_touch\\_provisioning.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b_166_programmability_cg/zero_touch_provisioning.html)

## Important Notes

The following sections contain important notes about Cisco ASR 1000 Series Aggregation Services Routers.

## Encrypted Traffic Analytics and Embedded Services Processors

Because of [CSCvg38872](#) Cisco ASR 1000 Series Aggregation Services Routers with ESP100 or ESP200 is not supported in .

### Deferrals

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following location to determine whether your software release is affected:

[http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.html)

### Field Notices and Bulletins

- Field Notices—We recommend that you view the field notices to determine whether your software or hardware platforms are affected. You can find the field notices at the following location:

[http://www.cisco.com/en/US/support/tsd\\_products\\_field\\_notice\\_summary.html](http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html)

- Bulletins—You can find bulletins at the following location:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod\\_literature.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html)

## Caveats

### Open and Resolved Bugs

The open and resolved bugs for a 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.

### 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 and FAQ](#).

#### Before You Begin

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:
- 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.
  - 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 <a href="#">Bug Search Tool Help and FAQ</a> .
Rating	The rating assigned to the bug by users of the <a href="#">Cisco Bug Search Tool</a> .
Support Cases	Whether a support case has been opened or not.

Your search results update when you choose a filter.

---

## Cavin Cisco IOS XE Everest 16.6.10

### Resolved Caveats—Cisco IOS XE Everest 16.6.10

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



Caveat ID Number	Description
<a href="#">CSCvt53563</a>	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability
<a href="#">CSCvw25564</a>	Cisco IOS and IOS XE Software IKEv2 AutoReconnect Feature Denial of Service Vulnerability
<a href="#">CSCvw46194</a>	IOS and IOS XE Software UDLD Denial of Service Vulnerability
<a href="#">CSCvx41294</a>	High CPU usage caused by "TCP Timer" process
<a href="#">CSCvx66699</a>	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability
<a href="#">CSCvv78028</a>	Cisco IOS XE Software Zone-Based Policy Firewall ICMP and UDP Inspection Vulnerability
<a href="#">CSCvx16081</a>	Cisco IOS XE Software H.323 Application Level Gateway Bypass Vulnerability
<a href="#">CSCvx37176</a>	Cisco IOS XE Software Rate Limiting Network Address Translation Denial of Service Vulnerability

### Open Caveats—Cisco IOS XE Everest 16.6.10

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

Caveat ID Number	Description
<a href="#">CSCvv12527</a>	Crash in SNMP Engine process while polling chassis id in lldp
<a href="#">CSCvw57495</a>	Cisco ASR 900 and ASR 920 Series Aggregation Services Routers Access List Bypass Vulnerability

### Cavin Cisco IOS XE Everest 16.6.9

#### Resolved Caveats—Cisco IOS XE Everest 16.6.9

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

Caveat ID Number	Description
<a href="#">CSCvg79590</a>	Traffic passed with port unauthorized
<a href="#">CSCvn68893</a>	ASR1k Process = TUN ETHER Thread crash
<a href="#">CSCvr26524</a>	Crash due to NBAR classification
<a href="#">CSCvr66463</a>	With CRL fetch failed, stuck at Failed to send the request. There is another request in progress
<a href="#">CSCvr93458</a>	Hub router crashed when run test_mpol_policy_qos_policy_template testcase
<a href="#">CSCvs48300</a>	Arkenstone boot fail in ISR4221
<a href="#">CSCvs58804</a>	Cisco IOS XE Software Arbitrary Code Execution Vulnerability

Caveat ID Number	Description
<a href="#">CSCvs71952</a>	Cisco IOS XE Software Zone-Based Firewall Denial of Service Vulnerabilities
<a href="#">CSCvs85642</a>	ISR G3 router crashes when rtp-nte DTMF packet arrives at MTP + BDI
<a href="#">CSCvt19873</a>	ASR1k:Router stops forwarding traffic with MPLS TE & FRR
<a href="#">CSCvt76844</a>	ASR1002-X ESP crash in multikey_hash_ager_tw_timer_to()
<a href="#">CSCvt79205</a>	ASR1001-X: 'show environment' is no longer monitoring R0 voltage sensors
<a href="#">CSCvu00800</a>	Unexpected reload when UC wsapi CLI is enabled.
<a href="#">CSCvu04413</a>	Cisco IOS XE Software for Cisco ASR 1000 Series ESP-20 IP ARP DoS Vulnerability
<a href="#">CSCvu11115</a>	IOS-XE MTP Fails to Interwork DTMF RFC2833 from Payload 100 to Payload 101
<a href="#">CSCvu34009</a>	Calls going through T1 are rejected with "no dsps found" Analog/TDM Hairpin calls
<a href="#">CSCvu99045</a>	NIM-1GE-CU-SFP/NIM-2GE-CU-SFP: Show interface output reports incorrect bandwidth
<a href="#">CSCvv98528</a>	ISR 4K SER parity error checks continuing till router crashes
<a href="#">CSCvw34157</a>	APPNAV CFT Crashes
<a href="#">CSCvw40079</a>	ASR1k crashes in ipv6 mgd timer code when removing vrf config
<a href="#">CSCvw57860</a>	Duplicate entries seen in MAC filter table.
<a href="#">CSCvw68171</a>	Duplicate Bytes and Packet when Q in Q is configured
<a href="#">CSCvx02515</a>	BGP IPv6 link-local session doesn't come up

### Open Caveats—Cisco IOS XE Everest 16.6.9

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

Caveat ID Number	Description
<a href="#">CSCve01479</a>	e2e ping is failed after configuring profiles qos-de and aaaauth1
<a href="#">CSCvf50723</a>	Packet-tracer error message % Error: Failed to collect packet info
<a href="#">CSCvf86185</a>	NIM-SSD: Inventory of disk0 and disk1 are interchanged on Polaris 16.x
<a href="#">CSCvg77924</a>	FRR feature not working in ESP100 and ESP200
<a href="#">CSCvi37580</a>	There is unexpected packets lost TCA reported on ISR4331 platform
<a href="#">CSCvj17326</a>	isr44xx crashes in o2_cavm_pci_unlock when forwarding large packets for VPLS
<a href="#">CSCvj56098</a>	CDP over EVC is not working
<a href="#">CSCvn82063</a>	Input CRC counter increasing on Tengi interface

Caveat ID Number	Description
<a href="#">CSCvp49863</a>	Incomplete arp in management interface
<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="#">CSCvr27554</a>	ASR1000-RP2/ASR1000-RP3: OIR after clock set doesn't save the time in RTC
<a href="#">CSCvr89973</a>	NIM interfaces go into shutdown after router bootup
<a href="#">CSCvt15551</a>	Crash observed in QFP in ASR1001-X running 16.06.05 when GPM is running low
<a href="#">CSCvt35331</a>	Console port goes unresponsive, reboot required to restore it
<a href="#">CSCvt53843</a>	Dataplane QFP crash with CAPWAP traffic when CAPWAP stripping is enabled
<a href="#">CSCvt71774</a>	C1111 HSRP preempt worked even though HSRP's preempt is not configured
<a href="#">CSCvt90424</a>	CRC increasing on down int Te0/0/20
<a href="#">CSCvv33576</a>	IGMP snooping table not populated on ISR4k
<a href="#">CSCvw52574</a>	ASR1K configured with 'no ip unreachable' sending ICMP Type 3 Code 13
<a href="#">CSCvw59276</a>	erspan classify ucode crash
<a href="#">CSCvw87188</a>	Stuck SGT pending-issue-update objects with CTS configured and NIM installed
<a href="#">CSCvw89147</a>	Crash at the moment of calculating tcp header
<a href="#">CSCvw90983</a>	ISR4K crashes with scaled QOS after applying QOS configuration to sub-interfaces
<a href="#">CSCvx23482</a>	ISR4321 reloading once NIM-1MFT-T1/E1 module is installed

## Caveats Cisco IOS XE Everest 16.6.8

### Resolved Caveats—Cisco IOS XE Everest 16.6.8

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

Caveat ID Number	Description
<a href="#">CSCua95810</a>	IOS PKI: trustpoint doesn't rollover regenerated RSA keys.
<a href="#">CSCva53392</a>	Polaris 16.3.1 : Machine and bus error failures in ESP20
<a href="#">CSCvh59431</a>	Byte counters for physical interface and subinterface don't match
<a href="#">CSCvi07924</a>	ASR1k ESP200 is missing suite B support when ESP200 is put into slot 1 only
<a href="#">CSCvi48253</a>	Self-signed certificates expire on 00:00 1 Jan 2020 UTC, cannot be created after that time
<a href="#">CSCvk71047</a>	Router fails to reserve necessary ports for VPN traffic (UDP 500 & 4500) for ISAKMP

Caveat ID Number	Description
<a href="#">CSCvm46362</a>	ASR1k node in HA pair might crash due to punt-keepalive failures
<a href="#">CSCvo46778</a>	ESP200X:ucode Crash seen with PR2650((URPF+QOS+ACL+Netflow Multicast)-with IMIX traffic)
<a href="#">CSCvo97985</a>	path-id discovery failure with "CENT throttle check fails, throttle type:0"
<a href="#">CSCvp23112</a>	OBS: ping stop working on replacing MIP100 ->>> SIP40 >>>>>>>MIP100
<a href="#">CSCvp70459</a>	IOS: Prevent crypto ACL change if already mapped with crypto map configuration
<a href="#">CSCvp89419</a>	Error messages seen when configuring "logging persistent protected" on ASR1K routers
<a href="#">CSCvp94050</a>	cpp_bqs_srt_yoda_csr_tree_seid_initialize:1744 is not in "placed" state
<a href="#">CSCvq61590</a>	ESP reload due to cpp_cp_svr exception at cpp_bqs_exponent_cnt_validate
<a href="#">CSCvq81620</a>	Router crashes with ZBF HA sync.
<a href="#">CSCvq90361</a>	NHRP process crash on using same tunnel address on multiple spokes
<a href="#">CSCvq98095</a>	Gi0/0/0 interface stays up/up and LED green after cable removed
<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="#">CSCvr15127</a>	ASR1K/ISR4K Calls fade to no-way audio due to media inactivity detection after 20 minutes
<a href="#">CSCvr17167</a>	High memory utilization under "ezman" due to excessive parity error logging
<a href="#">CSCvr27777</a>	ASR1k - Egress byte count is innacurate
<a href="#">CSCvr42114</a>	16.6.7 UTD: Signature download failure
<a href="#">CSCvr43037</a>	"sh macsec statistics int <>" and "sh macsec status interface <>" does not show output
<a href="#">CSCvr45917</a>	ASR1K DSP MIB cdspTotalChannels not responding
<a href="#">CSCvr58230</a>	While signalling forking the CUBE is not Sending Re-INVITE for T.38 with the Authorized header.
<a href="#">CSCvr76534</a>	ISR4k : Crash seen at Process Exec
<a href="#">CSCvr80706</a>	IOSXE - ucode crash in ZBF during flow creation for TCP subflows
<a href="#">CSCvr89957</a>	CFT crashed frequently
<a href="#">CSCvs04194</a>	Process = Exec crash seen on dmap longevity testbed with clear cry sa peer several times
<a href="#">CSCvs07609</a>	Portchannel stats not working on ASR1002-HX

Caveat ID Number	Description
<a href="#">CSCvs09052</a>	ASR1K OTV: Incorrect MAC address count on EFP/BD QFP stats
<a href="#">CSCvs28073</a>	IOS-XE memory leak seen in 16.3.7 in IOSd due to update_sn_ao_state not deleting TDL bucket.
<a href="#">CSCvs75958</a>	ISR4331/K9 Dialer cannot make calls suddenly
<a href="#">CSCvs86573</a>	Connect message is never forwarded to the calling side
<a href="#">CSCvt33799</a>	Virtual address not reachable: "mac:0000:0c07:xxxx download to DP failed" for HSRP / VRRP over BDI.

### Open Caveats—Cisco IOS XE Everest 16.6.8

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

Caveat ID Number	Description
<a href="#">CSCvj55210</a>	Memory leaks at __be_PKI_keypair_name_get
<a href="#">CSCvo70549</a>	CME SIP: BE4000 Smart Licensing - Extension Assigner temp registration uses endpoint license
<a href="#">CSCvp70211</a>	Crash when running show crypto map
<a href="#">CSCvp98673</a>	Inband to OOB DTMF Fails to Be Passed On CUBE If Media Inactive Comes During Digit Processing
<a href="#">CSCvq91046</a>	ASR 1000 crash in NAT code when processing PPTP traffic
<a href="#">CSCvr17169</a>	qfp ucode crash with media monitor
<a href="#">CSCvr48349</a>	ESP ucode crashed when running NAT with bpa (CGN)
<a href="#">CSCvt70723</a>	ASR 1000 router crashed due to Crypto IKEv2 memory leaks
<a href="#">CSCvt76844</a>	ASR1002-X ESP crash in multikey_hash_ager_tw_timer_to()
<a href="#">CSCvt78293</a>	ASR 1000 RP3 crash due to CpuCatastrophicError

### Caveats in Cisco IOS XE Everest Release 16.6.7

#### Resolved Caveats—Cisco IOS XE Everest 16.6.7

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

Caveat ID Number	Description
<a href="#">CSCvd55092</a>	C3650 traffic will not be block although hit deny ACL entry
<a href="#">CSCvd77610</a>	AAA always reports server down with non-management VRF also

Caveat ID Number	Description
<a href="#">CSCvg32153</a>	"show interface port-channel" falsely reports output drops when there are no actual output drops
<a href="#">CSCvh11088</a>	Crash on OPF_CSR32_OPF_LOGIC_ERR_LEAF_INT_INT_START_OF_BURST_MARKER_ERR
<a href="#">CSCvh23735</a>	CSR1000v HA vCUBE IP-4-DUPADDR detected after Active router goes down.
<a href="#">CSCvh49874</a>	FNF monitor download to DP failed after changing netflow record
<a href="#">CSCvh79264</a>	Change the punt cause of packets whose destination is virtual IP from SUBNET_BCAST to FOR_US
<a href="#">CSCvh92659</a>	BFD flaps everytime with dynamic tunnel creation in DMVPN
<a href="#">CSCvi04907</a>	T38 Packets are dropped by CUBE on ISR G2 in Multi VRF Scenario
<a href="#">CSCvi22263</a>	Crash when IOS is adapting shaping with Adaptive QoS over DMVPN configured
<a href="#">CSCvj00317</a>	Memory leak VOIP *MallocLite*
<a href="#">CSCvj08229</a>	ASR1001-X: interface LED remains amber after shut/no shut on the interface
<a href="#">CSCvj28921</a>	High CPU due to Alignment Corrections - SMEF & IWAN
<a href="#">CSCvj72294</a>	memory leak @ CCSIP_SPI_CONTR
<a href="#">CSCvj76866</a>	Partial Power Failure in Stack Causes Interfaces to Become "shutdown"
<a href="#">CSCvk17998</a>	Rekey Timer are same for both the Server and Client
<a href="#">CSCvk47271</a>	ISR4K crashed in FXS-FXS non-hairpin call
<a href="#">CSCvk51939</a>	SSS Manager Traceback observer when test MLPPP
<a href="#">CSCvk63764</a>	Driver code improvement for debug-ability of XAUI link issues
<a href="#">CSCvm10850</a>	Crash after CPUHOG in ISDN L2D SRQ Process
<a href="#">CSCvm47690</a>	Addition/Edits to numbered OG ACL using "access-list <>" command does not re-expand the ACL.
<a href="#">CSCvm65979</a>	ASR-CUBE: Crashes with call spike configuration changes
<a href="#">CSCvn00104</a>	Software crash due to memory corruption after packet trace was enabled.
<a href="#">CSCvn01507</a>	ISR not re-calculating the hash value correctly after payload change
<a href="#">CSCvn02456</a>	Router crashes when the calls doesn't establish after making 2 calls when we set "max-conn 2"
<a href="#">CSCvn03502</a>	SR: CFLOW input intf index is 0xffffffff for Service-engine DSP module interface
<a href="#">CSCvn23906</a>	DHCP Server sends Renew ACKs to Clients with 00:00:00:00:00:00 MAC in L2 frame

Caveat ID Number	Description
<a href="#">CSCvn38960</a>	pending objects seen which fp reload with OGACL config
<a href="#">CSCvn45732</a>	Device crashing if we unconfigure the NTP on the device
<a href="#">CSCvn57892</a>	High Memory utilization due to Wireless Manager IOSD process
<a href="#">CSCvn61039</a>	ISR4k - 'control-plane host' feature was moved to APPX feature set.
<a href="#">CSCvn71373</a>	IOS-XE routers cannot boot due to a bootflash problem
<a href="#">CSCvn78961</a>	Subscribers cannot re-login due to CoA time-out (lite-sessions in routed mode)
<a href="#">CSCvo03458</a>	PKI "revocation check crl none" does not fallback if CRL not reachable
<a href="#">CSCvo04856</a>	DataPlane (DP) crash observed in MMOH call flow
<a href="#">CSCvo06817</a>	Router crash while executing show commands using ' ' (pipe) to filter the output.
<a href="#">CSCvo08740</a>	TCP 3WAY handshake fail for redirected packet using PBHK
<a href="#">CSCvo10145</a>	Memory overlay crash when using include-cui
<a href="#">CSCvo10491</a>	PnP Agent should detect image upgrade scenario and configure dialer to bring up cellular interface
<a href="#">CSCvo11786</a>	SCCP Application does not clear failed sockets leading to leak and socket pool exhaustion
<a href="#">CSCvo12745</a>	Packet drop occurs after acl permit configurations
<a href="#">CSCvo12799</a>	Call is not getting connected in Forking Re-INVITE scenario
<a href="#">CSCvo17287</a>	ASR1001-X crashed upon receiving Radius Access-Accept message
<a href="#">CSCvo21122</a>	Memory leak at hman process
<a href="#">CSCvo36031</a>	WSMA crash formatting show command output
<a href="#">CSCvo46138</a>	Stuck CPP Thread while processing H323 packet
<a href="#">CSCvo46405</a>	qfp ucode crashed with sRTP traffic - chunk memory corruption
<a href="#">CSCvo47376</a>	Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability
<a href="#">CSCvo55194</a>	After RSP switchover label imposition was not programmed in Software on APS standby router
<a href="#">CSCvo57768</a>	NetFlow issue 3850 switch not sending TCP flags
<a href="#">CSCvo61610</a>	FXS - no busy tone is generated on remote-onhook condition with call pickup scenario
<a href="#">CSCvo65415</a>	ASR1k crashes by handling DHCP packet
<a href="#">CSCvo66216</a>	IPSec-Session count in "show crypto eli" reaches max causing VPN failure

Caveat ID Number	Description
<a href="#">CSCvo70504</a>	Missing Calling-Station-ID in Accounting Ticket for Web-Tal locations
<a href="#">CSCvo71721</a>	When sending account-logon ISG do not reply with ACK nor NACK.
<a href="#">CSCvo73897</a>	[SDA] [PI changes] No audio during first few seconds of voice call between 2 Fabric Edge
<a href="#">CSCvo73954</a>	ASR1001-HX: Excessive pause frames (IEEE802.3x compliant) affect traffic on other interfaces
<a href="#">CSCvo74486</a>	IOS-XE ACL port information preserved after encapsulation
<a href="#">CSCvo83945</a>	Ping failure on Port-channel sub interface when is using EVC in main port channel
<a href="#">CSCvo87827</a>	Crash when polling IPForwarding MIB
<a href="#">CSCvo90060</a>	Wrong label programming leading to traffic drop
<a href="#">CSCvo92514</a>	SDP attribute list corruption causes voice gateway crash
<a href="#">CSCvo94211</a>	Traffic stops flowing on Xconnect tunnel when upgraded to 16.9.2
<a href="#">CSCvp08353</a>	Add ERROR message over IOS console when HSPRDA TCAM region gets full
<a href="#">CSCvp10711</a>	Hierarchical QoS stops working on GRE tunnel if dest route flaps between 2nd tunnel and physical int
<a href="#">CSCvp24405</a>	Router crash after adding macsec reply-protection command on an interface
<a href="#">CSCvp24911</a>	SRTP ROC Stress: CPP crash with 6000+ concurrent calls - g729
<a href="#">CSCvp24981</a>	When FQDN used for APN, IOS DNS resolves FQDN to IP, but GTP stays in DNS pending and IP 0.0.0.0
<a href="#">CSCvp25052</a>	ISR4K: Router crash due to twice memory release
<a href="#">CSCvp27220</a>	Tail drops on IPSLA sender when using scaled udp-jitter probes
<a href="#">CSCvp31779</a>	Router Running IOS-XE 16 Crashes when Stopping EPC with ACL
<a href="#">CSCvp32910</a>	CHUNKBADROOTCHUNKPTR: Bad root chunk pointer in chunk header post SSO - ASRIK
<a href="#">CSCvp33578</a>	Crash at the moment of deleting a DVTI
<a href="#">CSCvp34230</a>	CUBE HA - Global bind is removed during interface flap
<a href="#">CSCvp38317</a>	MGCP GW doesn't reset SSRC/ROC on receiving MDCX with new IP/port/SDP parameter for SRTP call.
<a href="#">CSCvp38424</a>	On-Prem DMVPN fails to establish a dynamic tunnel between Spoke nodes.
<a href="#">CSCvp38852</a>	[SDA] 1st ARP getting dropped due to stale SISF IP-MAC binding



Caveat ID Number	Description
<a href="#">CSCvp39597</a>	Crashes with GRE tunnels configured with QoS over Multilink Frame-relay interfaces
<a href="#">CSCvp42709</a>	ISR44xx NO_PUNT_KEEPLIVE kernel crash due to CP drivers stuck punt and IPC rings
<a href="#">CSCvp47006</a>	QoS counter didn't generate at ASR1001-X
<a href="#">CSCvp47723</a>	ISR4K CME no way audio on calls across E1/PRI, reboot resolves for sometime
<a href="#">CSCvp56596</a>	ISR4K crashes after voice register reset command is applied
<a href="#">CSCvp56737</a>	Counters of interfaces are reporting inexistent peaks
<a href="#">CSCvp59848</a>	ASR1001-x crash while configuring policy-map
<a href="#">CSCvp63616</a>	Crash due to too many DSPs
<a href="#">CSCvp65151</a>	CPP Stuck thread when processing IPv6 traffic
<a href="#">CSCvp67530</a>	Corrupt free block of memory with high availability config for Session Initiation Protocol
<a href="#">CSCvp69393</a>	Router crashes after snmpget to OID related to NHRP
<a href="#">CSCvp70443</a>	isdn cause-location command support for switch-type primary-ntt
<a href="#">CSCvp72220</a>	crash at sisf_show_counters after entering show device-tracking counters command
<a href="#">CSCvp72379</a>	ip dns primary command does not get removed
<a href="#">CSCvp74674</a>	QoS fails to apply to tunnel2 when underlying tunnel1 reachability change
<a href="#">CSCvp77100</a>	ASR1k: Crypto Engine remains in stuck state post dataplane crash
<a href="#">CSCvp84831</a>	name-ip_address mapping is bypassed when the ip domain command is configured on Cisco C1111X Router
<a href="#">CSCvp86216</a>	Router ucode crash with NAT with interface flap
<a href="#">CSCvp87488</a>	no login on-success log CLI does not persist across device reloads
<a href="#">CSCvp92334</a>	Crash after Media monitor look up.
<a href="#">CSCvp96418</a>	ISR4k BRI ping failure with WIC-1B-S/T-V3 with ISDN 128 leased line
<a href="#">CSCvp99884</a>	CUBE not passing History-Info header in 181 Call is being forwarded
<a href="#">CSCvq00263</a>	Device crashed @ radius_io_stats_timer_handler due to dynamic-author
<a href="#">CSCvq02003</a>	ASR1002-X High Platform CPU for process mcpcclc-ms
<a href="#">CSCvq02215</a>	ASR1K-X WATCHDOG crashes while printing to console
<a href="#">CSCvq04828</a>	VRF aware reverse DNS lookup not working

Caveat ID Number	Description
CSCVq10660	ASR1006-X: cpp_cp_svr: QFP0.0 CPP Driver LOCKDOWN encountered due to previous fatal error
CSCVq10663	NAT SIP Contact Header changed to port 512
CSCVq12723	DPDK: Performing Shut/No-Shut with traffic running can cause packets to silently drop on TX
CSCVq18793	NIM-2FXS/4FXOP crashing due to DSP failed to reply properly
CSCVq19808	Egress shaping on port-channel sub-intf tail dropping traffic long before rate
CSCVq23869	ASR 1k sub-interface counters wrong.
CSCVq25297	BRI leased line can't come up automatically after remove/insert one side's cable
CSCVq29575	Voice gateway crash due to segmentation fault in process CCSIP_DNS
CSCVq30306	IOSXE: IOMD / TDL leak seen with tdl_response_xcode_stat_side_t
CSCVq31129	AppNav: Optimization failed with Asymmetrical traffic, VRF, FNF and NBAR
CSCVq32736	ARM - Marvell 7040 SoC Hardware Erratum - Kernel Driver Fix
CSCVq36130	Router is on Bootloop after QoS configuration.
CSCVq39121	ISR4k crash during packet inspection due to stuck thread
CSCVq45088	asr1k BDI not working properly for packet fragmentation - very small fragments are getting dropped
CSCVq49000	Supervisor reloaded due to cpp_cp_svr process crashing
CSCVq50202	Class-attributes duplicated after EAP reauthen. in ISG radius proxy scenario
CSCVq57205	Recording failures with XMF media forking and SIP preservation timer
CSCVq57862	cable-detect command not reflecting proper status in Analog ports on IOS-XE platforms
CSCVq58144	cpp_cp_svr crash in cpp_bqs_rm_yoda_select_sch_exponent
CSCVq58237	Supervisor reload due to cpp_cp_svr crash.
CSCVq58265	ASR1K BGP PIC Repair path broke after link flap
CSCVq58378	Crash after exiting RADIUS server configuration mode.
CSCVq58520	after reload dial-peers with ports that have the 'signal did' command show operational state none
CSCVq72560	More connections are getting passthrough with reason SNG_OVERLOAD
CSCVq74418	connectivity is broken on ingress-replication L2DP/VXLAN

Caveat ID Number	Description
<a href="#">CSCvq75610</a>	IWAN router crash after upgrading to 16.3.8
<a href="#">CSCvq92102</a>	VG450: SCCP crashing router while shutdown the process
<a href="#">CSCvq98949</a>	ASR1000-RP3: Punt Keepalive Failure (Punt LINK DOWN) or RP FREEZE

### Open Caveats—Cisco IOS XE Everest 16.6.7

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

Caveat ID Number	Description
<a href="#">CSCva53392</a>	Polaris 16.3.1 : Machine and bus error failures in ESP20
<a href="#">CSCvd65197</a>	IOSd crashed when dialer disconnect the ISDN call
<a href="#">CSCve54914</a>	NDSSO vrf ha table to be populated correctly
<a href="#">CSCve78446</a>	[1661]- Switch number is missing in stack merged logs.
<a href="#">CSCvf28977</a>	ESP Crash with FP Switchover
<a href="#">CSCvg23820</a>	CTS PAC download fails with VRF config on non-management interface
<a href="#">CSCvh59431</a>	Byte counters for physical interface and subinterface don't match
<a href="#">CSCvi36351</a>	standby rp crash on removing member link from port-channel
<a href="#">CSCvj17326</a>	isr44xx crashes in o2_cavm_pci_unlock when forwarding large packets for VPLS
<a href="#">CSCvj55210</a>	Memory leaks at __be_PKI_keypair_name_get
<a href="#">CSCvj56098</a>	CDP over EVC is not working
<a href="#">CSCvk75838</a>	netconf/yang or telemetry retrieval of /trustsec-state/cts-rolebased-policies breaks
<a href="#">CSCvm42345</a>	Ping failing due to missing address resolution entry on the XTR
<a href="#">CSCvn39506</a>	ISIS: system crashed when we configure ISIS on the interface.
<a href="#">CSCvn82063</a>	Input CRC counter increasing on Tengi interface.
<a href="#">CSCvo70549</a>	CME SIP: BE4000 Smart Licensing - Extension Assigner temp registration uses endpoint license
<a href="#">CSCvp70211</a>	Crash when running show crypto map
<a href="#">CSCvp77521</a>	Device-tracking tracking 0.0.0.0 mask ignored after Legacy IPDT to SISF conversion
<a href="#">CSCvp89419</a>	Error messages seen when configuring "logging persistent protected" on ASR1K routers
<a href="#">CSCvp98673</a>	Inband to OOB DTMF Fails to Be Passed On CUBE If Media Inactive Comes During Digit Processing

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="#">CSCVq43550</a>	C1111-4P doesn't restart authentication for "clear authen session" if "authen open" the port
<a href="#">CSCVq56114</a>	Cat3k crash in IGMP code due to invalid source count in DNS lookup
<a href="#">CSCVq61590</a>	ESP reload due to cpp_cp_svr exception at cpp_bqs_exponent_cnt_validate
<a href="#">CSCVq69866</a>	HSRPv2 crash whilst retrieving group from received packet
<a href="#">CSCVq73281</a>	TLS connections in WebEx between CUBE and iCP/CUSP breaks intermittently
<a href="#">CSCVq75307</a>	Crash due to watchdog after adding a prefix-list/ Route-map entry to existing route map.
<a href="#">CSCVq78692</a>	mGRE L3VPN broken after reload
<a href="#">CSCVq81620</a>	Router crashes with ZBF HA sync.
<a href="#">CSCVq85913</a>	FlexVPN with password encryption -- after MasterKey change password in profile is not working
<a href="#">CSCVq90361</a>	NHRP process crash on using same tunnel address on multiple spokes
<a href="#">CSCVq91046</a>	ASR1k crash in NAT code when processing PPTP traffic
<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
<a href="#">CSCvr00983</a>	Unrecoverable Error with PVDM in 0/4 and Thule+dreamliner in 1/0 on ISR4300
<a href="#">CSCvr05406</a>	LISP Map-cache not updated correctly after wired Host-mobility
<a href="#">CSCvr15127</a>	ASR1K/ISR4K Calls fade to no-way audio due to media inactivity detection after 20 minutes
<a href="#">CSCvr15253</a>	Router Crashes while Parsing and Printing Voice Packet IEs
<a href="#">CSCvr17167</a>	High memory utilization under "ezman" due to excessive parity error logging
<a href="#">CSCvr17169</a>	qfp ucode crash with media monitor
<a href="#">CSCvr17670</a>	The ISR4331 crash and lost all config files
<a href="#">CSCvr22969</a>	3850 switch crashes on Process "DHCPD Receive" (16.6.6)
<a href="#">CSCvr32292</a>	Router may crash due to segmentation fault after running EEM script

## Caveats in Cisco IOS XE Everest Release 16.6.6

### Resolved Caveats—Cisco IOS XE Everest 16.6.6

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

Caveat ID Number	Description
<a href="#">CSCuw36080</a>	SNMP with Extended ACL
<a href="#">CSCvb87675</a>	BGP event crash@bgp_afpriv_imp_is_imported_path
<a href="#">CSCve91084</a>	CUBE:ASR1004:sRTP-RTP (No TLS) calls failed at an input of 27CPS
<a href="#">CSCvg23363</a>	Virtual-access interface MTU wrongly set when using ipsec ipv4
<a href="#">CSCvg79610</a>	APPNAV - Overlapping Loopback Interface Causes Incorrect Forwarding Decision with AppNav and PfR
<a href="#">CSCvh57657</a>	NAT MIB not populated when using traditional NAT
<a href="#">CSCvi44855</a>	cEdge: not enough space when SSHing to bootflash having more than enough space
<a href="#">CSCvj12370</a>	ASR1002-X router crashed in cpp_qm_event_collapse_hl_node
<a href="#">CSCvk32822</a>	QoS stats process crash
<a href="#">CSCvk62792</a>	IKE Fragmentation payload incorrectly marked as critical
<a href="#">CSCvk63782</a>	Quick RP3 recovery after the Punt Path XAUI link goes down
<a href="#">CSCvm17883</a>	Standby switch crashes when adding a host name to an object-group
<a href="#">CSCvm42441</a>	Router crash when clearing ip nat translations
<a href="#">CSCvm51112</a>	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys
<a href="#">CSCvm56670</a>	ACL dropping packets after updating it - %CPPEXMEM-3-NOMEM
<a href="#">CSCvm64865</a>	[EIGRP] a summary route is updated by an external route
<a href="#">CSCvm65397</a>	Active RP crash at __be_datagram_done
<a href="#">CSCvm70471</a>	'hw-module subslot 0/2 reload' CLI does not activate the container after harddisk format
<a href="#">CSCvm75066</a>	MPLSoVPN: Change behavior of default route in NHRP. Must insert 0.0.0.0/0 instead of /32
<a href="#">CSCvm76452</a>	IPSec background crash while sending SNMP trap
<a href="#">CSCvm96960</a>	ASR1001-X throwing: ETH_SPA_MAC-3-SPI4_ERROR: SIP0/1: Marvel MAC
<a href="#">CSCvn00218</a>	CUBE Crash in sipSPIAppAddCallInfoUI
<a href="#">CSCvn00277</a>	ASR 1006-X RP2 : Standby RP Crashed after running command "license boot level advenenterprise"

Caveat ID Number	Description
<a href="#">CSCvn02419</a>	Device running IOS-XE 16 Polaris Sees Crash When Performing NAT ALG on FTP Packet
<a href="#">CSCvn07478</a>	Ethernet FRR switchover takes more than 200ms on EPA10 and EPA100 if remote Rx fiber is pulled
<a href="#">CSCvn17530</a>	Router Crashes When PKI-CRL-IO_0 Runs out of Stack Space During Failed DNS Lookup for CA Server
<a href="#">CSCvn18790</a>	Cube crash with %SDP-3-SDP_PTR_ERROR
<a href="#">CSCvn23226</a>	NHRP process is crashing
<a href="#">CSCvn27449</a>	PBR doesn't work for dialer intf when it doesn't have fixed ip address
<a href="#">CSCvn36359</a>	CUBE doesn't forward INVITE with "midcal-signalling passthru media-change" during a video escalation
<a href="#">CSCvn37237</a>	ASR1002-HX crashed after huge traffic is transmitted over it
<a href="#">CSCvn51553</a>	QFP crashes with a HW interrupt
<a href="#">CSCvn56017</a>	Crash while processing ISIS updates when DiffServ-TE is enabled
<a href="#">CSCvn56365</a>	In some cases non AppNav Configuration cause AppNav-XE Token changes
<a href="#">CSCvn57165</a>	Static Nat fails to translate SIP Trying L7 header
<a href="#">CSCvn59020</a>	Modified EIGRP timers on Virtual-Template put all associated Vi interfaces into passive mode
<a href="#">CSCvn66258</a>	ASR1000-2T+20X1GE interface speed change from 100 to 1000 after switchover
<a href="#">CSCvn71041</a>	TACACS group server is not seen, when "transport-map type console test" is configured.
<a href="#">CSCvn72208</a>	RP3 Punt Interface May Drop Traffic Due to VLAN Filter Hardware
<a href="#">CSCvn77783</a>	class-attributes support in ISG radius proxy scenario
<a href="#">CSCvn78349</a>	FlexVPN with password encryption - keyring aaa LIST password 6 xxxxx encrypted again upon reload
<a href="#">CSCvn83172</a>	Router reloads on 'show track' command when there is track object for deleted serial sub-interface.
<a href="#">CSCvn92709</a>	SNG_AO unavailable alarms are not clearing after removing the monitor-load feature under policy
<a href="#">CSCvo00585</a>	Split DNS in case of UDP query to WAN interface IP via LAN interface
<a href="#">CSCvo01298</a>	Correction to Quick RP3 recovery after the Punt Path XAUI link goes down
<a href="#">CSCvo05000</a>	SIP global binding disappears when the interface to which SIP is bound flaps.

Caveat ID Number	Description
<a href="#">CSCvo15141</a>	CLI "nat force-on" in voice service voip not working as expected
<a href="#">CSCvo19395</a>	Router crashes when removing a crypto map
<a href="#">CSCvo20934</a>	FMAN crash due to Flexible Netflow (fnf)
<a href="#">CSCvo24170</a>	Crash due to chunk corruption in ISIS code
<a href="#">CSCvo27553</a>	PKI incorrect fingerprint calculation during CA authentication
<a href="#">CSCvo36188</a>	Crash at NAT clear
<a href="#">CSCvo41815</a>	When roaming to another AP, services received from RADIUS are not applied to the session
<a href="#">CSCvo43953</a>	Memory leak in CENT-BR-0 process
<a href="#">CSCvo47436</a>	IOSXE - firewall corrupts half open list
<a href="#">CSCvo47866</a>	Crash at Process = SCCP Auto Config
<a href="#">CSCvo62584</a>	DHCP discover packets were being dropped at firewall since UDP source port as 0.
<a href="#">CSCvo99156</a>	Software crash in btrace routines due to division by NULL.

### Open Caveats—Cisco IOS XE Everest 16.6.6

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

Caveat ID Number	Description
<a href="#">CSCvk51939</a>	SSS Manager Traceback observer when test MLPPP
<a href="#">CSCvn01507</a>	ISR not re-calculating the hash value correctly after payload change
<a href="#">CSCvo17287</a>	ASR1001-X crashed upon receiving Radius Access-Accept message
<a href="#">CSCvo56553</a>	ASR1000: RP3 crash due to punt-keepalive failures
<a href="#">CSCvo60849</a>	Crash noticed when routes are getting imported twice(from vpnv4 to vrf to evpn) with route churn
<a href="#">CSCvo62122</a>	IOS-XE Router may crash when attempting to Fragment Corrupted IPv4 Packet
<a href="#">CSCvo65415</a>	ASR1k crashes by handling DHCP packet
<a href="#">CSCvo94943</a>	ESP100 - ucode crash in encryption routines with Illegal Instruction
<a href="#">CSCvp02119</a>	Crash at mpass_restore_nonbl_persist_state due to invalid vector
<a href="#">CSCvp03110</a>	After Configuring a New VRF Routes Are Not Imported From WAN Into l2vpn EVPN For Unrelated VRF

Caveat ID Number	Description
<a href="#">CSCvj72294</a>	Memory leak happens at CCSIP_SPI_CONTR process for every trunk out-of-dialog message with "contact" header in it.

## Caveats in Cisco IOS XE Everest Release 16.6.5

### Resolved Caveats—Cisco IOS XE Everest 16.6.5

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

Caveat ID Number	Description
<a href="#">CSCvb03610</a>	Watchdog crash after "% AAA/AUTHEN/CONT: Bad state in aaa_cont_login()."
<a href="#">CSCve31475</a>	SNMP Error: OID not increasing: @ipAddressIfIndex.ipv6z
<a href="#">CSCvf91392</a>	Catalyst switch crashes when editing wireless controller settings through web interface on c3650
<a href="#">CSCvg04712</a>	ESP crash with cpp-mcplo-ucode core file
<a href="#">CSCvg29105</a>	asr1k: Gec 5 tuple feautre not working in IOS-XE releases post 16.4.1
<a href="#">CSCvh92275</a>	QoS Overrides loadbalancing to per prefix even with only session level policing applied
<a href="#">CSCvi08303</a>	Standby RP Reloads due to Config Sync Failure When Applied Service-insertion WAAS on Physical Int
<a href="#">CSCvi52608</a>	CLI show aaa clients detailed command triggered SSH to crash
<a href="#">CSCvi65958</a>	Standby RP crashes due to shortage of memory when running OSPF
<a href="#">CSCvi70145</a>	ASR1k   Segmentation fault in dhcp_sip process
<a href="#">CSCvi72480</a>	Memory leak seen when having same src mac -address with different src ip address
<a href="#">CSCvi79674</a>	CPP 0 failure Stuck Thread resulting in Unexpected Reboot
<a href="#">CSCvi83306</a>	Crash with IOSXE-WATCHDOG: Process = IPv6 RIB Event Handler
<a href="#">CSCvi83419</a>	Router crash when removing route-target and with hard clear
<a href="#">CSCvi92528</a>	ZBFW HA: Configuring redundancy RII on virtual template auto-tunnel does not take effect
<a href="#">CSCvi96450</a>	Router crashed when lsp-mtu is changed
<a href="#">CSCvj02910</a>	Reload removing ipv6 VRRP group
<a href="#">CSCvj22537</a>	Standby switch crashes when flow-exporter destination configured with Hostname
<a href="#">CSCvj31705</a>	ASR1k unexpected crash when appNav holds a stale pointer.
<a href="#">CSCvj37835</a>	EPA-1X100GE/CPAK-100G-SR4 stays in a down/down state after a reset.



Caveat ID Number	Description
<a href="#">CSCvj43156</a>	Crash in XDR process: "fib_rp_table_broker_encode_buf.size <= FIB_RP_TABLE_BROKER_ENC_BUF_SZ"
<a href="#">CSCvj44507</a>	16.10 ASR1K: IOSd crash @SSS Manager during sessions teardown
<a href="#">CSCvj45781</a>	QFP CGM Memory depletion during ISG session churn
<a href="#">CSCvj68607</a>	ASR1K crash in tplus_handle_req_timeout
<a href="#">CSCvj71845</a>	Backup path incorrect for ring topology where high ISIS cost is configured on 1 link.
<a href="#">CSCvj76285</a>	Snmp v2 breaks due to Authentication failure, bad community string, 16.03.06
<a href="#">CSCvj76316</a>	subscriber template not cleared after idle time exceed as well as traceback generation
<a href="#">CSCvj77688</a>	Shimming have some issue over selecting idb
<a href="#">CSCvj78551</a>	ASR1001X @incorrect traffic statistics reported of port-channel sub interface using SNMP.
<a href="#">CSCvj78647</a>	mtu cli is disappeared from show run when interface dialer sh/no shu
<a href="#">CSCvj79542</a>	Missing interface source template model
<a href="#">CSCvj79694</a>	sgt-map gets cleared for some of the end points for unknown reason
<a href="#">CSCvj83551</a>	SISF crash in IPV6 neighbor discovery packets
<a href="#">CSCvj88805</a>	ASR1K - No kernel/coredump generated with watchdog reload event
<a href="#">CSCvj90145</a>	Zero Touch Provisioning (ZTP) fails to apply certain service instance configuration.
<a href="#">CSCvk07070</a>	Observing bmalloc smd leaks at OBJ_WEBAUTH_LOGOUT_URL with webauth
<a href="#">CSCvk10633</a>	bgp crash while running show command and same time bgp peer reset
<a href="#">CSCvk12253</a>	ASR1001-HX crashed due to critical software exception on operation group-object add/remove
<a href="#">CSCvk12448</a>	ESP crash due to fatal error
<a href="#">CSCvk20589</a>	SSH V2 crash
<a href="#">CSCvk23363</a>	ASR1k PWLAN: Cisco-AVPair = remote-id-tag=5 missing after roaming
<a href="#">CSCvk24143</a>	ASR1001-X crash due to free block at tty_handle
<a href="#">CSCvk26471</a>	Traffic fails after changing Copper SFP to Fiber SFP on 1GE built-in interface.
<a href="#">CSCvk45142</a>	3850 crash with smd fault on rp_0_0
<a href="#">CSCvk46664</a>	DNA Center SWIM Upgrade fails and unable to upgrade manually
<a href="#">CSCvk50734</a>	Device Tracking - Memory leak observed with IPv6 NS/NA Packets .

Caveat ID Number	Description
<a href="#">CSCvk58143</a>	500~600 secs Increase in boot time when "ip domain lookup" configured.
<a href="#">CSCvk59419</a>	Crash in xoslib code for onepk process when using yang-netconf
<a href="#">CSCvk63602</a>	WAAS Policy Configuration push may caused AppNav Class-maps programming issue in TCAM
<a href="#">CSCvk63706</a>	ASR1000-6TGE / ASR1000-2T+20X1GE in status Unknown after Active RP3 OIR
<a href="#">CSCvk67137</a>	Crash observed on ASR1002-X @ fnf_age_recalculate_record_len with AVC performance monitor config
<a href="#">CSCvm12196</a>	Memleak (IP: RIB Alternate Preference); provides fix for CSCvk68355
<a href="#">CSCvm21219</a>	Crash on Running "show vpdn tunnel summary" command.
<a href="#">CSCvm33871</a>	ASR1K: ipv6 telnet session with vrf is failing
<a href="#">CSCvm39130</a>	16.6 and 16.9: cannot OIR harddisk on ASR1000-RP2
<a href="#">CSCvm40441</a>	CFD: PNP DNS discovery with trust pool flow uses IP address in PNP profile instead of FQDN
<a href="#">CSCvm43071</a>	[IBNS 2.0] aaa-available event is not being triggered when using authentication/authorization list
<a href="#">CSCvm44488</a>	ASR1001-HX 10GE SFP+ ports may operate as 1000Mbps
<a href="#">CSCvm50139</a>	2nd phase fix for CSCvk45142
<a href="#">CSCvm51739</a>	SNMP v3 discloses password in the parser warning syslog trap
<a href="#">CSCvm55465</a>	BGP updates missing ISIS advertising-bits led to LDP label purge on peer.
<a href="#">CSCvm57817</a>	ASR1002-X crash due to ccp_cp_svr going into lockdown state.
<a href="#">CSCvm59172</a>	"autoroute announce" and "loose" path not working on intra-area TE tunnel
<a href="#">CSCvm76464</a>	ASR1k crash due to QoS in case of 4k subscribers per subinterface
<a href="#">CSCvm95929</a>	100FX OPNEXT SFP does not come up on ASR1001-X
<a href="#">CSCvn02171</a>	POLARIS: HOLE is not created when 'acl default passthrough' configured

### Open Caveats—Cisco IOS XE Everest 16.6.5

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

Caveat ID Number	Description
<a href="#">CSCus13106</a>	IOS-XE - RSA key-gen: Error in generating keys:no available resources
<a href="#">CSCvd65197</a>	IOSd crashed when dialer disconnect the ISDN call

Caveat ID Number	Description
<a href="#">CSCve32648</a>	Traceback@cpp_mlp_bundle_stats_query_all_cmn on fp reload
<a href="#">CSCve54914</a>	NDSSO vrf ha table to be populated correctly
<a href="#">CSCve78446</a>	[1661]- Switch number is missing in stack merged logs.
<a href="#">CSCvg23820</a>	CTS PAC download fails with VRF config on non-management interface
<a href="#">CSCvg77859</a>	ASR1k: 16.5 and later: tracelogs/punt_debug.log* missing when punt keepalive timeout / crash occurs
<a href="#">CSCvh57657</a>	NAT MIB not populated when using traditional NAT
<a href="#">CSCvh59431</a>	Byte counters for physical interface and subinterface don't match
<a href="#">CSCvh66584</a>	ESP100: wrong show platform software ipsec fp active encryption-processor 1 registers result
<a href="#">CSCvi36351</a>	standby rp crash on removing member link from port-channel
<a href="#">CSCvj12370</a>	ASR1002-X router crashed in cpp_qm_event_collapse_hl_node
<a href="#">CSCvj79547</a>	Complete content for interface templates
<a href="#">CSCvj89047</a>	Quake-sessmgrd Huge Mem Leak After Master switchover
<a href="#">CSCvk15062</a>	Modification to ZBFW access-lists do not reflect in TCAM
<a href="#">CSCvk22449</a>	BGP Traceback/Crash seen with 20k IPv4 BGP scale after reload/clearing bgp
<a href="#">CSCvk32822</a>	QoS stats process crash
<a href="#">CSCvk63782</a>	Quick RP3 recovery after the Punt Path XAUI link goes down
<a href="#">CSCvk75838</a>	netconf/yang or telemetry retrieval of /trustsec-state/cts-rolebased-policies breaks
<a href="#">CSCvm06775</a>	ATOM CW is not exchanged after node reload
<a href="#">CSCvm25921</a>	Signaling interface inactive on "show snmp mib ifmib ifindex de" on IOS 16.6.3
<a href="#">CSCvm42441</a>	ASR 1001-X reboots when clearing ip nat translations
<a href="#">CSCvm51112</a>	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys
<a href="#">CSCvm56670</a>	ACL dropping packets after updating it - %CPPEXMEM-3-NOMEM
<a href="#">CSCvm70471</a>	'hw-module subslot 0/2 reload' CLI does not activate the container after harddisk format
<a href="#">CSCvm76452</a>	IPSec background crash while sending SNMP trap
<a href="#">CSCvm78822</a>	config-sync failure 'aaa authorization commands'
<a href="#">CSCvm84742</a>	Crash after issuing "no ip dhcp snooping VLAN <VLAN #>" command
<a href="#">CSCvm96960</a>	ASR1K throwing: ETH_SPA_MAC-3-SPI4_ERROR: SIP0/1: Marvel MAC

Caveat ID Number	Description
<a href="#">CSCvn00277</a>	ASR 1006-X RP2 : Standby RP Crashed after running command "license boot level adventerprise"
<a href="#">CSCvn02419</a>	Router crash occurs while running Dell software update
<a href="#">CSCvn07478</a>	Ethernet FRR switchover takes more than 200ms on EPA10 and EPA100 if remote Rx fiber is pulled
<a href="#">CSCvn17655</a>	Removing ip flow monitor from an interface caused ESP crash
<a href="#">CSCvn19382</a>	Crash after comparing tunnel FIB entries
<a href="#">CSCvn23732</a>	show interface output reports incorrect bandwidth
<a href="#">CSCvn23906</a>	DHCP Server sends Renew ACKs to Clients with 00:00:00:00:00:00 MAC in L2 frame
<a href="#">CSCvn24569</a>	No MPLS label after SSO with ISIS segment routing
<a href="#">CSCvn30280</a>	ASR1000 Flexible NerFlow ucode crash
<a href="#">CSCvn37237</a>	ASR1002-HX crashed after about 40G traffic is transmitted over it
<a href="#">CSCvn38313</a>	Traceback: crash on load/store transfer error
<a href="#">CSCvn44891</a>	Policy-map on GEC suspended even if total required BW is below interface BW
<a href="#">CSCvn47929</a>	ASR1k crashes when reconfiguring netflow, getting FMFP-3-OBJ_DWNLD_TO_DP_FAILED logs
<a href="#">CSCvn49372</a>	Unexpected flood in case of MVPN profile 0 with BiDir in VRF
<a href="#">CSCvn49911</a>	Stuck thread crash after executing 'clear ip nat translation vrf <VRFNAME>'

## Caveats in Cisco IOS XE Everest Release 16.6.4

### Open Caveats—Cisco IOS XE Everest 16.6.4

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

Caveat ID Number	Description
<a href="#">CSCuy75886</a>	Lots of chunk memory leak about SNMP SMALL CHUN and SNMP MEDIUM CHU
<a href="#">CSCvb72829</a>	show ipv6 neighbor statistics not updated post RPSO for entries synced
<a href="#">CSCvc73961</a>	OSPF BGP LS: When seg mpls is disabled on the nbr, the unnumbered links not withdrawn from LSLIB.
<a href="#">CSCvd20054</a>	Polaris 16.4: Traceback @mpls_ldp_cfg_interface while enabling isis
<a href="#">CSCvd65197</a>	IOSd crashed when dialer disconnect the ISDN call
<a href="#">CSCve01479</a>	e2e ping is failed after configuring profiles qos-de and aaaauth1

Caveat ID Number	Description
<a href="#">CSCve05486</a>	ISDN switch-type configure issue for BRI leased-line
<a href="#">CSCve12319</a>	ISIS SRTE: When one of ECMP path for prefix is not enabled for SR, SRTE tunnel does not come up.
<a href="#">CSCve16269</a>	IKEv2 CoA does not work with ISE
<a href="#">CSCve32648</a>	Traceback@cpp_mlp_bundle_stats_query_all_cmn on fp reload
<a href="#">CSCve39101</a>	OSPF SROAM: “%ARP-3-ARPADJ: Internal software error during updating CEF Adjacency” when box comes up
<a href="#">CSCve39572</a>	BGP net should have inlabel if bgp mpls-local-label is configured
<a href="#">CSCve54914</a>	NDSSO vrf ha table to be populated correctly
<a href="#">CSCve78446</a>	[1661]- Switch number is missing in stack merged logs.
<a href="#">CSCve96308</a>	Observing memory leak in AAA_MALLOC_LITE
<a href="#">CSCvf22725</a>	OSPF SR/SIDredistribute: when SID configured > avbl SRGB, that sid should not be advertised in EPL.
<a href="#">CSCvf28564</a>	Show details soft key is not functioning in a conference call
<a href="#">CSCvf28977</a>	ESP Crash with FP Switchover
<a href="#">CSCvf34848</a>	License synchronized to SSMS despite being removed from SL Portal
<a href="#">CSCvf37923</a>	Crash due to Stack overflow
<a href="#">CSCvf50723</a>	Packet-tracer error message % Error: Failed to collect packet info
<a href="#">CSCvf51917</a>	dns-a-override CLI not working due to breakage since 16.4 IOS
<a href="#">CSCvf76436</a>	Combination of add-path, backup path and advertised-to leaves is not giving expected netconf values
<a href="#">CSCvf95739</a>	Remove “dns-vrf-aware” CLI and make DNS vrf aware by default.
<a href="#">CSCvg23363</a>	Virtual-access interface MTU wrongly set when using ipsec ipv4
<a href="#">CSCvg23820</a>	CTS PAC download fails with VRF config on non-management interface
<a href="#">CSCvg29105</a>	asr1k: Gec 5 tuple feautre not working in IOS-XE releases post 16.4.1
<a href="#">CSCvg77859</a>	ASR1k: 16.5 and later: tracelogs/punt_debug.log* missing when punt keepalive timeout / crash occurs
<a href="#">CSCvg77924</a>	FRR feature not working in ESP100 & ESP200
<a href="#">CSCvg81772</a>	VRF import config missing ipv4 unicast after no router bgp
<a href="#">CSCvh49364</a>	PFRv3 Incorrect time-stamp in traffic-class router change history

Caveat ID Number	Description
<a href="#">CSCvh57657</a>	NAT MIB not populated when using traditional NAT
<a href="#">CSCvh66584</a>	ESP100: wrong show platform software ipsec fp active encryption-processor 1 registers result
<a href="#">CSCvh67422</a>	IPSLA ICMP-jitter stats reporting some of the received packets as lost.
<a href="#">CSCvh85031</a>	Branch MC crashed@cent_send_syslog_on_violated_policies under stress test
<a href="#">CSCvi06417</a>	SIP stack matching the dial-peer when processing NOTIFY message causing call routing issues
<a href="#">CSCvi10089</a>	EXEC process stuck vty line where “no exec” is set
<a href="#">CSCvi15955</a>	Call failure after Bye-Also blind transfer from CUE requires failure indication
<a href="#">CSCvi36351</a>	standby rp crash on removing member link from port-channel
<a href="#">CSCvi54372</a>	%NHRP-3-PAKERROR loop detected Pak sanity failure
<a href="#">CSCvi70145</a>	ASR1k Segmentation fault in dhcp_sip process
<a href="#">CSCvi72480</a>	Memory leak seen when having same src mac -address with different src ip address
<a href="#">CSCvi83419</a>	Router crash when removing route-target and with hard clear
<a href="#">CSCvi86093</a>	Switch reloads when kron job scheduled in 0 minutes
<a href="#">CSCvi90729</a>	IKEv2 CoA does not work with ISE (coa-push=TRUE instead of true)
<a href="#">CSCvi92505</a>	MWI info is not preserved on CME SIP phone after a reboot for unsolicited method
<a href="#">CSCvi93972</a>	IWAN versions with prefix tracking only allow prefix splitting for internet and not enterprise
<a href="#">CSCvi97233</a>	CME radius accounting does not generate complete called number for EA
<a href="#">CSCvi97572</a>	ASR 1K Running 16.6.x Code Experiences CPP Crash When Processing Packet Through NBAR / MTP
<a href="#">CSCvj08942</a>	SNMPwalk of cipslaPercentileLatestStatsTable does not give all the cipslaPercentileTypeVar types
<a href="#">CSCvj09305</a>	slow convergence when configuring ha-mode sso for IPv6 peers
<a href="#">CSCvj11263</a>	nbar2: resource exhaustion might occur in FNF with vmware-vsphere and flow monitors
<a href="#">CSCvj15262</a>	ASR1k with stateful nat conf, mapping ID got locked after vrf delete
<a href="#">CSCvj35317</a>	Ti-LFA Repair Path is not Loop-Free
<a href="#">CSCvj44615</a>	Ringback stops on REFER based xfer when CUBE receives 180 followed by 183 w/SDP media change

Caveat ID Number	Description
<a href="#">CSCvj45781</a>	QFP CGM Memory depletion during ISG session churn
<a href="#">CSCvj47270</a>	IKEv2 sessions cannot establish due to CAC leakage
<a href="#">CSCvj51510</a>	Crash after service-policy APPNAV change on WAAS instance
<a href="#">CSCvj51929</a>	Out of order ESP packets triggering IPSEC replay error message
<a href="#">CSCvj57453</a>	OSPF TILFA: tilfa repair path computation ALGORITHM fails with reason code BAD FH NBR
<a href="#">CSCvj57487</a>	OSPF TILFA: tilfa repair path computation ALGORITHM uses incorrect firsthop router-id
<a href="#">CSCvj59152</a>	Evaluation of all for May CPU Side-Channel Information Disclosure Vulnerabilities
<a href="#">CSCvj60144</a>	OSPF TILFA: tilfa ALGORITHM fails to get repair node n-sid label when vertex is beyond PGW node
<a href="#">CSCvj64493</a>	Standby switch crash when removing kron scheduler command
<a href="#">CSCvj66204</a>	initial SNMP traps take agent-addr from shutdown interface
<a href="#">CSCvj67623</a>	DNS ALG will not work when trying to match specific destination hosts
<a href="#">CSCvj68607</a>	ASR1K crash in tplus_handle_req_timeout
<a href="#">CSCvj70568</a>	FlexVPN DHCP entries not flushing for ikev2 timed out reconnect sessions
<a href="#">CSCvj72854</a>	Router crash due to NHRP process Segmentation fault(11)
<a href="#">CSCvj74888</a>	Kernel OOPS reporting ECC error
<a href="#">CSCvj75853</a>	Device crash after execute command “show lldp neighbor [int] detail”
<a href="#">CSCvj76285</a>	Snmp v2 breaks due to Authentication failure, bad community string, 16.03.06
<a href="#">CSCvj76316</a>	subscriber template not cleared after idle time exceed as well as traceback generation
<a href="#">CSCvj76662</a>	GetVPN TBAR failure does not generate syslogs
<a href="#">CSCvj77638</a>	“Disabled” counter increase after enter “interface Async1”
<a href="#">CSCvj78876</a>	CUBE: FPI Hung Sessions and Provisioning Failures observed in Standby CUBE
<a href="#">CSCvj79019</a>	ASR: SCH Diagnostic Signature Feature is missing in IOS XE 16.x releases
<a href="#">CSCvj81382</a>	IPv6 AAA Prefix Support for 3rd party PPP clients no password for -dhcipv6 Access-Request
<a href="#">CSCvj82095</a>	nbar mismatch cisco video traffic
<a href="#">CSCvj83551</a>	SISF crash in IPV6 neighbor discovery packets

Caveat ID Number	Description
<a href="#">CSCvj84104</a>	PLR channel is not muted for some time
<a href="#">CSCvj84158</a>	PfRv3: BR May Crash due to Channel Creation/Modification and Next-Hop State
<a href="#">CSCvj88805</a>	ASR1K - No kernel/coredump generated with watchdog reload event
<a href="#">CSCvj89345</a>	AVC license should be activated only in case of smart licensing model
<a href="#">CSCvj90089</a>	Crash while doing a conference call

#### Resolved Caveats—Cisco IOS XE Everest 16.6.4

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

Caveat ID Number	Description
<a href="#">CSCsd58148</a>	%SEC_LOGIN-4-LOGIN_FAILED does not show username in [user: ]
<a href="#">CSCut56684</a>	Appnav Passthrough Counter goes to infinite
<a href="#">CSCuv14856</a>	WATCHDOG timeout crash during IPSEC phase 2
<a href="#">CSCuv90519</a>	Map does not get updated with socket change on local address change
<a href="#">CSCuw90084</a>	DS: Download should print alerts in case of unresolved variables
<a href="#">CSCux20847</a>	R0/0: ASR1002-X kernel: bullseye_i2c_master_xfer Error Repeats Every Hour
<a href="#">CSCvb34443</a>	IKEv2 fragmentation not working with aes-gcm encryption - hmac failure
<a href="#">CSCvb69966</a>	Memory leak under LLDP Protocol process
<a href="#">CSCvb88867</a>	Excess BGP Traps Generated after upgrade
<a href="#">CSCvd14310</a>	IP Tunnels: Overlapping Loopback Interface Causes Incorrect Forwarding Decision with AppNav and PfR
<a href="#">CSCvd21937</a>	Unknown unicast packet need be filtered before to BDI
<a href="#">CSCvd81374</a>	Orthrus: FP 100 crashed when sending traffic around 55 MPPS with pkts size 64 byte
<a href="#">CSCvd90410</a>	Router loses RSA keys upon boot with private-config encryption and config archive enabled
<a href="#">CSCve11959</a>	Memory leak occurs on DHCP client
<a href="#">CSCve41775</a>	crash over CCSIP_SPI_CONTROL process due to null pointer / segmentation fault
<a href="#">CSCve55004</a>	OSPF GIR BASE: not all repair paths calculated for AS ext routes when routes rxd with maxmetric
<a href="#">CSCve61143</a>	CME SIP sip-ua do not send registration request when vrf forwarding is enabled.
<a href="#">CSCvf05864</a>	BGP RR changes tunnel parameters for bgp evpn route type 3



Caveat ID Number	Description
<a href="#">CSCvf06123</a>	Route-map not checked when packet is flowing from OUT to IN with Static NAT
<a href="#">CSCvf07153</a>	SIP Date header format not in GMT Format
<a href="#">CSCvf07576</a>	router reloaded when doing show BGP RT filter routes
<a href="#">CSCvf19460</a>	CTS Pac download fails with ISE reachability through loopback interface over vrf
<a href="#">CSCvf23485</a>	DS: Increase the size of command and prompt strings
<a href="#">CSCvf26916</a>	RTCP/RTP based Media Inactivity timers for MGCP GW do not work in newer releases
<a href="#">CSCvf34608</a>	Excessive Reflector Tracelogs
<a href="#">CSCvf49126</a>	Stub is not leaking the network as expected
<a href="#">CSCvf51773</a>	NHRP redirect overriding routing table
<a href="#">CSCvf53053</a>	Crash when issuing no dspfarm profile x stuck on DOWN_PENDING state.
<a href="#">CSCvf57090</a>	CUBE automatically considers re-INVITE with a=silenceSupp:off - - - as fax call
<a href="#">CSCvf66030</a>	OSPF SR: When SRGB range is changed, mapping server entries do not get re-installed.
<a href="#">CSCvf66860</a>	IOS crash in SOCK TCP Test Server process
<a href="#">CSCvf70383</a>	Crash in SDP Passthru when T.38 as 1st mline in mid-call SDP
<a href="#">CSCvf80363</a>	rotate nginx access/error log files
<a href="#">CSCvf84528</a>	False indication of RTP port leak on ISR4K & Neptune
<a href="#">CSCvf88705</a>	Malformed GETVPN message %GDOI-4-COOP_KS_UNAUTH
<a href="#">CSCvf89894</a>	GETVPN // Primary KS sending rekey first to GMs and then to Secondary KS via scheduled rekey.
<a href="#">CSCvf96009</a>	OSPF SR: When loopback is configured with prefix suppression, EPL should be withdrawn
<a href="#">CSCvf96294</a>	MIB counter for IPsec tunnels does not decrement under high tunnel scale and churn
<a href="#">CSCvf97908</a>	When NSSA ASBR is reloaded, ECMP to ext routes not installed in other routers.
<a href="#">CSCvf98378</a>	IOSXE_INFRA-6-PROCPATH_CLIENT_HOG: IOS shim client 'fman stats bipc' has taken 278 msec
<a href="#">CSCvg01774</a>	OSPF SSPF: when seg area is disabled and enabled, mapping server EPL entries not re-generated.
<a href="#">CSCvg03444</a>	Hub MC continues to send EIGRP SAF hellos after adjacency removed
<a href="#">CSCvg05172</a>	Crash in VOIP media loop detection

Caveat ID Number	Description
<a href="#">CSCvg05452</a>	IOS-XE router crash from memory corruption during CCB cleanup
<a href="#">CSCvg06142</a>	'ipsm Tunnel Entry' and 'Crypto IKMP' memory leak due to IKE tunnel entry not deleted
<a href="#">CSCvg06428</a>	After reloading the ELC40 linecards are not coming up online
<a href="#">CSCvg08471</a>	OSPF; process ospf segmentation fault when shut and no shut is performed in active RP.
<a href="#">CSCvg08768</a>	OSPF BGP LS: After fail over, error msg seen: %LSLIB-4-EOD: Producer OSPF-0x0 did not send EOD
<a href="#">CSCvg12605</a>	Corrupted NOTIFY leads to %CRYPTO-4-IKMP_BAD_MESSAGE, stale ISAKMP SA and traffic failure
<a href="#">CSCvg16234</a>	ISR receives a control packet (CDP) with a CMD tag it should process it, not drop it
<a href="#">CSCvg18094</a>	GETVPN: show crypto gdoi ks member summary missing last octet in IP address
<a href="#">CSCvg19259</a>	MPLSoFlexVPN: Hub does not forward resolution req when default route is advertised to spokes
<a href="#">CSCvg25874</a>	Toggling the switchport then default the interface, load-interval config reapplied
<a href="#">CSCvg30133</a>	EPAs failed to boot in IOS, with multiple ASR1000-MIP100 installed.
<a href="#">CSCvg30991</a>	IOS-XE routers: Memory leak observed on process ivr: peer_item_t in AFW_application_process
<a href="#">CSCvg32701</a>	Night-Service fails if it overlaps with FAC codes
<a href="#">CSCvg32858</a>	Snort control plane connectivity with Mgmt-intf is broken
<a href="#">CSCvg33454</a>	Pass load balancing information in IP header to container
<a href="#">CSCvg34986</a>	Media recording on IOS-XE does not work if a refer is received immediately after the call is answered
<a href="#">CSCvg36598</a>	ISAKMP Fails When Multiple HSRP tunnel/SVTI Interfaces Configured
<a href="#">CSCvg39082</a>	Crash after TCP session timeout
<a href="#">CSCvg41950</a>	Cisco IOS XE Software Diagnostic Shell Path Traversal Vulnerability
<a href="#">CSCvg43263</a>	when shutting interface with no isis adjacency, local micro-loop avoidance blocks FRR recalculation
<a href="#">CSCvg44135</a>	OSPF SRTE: prefix information is not provided to SRTE when it is learnt via mapping server.
<a href="#">CSCvg45950</a>	packet drop seen intermittently if 40G traffic sent via cts interface
<a href="#">CSCvg47453</a>	Default route redistributed into RIP from EIGRP is not removed from RIP database

Caveat ID Number	Description
<a href="#">CSCvg48470</a>	ISIS 11-12 redistribution prefix doesnt get redistributed till clear isis rib redistribution is done
<a href="#">CSCvg51358</a>	DHCPNAK is not sent in roaming scenario.
<a href="#">CSCvg53159</a>	%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch
<a href="#">CSCvg54267</a>	CDP Protocol can run device out of memory
<a href="#">CSCvg56088</a>	Getting "HA Module DSP_MSP reported CALL_MODIFY RECREATE failure" in CUBE HA.
<a href="#">CSCvg56110</a>	Error and pending objects when mma policy flap with egress monitor for multi-VRF case
<a href="#">CSCvg58096</a>	Increase of dampening penalty on route refresh
<a href="#">CSCvg58599</a>	Syslog: Logging host is truncating lines causing debug output to be cutoff in the middle of a msg
<a href="#">CSCvg59604</a>	Cube crashes intermittently multiple times within every two days.
<a href="#">CSCvg67028</a>	VRF deletion status <being deleted> after removing the RD
<a href="#">CSCvg67820</a>	HIGH CPU observation on FMAN RP ESS EVENT TRACING
<a href="#">CSCvg68391</a>	ISIS SR: When seg mpls is shut globally, ISIS SID entries not withdrawn from the entire network.
<a href="#">CSCvg71944</a>	OSPF SR: When loopback is defined as /24 address, EPL should not be sent for the prefix.
<a href="#">CSCvg75315</a>	ASR1K BGP scanner crash when change VRF and BGP configuration
<a href="#">CSCvg75419</a>	ISIS SRTE: Explicit SRTE keeps flapping when ISIS is not the winning route in the RIB
<a href="#">CSCvg76664</a>	OSPF SSPF: With SRTE tunnel, constrained bind of SID0 uses invalid old repair path in some cases
<a href="#">CSCvg76990</a>	Missing LSP sending after configuration change
<a href="#">CSCvg77128</a>	ASR1009-X FAN SN in show inventory display incorrectly after replace the FAN and do RP switchover
<a href="#">CSCvg82855</a>	OSPF SSPF: mapping-server strict SID is processed by images which are not strict spf capable
<a href="#">CSCvg84181</a>	“CLID restrict” on outbound leg is setting “Privacy=Full” on inbound leg
<a href="#">CSCvg85146</a>	OSPFv2 Encoding for local-id in LLS needs to be fixed
<a href="#">CSCvg85879</a>	BGP sets the wrong Local Preference for routes validated by RPKI server

Caveat ID Number	Description
<a href="#">CSCvg89163</a>	CUBE does not acknowledge Session-Expires header in UPDATE
<a href="#">CSCvg94978</a>	CUBE Router crashed - Critical software exception, Process = CCH323_CT
<a href="#">CSCvg96936</a>	IOS-XE : PAT entry using the same port which is configured for static NAT
<a href="#">CSCvg97010</a>	load-balance advanced moving traffic to fallback path when primary path are not over utilized
<a href="#">CSCvg99559</a>	OSPF SSPF/TILFA: TILFA ECMP tunnels are not created when the last segment is adjacency sid.
<a href="#">CSCvh00630</a>	ISRV/QOS - service-policy defined in bootstrap config may not be applied
<a href="#">CSCvh01652</a>	Multicast IPSLA UDP Jitter throws Socket open error if vrf interface is configured on responder
<a href="#">CSCvh02109</a>	WSMA: Server responds with HTTP 404 on wsma-exec with http transport profile
<a href="#">CSCvh03359</a>	EIGRP network statement reappearing after reboot
<a href="#">CSCvh03788</a>	EIGRP Name mode Summary route is not being apply on Virtual-Access on HUB
<a href="#">CSCvh05611</a>	IOSd crash while applying dial peer configuration
<a href="#">CSCvh06249</a>	Crash when receiving EVPN NLRI with incorrect NLRI length field value
<a href="#">CSCvh09334</a>	SDA-IPV6::SISF traceback @ar_relay_create_entry - L2 Binding tbl entry insertion failed
<a href="#">CSCvh09525</a>	CME: BLF monitor function fails intermittently with TCP connection
<a href="#">CSCvh10607</a>	ISG: IETF-Disc-Cause = 0 if DHCP SIP disconnect
<a href="#">CSCvh14715</a>	CVLA crash on memory merge scan task
<a href="#">CSCvh15336</a>	OSPF SSPF: ECMP combination of SRTE tunnels and MPLS-TE tunnels does not work properly sometimes.
<a href="#">CSCvh15484</a>	ISIS SR: When the SRGB range is increased, the local SIDs which are in new range are re-installed.
<a href="#">CSCvh18001</a>	Crash due to race condition caused by IOS radioactive trace code
<a href="#">CSCvh21564</a>	AAA Attribute list leak in Polaris 16.6.2
<a href="#">CSCvh21909</a>	LISP: Overlapping prefix causes “probe-down” for map-cache entry
<a href="#">CSCvh21973</a>	QFP crashed to while sending oversubscribe traffic
<a href="#">CSCvh22278</a>	OSPF Hello timer 10sec is not applied in network type non-broadcast
<a href="#">CSCvh22300</a>	Update IOS XE OSPFv2 ELL private TLVs to IANA codepoints

Caveat ID Number	Description
<a href="#">CSCvh22589</a>	Preempt timer does not work due to old HSRP Hello packet get just after interface up
<a href="#">CSCvh22775</a>	SIP40 in slot 5 of ASR1013 when inserted ESP-200 in F1 by replacing ESP-40, showed ESI lock failure
<a href="#">CSCvh24315</a>	Memory leak for CCSIP_TCP_SOCKET and CCSIP_UDP_SOCKET on CUBE
<a href="#">CSCvh25624</a>	ISIS SR: When seg mpls is shut under ISIS, sid entries not cleared in the local router.
<a href="#">CSCvh26072</a>	EIGRP SAF Adjacency does not form with /31 mask
<a href="#">CSCvh26560</a>	ESP crashes with high scale QoS configuration
<a href="#">CSCvh28323</a>	ASR1002HX FP Crash post LNS path switchover
<a href="#">CSCvh29771</a>	Kernel crash in ASR1002-HX during LNS path switchover
<a href="#">CSCvh29821</a>	CME should send out a refer with notify_clear when night-service is manually disabled
<a href="#">CSCvh30968</a>	ISIS BGP LS: When distribute link state changed from level 1 to level 2, entries not given to BGP LS
<a href="#">CSCvh32216</a>	Sporadic Crashes Due to IPsec (during ISAKMP AAA interaction)
<a href="#">CSCvh47626</a>	"ERR: Unable to connect to domain socket tamc_tams_socket" seen continuously
<a href="#">CSCvh48085</a>	OSPF SSPF/SRTE: when we have ABR with multiple interfaces to backbone area, SPF keeps running.
<a href="#">CSCvh48610</a>	iwan router crash while updating pmi policy
<a href="#">CSCvh49600</a>	Output "sh sip-ua connections tcp tls detail" shows that CUBE has stuck connection ids.
<a href="#">CSCvh51038</a>	[168] OSPF process crash on P router when "router ospf" is unconfigured on another PE or P router
<a href="#">CSCvh53691</a>	FP reload with IMGR deregister interface
<a href="#">CSCvh53764</a>	RP Unexpected reboot when using conditional debugging with CCSIP debug
<a href="#">CSCvh54229</a>	TCAM critical limit shows incorrect value of 55 %.
<a href="#">CSCvh54672</a>	VRRP doesnt work over Port-channel L3 interface
<a href="#">CSCvh56594</a>	EIGRP offset-list still active if ACL used in offset-list is removed before offset-list
<a href="#">CSCvh57091</a>	ESP crash when flapping interface with l2tp tunnels that have qos applied to the tunnels.
<a href="#">CSCvh57108</a>	CPUHOG on QoS statistics collection for DMVPN. QoS crash with DMVPN/NHRP.
<a href="#">CSCvh57242</a>	cpp-mcpl0-ucode crash when layer 2 switching packet
<a href="#">CSCvh57340</a>	DMVPN: Crypto session stuck into UP-IDLE status after reconfiguring tunnel

Caveat ID Number	Description
<a href="#">CSCvh58702</a>	Router crashes after interface flap where sessions get moved from one interface to another
<a href="#">CSCvh58909</a>	OSPFv3 cost calculation not correct in some specific topology
<a href="#">CSCvh61453</a>	NULL remote_hostname from LAC
<a href="#">CSCvh62532</a>	System reload when clearing cts pac
<a href="#">CSCvh62615</a>	There is junk entry in route-import table on branch when shutdown/no shutdown WAN interface
<a href="#">CSCvh62925</a>	ASR1001-HX log alarm “Install interface_10g license to unshut the port”
<a href="#">CSCvh63932</a>	Noisy debugs in “periodic” tracelog
<a href="#">CSCvh64729</a>	FP crash @cpp_qm_create_queue while adding fair-queue
<a href="#">CSCvh66033</a>	IKEv2 - Crash with segmentation fault when debugs crypto ikev2 are enabled
<a href="#">CSCvh66642</a>	uIDB leaks at the DMVPN hub if the route to remote NBMA is not learned
<a href="#">CSCvh68228</a>	CUBE Unsolicited NOTIFY returns 481 Subscription does not exist
<a href="#">CSCvh70297</a>	Redundancy Mode None does not Sync
<a href="#">CSCvh70356</a>	ASR1K - ECMP load-balance w/ DPI L2TP Tunnel visibility and QoS may generate ucode crash
<a href="#">CSCvh71539</a>	Command “show aaa servers” reloads the switch
<a href="#">CSCvh71856</a>	IOSd crash when enabling dot1q in a port-channel sub-interface
<a href="#">CSCvh72700</a>	CME: GUI user page does not load correctly. It is showing “View Window”
<a href="#">CSCvh73805</a>	Explicit SRTE tunnels are not come up when a prefix is redistributed between levels
<a href="#">CSCvh75132</a>	CPP crash stuck thread detected multikey_hash_replace_int
<a href="#">CSCvh77733</a>	RR does not send VPNv4 routes to peer
<a href="#">CSCvh79067</a>	Call Park with standard FAC fails if phones extensions overlap with FAC codes
<a href="#">CSCvh79942</a>	Chunk corruption crash related to PNP or Guestshell
<a href="#">CSCvh82112</a>	Polaris Routers - Memory leak under process RECMSPAPP in IOSd
<a href="#">CSCvh83215</a>	IOS-XE Voice NIM/PVDM Service-Engine Admin Down leads to one-way audio
<a href="#">CSCvh85788</a>	Local LAN-only prefix present in master route-import table but not present in site prefix DB
<a href="#">CSCvh88330</a>	VAI Leaks with IKEv1 DVTI

Caveat ID Number	Description
<a href="#">CSCvh88975</a>	performance-monitor does not report classification after tunnel shutdown
<a href="#">CSCvh91443</a>	ISR4k Crashed due to CPUHOG Net background.
<a href="#">CSCvh92130</a>	downloaded policies hit by traffics were all gone after the second SSO
<a href="#">CSCvh92378</a>	High CPU utlization with presence feature when reset is issued under voice register global
<a href="#">CSCvh93071</a>	Redistributing connected route with AIGP attribute is being continuously readvertised
<a href="#">CSCvh95376</a>	ASR1k reloaded after IPv4 RR stress test
<a href="#">CSCvh96542</a>	CCSIP_SPI_CONTROL holding memory increasing
<a href="#">CSCvh96821</a>	ASR1004 started relaying clients DHCP Discover messages to DHCP Server with the wrong IP address
<a href="#">CSCvh97691</a>	tacacs-server is missing keyword “key” in argument/option available
<a href="#">CSCvh97923</a>	Erroneous fan failure indication on some units - Speed Racer (ASR1001-HX)
<a href="#">CSCvh99576</a>	LACP Rate defaults to fast with no way to change it to normal
<a href="#">CSCvh99651</a>	AAA-Proxy errors in dmiauthd tracelogs
<a href="#">CSCvh99949</a>	Options Keepalive not triggered on applying profile to dial-peer
<a href="#">CSCvi01558</a>	iBGP dynamic peer using TTL 1
<a href="#">CSCvi01650</a>	SIP Out-of-Dialog OPTIONS Ping Group Shows Dial-Peers Marked as None
<a href="#">CSCvi01745</a>	cpp_cp_svr crashes, causing reload
<a href="#">CSCvi01805</a>	Router with SIP traffic crashes at ccsip_free_kpml_info
<a href="#">CSCvi02816</a>	ZBF not able to identify the WAAS optimized flow and drops ACK
<a href="#">CSCvi03339</a>	[ECA-SIT] IOSd crash seen on xTR with baseline @ sisf_macdb_get_vlanid
<a href="#">CSCvi04666</a>	ISIS SRTE: SRTE tunnel not created due to R-flag set
<a href="#">CSCvi05126</a>	ISAKMP Notification messages carry unnecessary data
<a href="#">CSCvi05408</a>	Memory leak due to asnl
<a href="#">CSCvi06312</a>	Subsystem stopped: ios-emul-oper-db due to bgp table issue
<a href="#">CSCvi06357</a>	config issue after remove Standby RP and insert it into active slot
<a href="#">CSCvi06480</a>	OSPF SSPF: EPL not sent for secondary addresses on loopback interfaces.
<a href="#">CSCvi06897</a>	dialpeer matching for inbound SIP profile fails with VRFs
<a href="#">CSCvi07387</a>	ip dhcp excluded-address deletion issues via netconf

Caveat ID Number	Description
CSCvi08933	Crash processing MMA punt records
CSCvi10166	ASR1009-X/RP2:power supplies are seen as ASR1000X-FAN and Insufficient number of power supplies (0)
CSCvi11065	Router cpp_cp_svr process crashes at cpp_qm_event_parent_event_create
CSCvi11123	FMFP-3-OBJ_DWNLD_TO_DP_FAILED error after modifying QoS policy
CSCvi11665	Virtual-service guest IP accepts broadcast address
CSCvi11970	Abnormal output for show pnp tech-support
CSCvi12657	BQS pending deferred is stuck
CSCvi13062	FP cpp_cp_svr crash @cpp_bqs_srt_yoda_place_child
CSCvi14656	Loss TCA is not generated for traffic with DSCP0 when 0-SLA enabled
CSCvi14745	EPA-10X10GE or EPA-18X1GE - Memory leak with input mac-address accounting
CSCvi15950	DTMF fails when mid-call renegotiation changes DTMF method
CSCvi16306	Cube sends reinvite with annexb=yes even when it receives annexb=no
CSCvi16454	Router crash due to PuntInject Keepalive Process - kmalloc failures
CSCvi20882	Netconf IP-SLA udp-jitter case missing leaf codec
CSCvi21288	PFRv3 RC FIA is not enabled on interfaces with one of sub-interface with xconnect config
CSCvi21353	ASR1000X-AC-1100W PEM status displayed as "Unknown" in CCO-16.06.02 on 6X chassis
CSCvi23169	ASR1006-X EPA card input errors
CSCvi24515	IOS-XE - FTP closing connection as NAT device does not process the 230 reply message
CSCvi26061	RP crash @policymap_associated_to_multiple_instances
CSCvi26398	“%LISP-4-LOCAL_EID_RLOC_INCONSISTENCY” should be suppressed in SDA context
CSCvi27958	MIP100 get struck in disconnecting state on FP reload
CSCvi28362	Unexpected metric value for route redistribution from BGP to OSPF
CSCvi28746	ASR1k “add-route” does not work with “ip nat outside static” statement under VRF
CSCvi31038	Interface on ASR1001-X will become down/down after shut/no shut
CSCvi32156	Router crashes when DMVPN tunnel moves access ports



Caveat ID Number	Description
<a href="#">CSCvi34260</a>	16.8.1: dot1x Clients stops responding ( ping to clinet IP fails) after SSO
<a href="#">CSCvi35143</a>	Repeatedly Tracebacks seen: %INFRA-3-INVALID_GPM_ACCESS: Invalid GPM Load
<a href="#">CSCvi35960</a>	VRF aware CUBE fails to send OOD OPTIONS pings
<a href="#">CSCvi36290</a>	Incorrect BDI configuration state shown by NETCONF on interface creation
<a href="#">CSCvi38244</a>	IPv6 VRRP Master is using using vlan BIA MAC while sending Neighbor advertisements (NA)
<a href="#">CSCvi38391</a>	H.245 messages are not translated by NAT outside when H.323 video call is initiated from Out-2-In
<a href="#">CSCvi38916</a>	Persistent Telnet and SSH crashes when configured in 16.6.2
<a href="#">CSCvi40033</a>	802.1x authentications are failing if there was interface template config applied before
<a href="#">CSCvi41050</a>	PFRv3 route-control is inconsistently set to “Disabled” on BR devices
<a href="#">CSCvi41465</a>	All router mcast is removed by “no ipv6 mld router” in specific timing
<a href="#">CSCvi42002</a>	CDP packets not getting encapsulated over multipoint GRE tunnel
<a href="#">CSCvi44476</a>	IS-IS unnecessarily updates RIB when in metric-style narrow
<a href="#">CSCvi48837</a>	Ensure load-balance internet TCs do not match “class DEFAULT” if configured
<a href="#">CSCvi50061</a>	Evaluate NTP February 2018 Vulnerabilities.
<a href="#">CSCvi51398</a>	ASR 1001-X Te0/0/1 link fails when AOC transceivers are used
<a href="#">CSCvi52659</a>	Incorrect “Hop count” observed in IPv6 EIGRP
<a href="#">CSCvi54878</a>	Memory leaks seen at PKI_name_list_add(0xa139cc0)+0x3e
<a href="#">CSCvi56463</a>	Unexpected Reset, Crypto IKMP Segmentation fault with IPSec AAA Configuration
<a href="#">CSCvi57096</a>	MATM RP Shim Process memory leak @aaa_attr_list_alloc make_a_sublist_max
<a href="#">CSCvi58526</a>	CPUHog and crash on DNS-SRV-1 process
<a href="#">CSCvi58996</a>	Several OID from CISCO-CLASS-BASED-QOS-MIB stop working when performing upgrade to Denali-16.3.x
<a href="#">CSCvi61745</a>	Crash when running “mpls tunnel protection” command
<a href="#">CSCvi63840</a>	vif interface counters do not increment with multicast service reflection on IOS-XE
<a href="#">CSCvi64534</a>	Remove stack 1+1 CLI for WS-C3850-48XS
<a href="#">CSCvi67613</a>	Protocol type for GRE header does not work consistently with “cts sgt inline” enable over auto-tunnel

Caveat ID Number	Description
<a href="#">CSCvi71376</a>	OSPF SSPF: tilfa ALGORITHM fails to compute repair path, reports incorrect reason of too many labels
<a href="#">CSCvi72996</a>	NMR TTL is wrongly considering eid-record of 0.0.0.0/0 for its calculation
<a href="#">CSCvi74088</a>	link local multicast packets are received when the SVI is in down state
<a href="#">CSCvi74893</a>	ICMP Redirect send even if destination and source address are in different networks
<a href="#">CSCvi75086</a>	Rapid TDL memory leak in SMD process leads to crash of active switch in stack for ipv6 clients
<a href="#">CSCvi76084</a>	Device-tracking entry stuck in TENTATIVE for certain Mac Pro hosts configured with static IP
<a href="#">CSCvi79948</a>	OSPF TILFA: tilfa ALGORITHM preference rules does not pick repair path with lowest number of labels
<a href="#">CSCvi86082</a>	ASR1001-x crash due to wrong packet size
<a href="#">CSCvi86630</a>	Crash due appnav SYN-ACK packets without a flow
<a href="#">CSCvi86983</a>	ZBFW HA: active router stuck in cold standby state after shut no shut the wan interface
<a href="#">CSCvi91714</a>	IPv6 address not assigned or delayed when RA Guard is enabled
<a href="#">CSCvi92571</a>	On IOSXE neighbor command under pseudowire interface is rejected
<a href="#">CSCvi94425</a>	TBAR issues on KS after running “clear crypto gdoi ks coop role”
<a href="#">CSCvi95775</a>	Reverse-tunnel routes under PMIPv6 MAG config not using configured distance metric
<a href="#">CSCvi96874</a>	ASR1001 has crashed with cgm_avlmgf_find_node
<a href="#">CSCvi96933</a>	mac-move does not work on IBNS 2.0 unless you disable it then enable it back
<a href="#">CSCvj00858</a>	CPP Microcode Crash during sRTP Call Encryption
<a href="#">CSCvj01098</a>	Evaluation of IOS-XE and IOS for OpenSSL CVE-2018-0739 and CVE-2018-0733
<a href="#">CSCvj02081</a>	CPP crash on L2TP router
<a href="#">CSCvj03263</a>	H225 gatekeeper request dropping under “ALG PARSER” with ZBF
<a href="#">CSCvj04717</a>	OSPF SSPF: With SRTE tunnel scale, SRTE SID0 constraint Label Bind fails with LABEL_BROKER error msg
<a href="#">CSCvj05446</a>	Initial Trustpool installation not successful before PKI is ready
<a href="#">CSCvj06388</a>	Type 7 password parsed incorrectly in dot1x credentials causing auth failure
<a href="#">CSCvj06391</a>	Recommit of CSCvg77924 - FRR feature not working in ESP100 & ESP200
<a href="#">CSCvj06909</a>	Reverse-route configuration is unsupported under gdoi crypto map

Caveat ID Number	Description
<a href="#">CSCvj08248</a>	Packet throughput drops down when enable tunnel visibility with single tcp flow(>1MPPS)
<a href="#">CSCvj11876</a>	Provide Passthrough Reason in IOS-XE for AppNav
<a href="#">CSCvj13382</a>	ASR1K crash with Last reload reason: Critical process fman_fp_image fault on fp_0_0 (rc=134)
<a href="#">CSCvj14521</a>	Web redirect clients do not get redirected, Create IO ctx, too many intercepted connections
<a href="#">CSCvj16825</a>	“VoIP dial-Peer is Up” incorrectly log prints at every up interval when server-group is configured
<a href="#">CSCvj21692</a>	UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ACCT Periodic Proc
<a href="#">CSCvj23301</a>	IOS: Crypto Ruleset fails to get deleted
<a href="#">CSCvj24940</a>	Voice VRF with No Bind OPTIONS Ping response not sent
<a href="#">CSCvj27172</a>	Crash during Generic Call Filter Module cleanup
<a href="#">CSCvj27526</a>	BGP attribute map for aggre address can not set attribute
<a href="#">CSCvj29126</a>	RADIUS client on network fails to solicit PAC key from CTS even though the device has a valid PAC
<a href="#">CSCvj30023</a>	DNS Debug seen without enabling any debug
<a href="#">CSCvj30995</a>	ASR1K - exhausted IP Session Handles - %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0)
<a href="#">CSCvj38384</a>	%PMIPV6-5-TUNNELDELETE:
<a href="#">CSCvj39346</a>	OSPF SSPF: When sid 0 is removed, wrong implicit-null label used for inter-area prefix.
<a href="#">CSCvj41224</a>	Crash when doing SNMP walk and applying QOS over a GRE tunnel
<a href="#">CSCvj41550</a>	default channel operation state changing from I/O to D/O failed when zero-sla enabled
<a href="#">CSCvj49476</a>	Telnet Sessions Hang/Become unavailable at execution of “show run”
<a href="#">CSCvj52231</a>	ACEs after an object-group reference not being processed in software if ACL has more than 13 ACEs
<a href="#">CSCvj52681</a>	dynamic vlan assignment causes all sisf entires under the port to be deleted
<a href="#">CSCvj53634</a>	The OID - adslAtucCurrOutputPwr returns incorrect output.
<a href="#">CSCvj57502</a>	Memory leak@CENT-BR-0 when change the path label frequently
<a href="#">CSCvj61603</a>	“dtmf-interworking rtp-nte” command breaking software MTP.

Caveat ID Number	Description
<a href="#">CSCvj65296</a>	“ip rsvp bandwidth” max value limitation to 10GE

## Caveats in Cisco IOS XE Everest Release 16.6.3

### Open Caveats—Cisco IOS XE Everest 16.6.3

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

Caveat ID Number	Description
<a href="#">CSCux20847</a>	R0/0: ASR1002-X kernel: bullseye_i2c_master_xfer Error Repeats Every Hour
<a href="#">CSCuy30341</a>	Skywalker: Failed to create, Pseudowire interface
<a href="#">CSCvb88867</a>	Excess BGP Traps Generated just after upgrade
<a href="#">CSCvc80822</a>	OSPF SRTE: Invalid primary paths and metric seen with SRTE autoroute announce with metric option
<a href="#">CSCvd14310</a>	IP TUNNELS: Overlapping Loopback Interface Causes Incorrect Forwarding Decision with AppNav and PfR
<a href="#">CSCvd65197</a>	IOSd crashed when dialer disconnect the ISDN call
<a href="#">CSCve01479</a>	e2e ping is failed after configuring profiles qos-de and aaaauth1
<a href="#">CSCve54914</a>	NDSSO vrf ha table to be populated correctly
<a href="#">CSCve69049</a>	Crash when it tries to write over a TTY session
<a href="#">CSCvf07576</a>	router reloaded when doing show BGP RT filter routes
<a href="#">CSCvf28977</a>	ESP Crash with FP Switchover
<a href="#">CSCvf34608</a>	Excessive "Reflector" Tracelogs
<a href="#">CSCvf38050</a>	Voice Gateway crash due to memory corruption while finding DN index during redirect
<a href="#">CSCvf70383</a>	Crash in SDP Passthru when T.38 as 1st mline in mid-call SDP
<a href="#">CSCvf89894</a>	GETVPN // Primary KS sending rekey first to GM's and then to Secondary KS via scheduled rekey.
<a href="#">CSCvf96294</a>	MIB counter for IPSec tunnels does not decrement under high tunnel scale and churn
<a href="#">CSCvf98231</a>	Broadcast counters issue on ISR4400
<a href="#">CSCvg05452</a>	IOS-XE router crash from memory corruption during CCB cleanup
<a href="#">CSCvg08471</a>	OSPF; process ospf segmentation fault when shut and no shut is performed in active RP.

Caveat ID Number	Description
<a href="#">CSCvg19259</a>	MPLSoFlexVPN: Hub doesn't forward resolution req when default route is advertised to spokes
<a href="#">CSCvg19671</a>	ASR1K not dropping frames with unknown MAC when EVC + Sub-interface is configured
<a href="#">CSCvg23820</a>	CTS PAC download fails with VRF config on non-management interface
<a href="#">CSCvg29105</a>	asr1k: Gec 5 tuple feautre not working in IOS-XE releases post 16.4.1
<a href="#">CSCvg40893</a>	BE4K Registration failed for REGISTER matching wrong voip dial-peer
<a href="#">CSCvg42218</a>	BE4K VRF failed to associate if binding is used in tenant
<a href="#">CSCvg43408</a>	IOS-XE Router crashed unexpectedly with critical process fault, fman_fp_image, fp_0_0, rc=134
<a href="#">CSCvg48492</a>	BE4000 one way audio seen line to trunk side call with VRF enabled
<a href="#">CSCvg53159</a>	%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch
<a href="#">CSCvg60185</a>	ISR 4000 discards private RSA key after upgrade and reload with WAAS module
<a href="#">CSCvg67820</a>	HIGH CPU observation on FMAN RP ESS EVENT TRACING
<a href="#">CSCvg75315</a>	ASR1K BGP scanner crash when change VRF and BGP configuration
<a href="#">CSCvg77128</a>	ASR1009-X FAN SN in show inventory display incorrectly after replace the FAN and do RP switchover
<a href="#">CSCvg79608</a>	PfR: Overlapping Loopback Interface Causes Incorrect Forwarding Decision with AppNav and PfR
<a href="#">CSCvg91169</a>	3850 standby switch reloads due to configuration-mismatch after use "exception crashinfo" command
<a href="#">CSCvg94600</a>	crash with "debug platform condition ipv4 access-list "
<a href="#">CSCvg94978</a>	CUBE Router crashed - Critical software exception, Process = CCH323_CT
<a href="#">CSCvg95032</a>	Crash when downloading configuration from APIC-EM server
<a href="#">CSCvh02109</a>	WSMA: Server responds with HTTP 404 on wsma-exec with http transport profile
<a href="#">CSCvh02575</a>	PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT error with traceback
<a href="#">CSCvh05611</a>	IOSd crash while applying dial peer configuration
<a href="#">CSCvh09620</a>	Continuous crash in "/kernel/mki/src/free" after upgrade to version 15.5(3)S6
<a href="#">CSCvh20302</a>	"HTTP CORE" Process Crashes When Parsing PNP Transport Config

Caveat ID Number	Description
<a href="#">CSCvh22775</a>	SIP40 in slot 5 of ASR1013 when inserted ESP-200 in F1 by replacing ESP-40, showed ESI lock failure
<a href="#">CSCvh24315</a>	Memory leak for CCSIP_TCP_SOCKET and CCSIP_UDP_SOCKET on CUBE
<a href="#">CSCvh24730</a>	PfRv3: Crash while Printing the Same TCA Message
<a href="#">CSCvh26241</a>	Crash after crypto map removal
<a href="#">CSCvh26560</a>	ESP crashes with high scale QoS configuration
<a href="#">CSCvh32216</a>	Sporadic Crashes Due to IPSec (during ISAKMP AAA interaction)
<a href="#">CSCvh47124</a>	Nexthop is wrong in route-import table on branch when delete WAN interface and reconfigure it
<a href="#">CSCvh48610</a>	iwan router crash while updating pmi policy
<a href="#">CSCvh52882</a>	Memory Leak due to nbar config
<a href="#">CSCvh53691</a>	FP crash with scaled IKE sessions.
<a href="#">CSCvh53764</a>	RP Crash @ gcfm_check_percall_status
<a href="#">CSCvh54229</a>	TCAM critical limit shows incorrect value of 55 %.
<a href="#">CSCvh57091</a>	ESP crash when flapping interface with l2tp tunnels that have qos applied to the tunnels.
<a href="#">CSCvh57108</a>	CPUHOG on QoS statistics collection for DMVPN. QoS crash with DMVPN/NHRP.
<a href="#">CSCvh57242</a>	cpp-mcplo-ucode crash when layer 2 switching packet
<a href="#">CSCvh58702</a>	Router crashes after interface flap where sessions get moved from one interface to another
<a href="#">CSCvh59431</a>	Byte counters for physical port-channel interface and port-channel subinterface don't match
<a href="#">CSCvh61453</a>	NULL remote_hostname from LAC
<a href="#">CSCvh62925</a>	ASR1001-HX log alarm "Install interface_10g license to unshut the port"
<a href="#">CSCvh63857</a>	Memory leak in some SBC functions
<a href="#">CSCvh64729</a>	FP crash @cpp_qm_create_queue while adding fair-queue
<a href="#">CSCvh66445</a>	ISR4k router crashes during status check on WAAS Express
<a href="#">CSCvh70356</a>	ASR1K - ECMP load-balance w/ DPI L2TP Tunnel visibility and QoS may generate ucode crash
<a href="#">CSCvh71668</a>	ASR1002-HX/Polaris 16.5: Traceback seen for full VMI when lcp AVPs pushed by RADIUS

Caveat ID Number	Description
<a href="#">CSCvh72004</a>	ARP for the gateway on ASR1k for Mgmt-intf g0 is not generated on Dataplane after it times out
<a href="#">CSCvh74076</a>	Performance monitor related field (like SSRC) is not collected.
<a href="#">CSCvh75132</a>	CPP crash stuck thread detected multikey_hash_replace_int
<a href="#">CSCvh77439</a>	traffic is dropped when goes over tunnel
<a href="#">CSCvh77835</a>	ucode core due to stuck thread detected - DoubleExceptionVector
<a href="#">CSCvh82112</a>	Polaris Routers - Memory leak under process RECMSPAPP in IOSd

### Resolved Caveats—Cisco IOS XE Everest 16.6.3

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

Caveat ID Number	Description
<a href="#">CSCua00661</a>	Memory leak seen while creating vlans using Tcsh
<a href="#">CSCus83515</a>	Unable to verify files on stby-bootflash: filesystem.
<a href="#">CSCuy74937</a>	upgrade rom-monitor filename flash: returns "Invalid File"
<a href="#">CSCuz93679</a>	"dot1x auth-fail eapol" is always seen in "show run all"
<a href="#">CSCvc48752</a>	VPDN not switching traffic to new path after link failover or routing protocol convergence
<a href="#">CSCvc60745</a>	tcp_getbuffer memory leak - refcount not reduced when packet dropped
<a href="#">CSCvd04871</a>	Crash after IWAN does a recalculation in the RIB
<a href="#">CSCvd64670</a>	SCEP enrollment failing with HTTP/1.1 500 Internal Error
<a href="#">CSCvd82858</a>	Standby RP3 fails to boot on soft start
<a href="#">CSCvd96815</a>	Enhancement: Un-controlled TC in DISCARDED state is dropped instead of RIB-routed
<a href="#">CSCve08418</a>	IPsec/IKEv2 Installation Sometimes Fails With Simultaneous Negotiations
<a href="#">CSCve18549</a>	CME/BE4000 Intermittently Crash when making configuration changes
<a href="#">CSCve32330</a>	%UTIL-6-RANDOM: A pseudo-random number was generated twice in succession
<a href="#">CSCve53263</a>	Configured Speed/Duplex are not supported on Mgmt Eth port
<a href="#">CSCve55089</a>	BGP crashes at bgp_ha_sso_enable_ssmode
<a href="#">CSCve58650</a>	System Boot Hung without EULA Acceptance
<a href="#">CSCve64341</a>	920 : Mid Point LSP creation failure after reload with latest polaris Image

Caveat ID Number	Description
CSCve66601	Crash in CISCO-SLB-EXT-MIB code
CSCve75579	CUBE crashed on executing "show sip-ua calls called-number"
CSCve75919	In-dialog options ping received post ACK (call completion) cause cube to change codec and no audio
CSCve78038	IKE_INIT is sent before PPPoE dialer obtains its IP address
CSCvf16338	voiprtp_register_transport_port_manager_and_reserve: Alloc ports failed, min: 8000, max: 48199 248
CSCvf16626	iwan router crash while updating pmi policy
CSCvf24928	QFP exmem memory leak in cpp_fm_sce_result_chunk
CSCvf31368	router crash after EEM-wanfailover script triggered
CSCvf33947	CUBE can't handle mid-call re-invite when midcall-signalling passthrough mediachange is configured
CSCvf36269	Cisco IOS and IOS XE Software Plug-and-Play PKI API Certificate Validation Vulnerability
CSCvf36888	IOS-XE DMVPN Per-tunnel QoS not working on CSR1k without AX license
CSCvf39474	GETVPN: TBAR sync "timer is not running" after KS upgrade causing anti-reply drops and GM outages
CSCvf43271	Traceback: Stack master crash at dot1x authentication
CSCvf48159	Router crash during T38 fax bitrate negotiation
CSCvf60862	Cisco IOS and IOS XE Software IOS daemon Cross-Site Scripting Vulnerability
CSCvf65522	ESP crashed - double_exception_has_occured - malformed PIM packet over GRE tunnel & ERR_DTL_INV_ADDR
CSCvf68261	Crash when printing IPSEC anti-replay error
CSCvf84349	Router crash on polling cEigrpPeerEntry
CSCvf90066	ASR1K RP2 crash due to CPUHOG occurred by arp input process infinite loop
CSCvf92460	show gtp parameters causes RP to crash
CSCvf93129	Mid-call failure because all available Crypto is not Offered in SDP
CSCvf97230	RE-INVITE and OPTIONS Glare not handled by CUBE
CSCvg02533	router crashed after triggers with debug
CSCvg03542	[RIB route watch] detect stale pointer from client to avoid system crash with corrupted memory



Caveat ID Number	Description
<a href="#">CSCvg04055</a>	Re-calculate PKI SHADOW timer after NTP synchronization
<a href="#">CSCvg05896</a>	IWAN EIGRP SAF - seq number mismatch after branch reload
<a href="#">CSCvg09010</a>	KS merge fails for groups with TBAR due to PST update failure on primary KS
<a href="#">CSCvg09235</a>	OPTIONS not replied by CUBE over TCP without interface bind
<a href="#">CSCvg14256</a>	Crash at cc_detect_mute_call
<a href="#">CSCvg15158</a>	DMVPN session get stuck in NHRP and UP-NO-IKE state without active IKEv2 session until rekey
<a href="#">CSCvg16357</a>	Copying file larger than 2GB to FTP destination fails with "Invalid argument" (revisit CSCug41449)
<a href="#">CSCvg17971</a>	ASR1k ESP may crash after a switchover if IPsec configured
<a href="#">CSCvg20200</a>	Polaris: Crash observed while client association with key-wrap enabled in controller.
<a href="#">CSCvg22515</a>	After upgrade of IOS, SSH passwords longer than 25 characters do not work
<a href="#">CSCvg26073</a>	QFP Memory leak in 'cpp_ep_svr' with 'CPP List Hdr Chunk'
<a href="#">CSCvg29183</a>	ISR4K - XE 16.3.4 - SIP-TDM GW - FLEXDSPRM-3-TDM_CONNECT errors and crash
<a href="#">CSCvg29609</a>	Crash when crypto map applied to several tunnel interfaces
<a href="#">CSCvg30722</a>	EAPTLS:- Session manger crashing with MKA/EAPTLS session bring up with newly installed certificates.
<a href="#">CSCvg31525</a>	In HA system, with secure storage, the private-config is being encrypted multiple times
<a href="#">CSCvg34034</a>	Te0/0/0 or Te0/0/1 shows up/up without cable
<a href="#">CSCvg34731</a>	IOS-XE MOS scores always show 4.x even with massive packet loss.
<a href="#">CSCvg34783</a>	Voice-port command compand-type is remove during a reboot
<a href="#">CSCvg34790</a>	Device crashes due to crypto pki functions
<a href="#">CSCvg38307</a>	CME/BE4000 crash occurs when call is made to invalid SNR destination
<a href="#">CSCvg38313</a>	both ESP100 crashed when the ATM interface input QOS configure is applied
<a href="#">CSCvg40085</a>	ISR4K - IOSd crash with SIGABRT with CCVPM_HTSP
<a href="#">CSCvg40430</a>	4431 QFP crashes by a LLC packet received in a Serial Interface
<a href="#">CSCvg42042</a>	crash seen on clearing "ip nat translation" while also doing show "ip nat translation"
<a href="#">CSCvg46973</a>	ASR1K -LNS ESP crash after failing/flapping TeGig interfaces

Caveat ID Number	Description
CSCvg49753	Received EVPN route type 2 ignored by ASR1K RR
CSCvg52500	cpp_cp_svr 100% CPU due to dumping 'TX idle timer expire (channel 111055)'
CSCvg52560	Traceback: OCSF creates a large number of lists and triggers a memory problem
CSCvg52687	quiet mode exit does not re-apply "vrf-also" to config.
CSCvg54074	3rd Party SIP Phones not registering from CME 11.6
CSCvg55316	Multiple crashes on ASR1k at iWAG GTP PDP director event dispatcher
CSCvg56518	ASR920 / ASR1k: PING MIB not returning results / Counter 32 = 0
CSCvg60135	Yoda based platform : Crash on cpp_qm_obj_destroy with reason as LocalSoft on Polaris Release
CSCvg60288	Device IP address AV pair replaced with 192.168.1.5
CSCvg71566	"no cdp enable" is rewritten to "no cdp tlv app" after reload.
CSCvg71581	hub BR gets crashed after issue "show domain iwan border channels" following with border shutdown
CSCvg72960	ASR1K - LNS node de-aggregation w/ POLARIS image
CSCvg74048	PKI: All SCEP requests fail with "Failed to send the request. There is another request in progress"
CSCvg75380	Polaris 16.3.5: Crash at auth_mgr_show_dc_details
CSCvg76912	CFD: pnp config upgrade failed when IFS returns size 0 for all TFTP files
CSCvg77410	qos/cce AOM pending batch ack due to BQS pending config
CSCvg84039	Traceback: Crash on WAAS menu prompt for WAN Interface
CSCvg88988	Crash in IP SLAs Responder process when removing 'ip sla responder' from config during TWAMP session
CSCvg89855	ESP crashed - cpp_cp failed in cpp_qm_event_proc_defer_parent_event
CSCvg90226	Crypto Traceback: Router crash at 'Crypto Support' segmentation fault
CSCvg92437	AToM: MSPW VC Down with Reason as No VC Remote Label Binding Received on RP SSO
CSCvg93473	IOSd crash due to segfault in show_snmp
CSCvg94908	Mgig stack keeps crashing while configuring with Radius commands
CSCvg98890	IOS-XE GM router might crash after the rekey method is changed from unicast to multicast

Caveat ID Number	Description
<a href="#">CSCvh00038</a>	Device IP address AV pair replaced with 192.168.1.5
<a href="#">CSCvh02516</a>	Cannot add static route through dynamic NEMO tunnel interface
<a href="#">CSCvh05575</a>	ISR 4k SCCP Process Does Not Wait for All PVDM Modules to Come Up Before Registering
<a href="#">CSCvh14580</a>	Router Crashes on command show ip dhcp vrf <vrf name > binding remembered
<a href="#">CSCvh15305</a>	"ip access-list resequence" causing crash on CBR-8
<a href="#">CSCvh17481</a>	PKI: Device crash during srl download with multiple CDP URI
<a href="#">CSCvh29981</a>	Suite-B Not Supported with ESP-200 on ASR1000-X Platform
<a href="#">CSCvh32416</a>	Evaluation of all for CPU Side-Channel Information Disclosure Vulnerabil
<a href="#">CSCvh54813</a>	Output Qos policy is removed from Dialer interface after reloading the device if input policy exists
<a href="#">CSCvh60525</a>	CLI 'aaa common-criteria' not available on IPBASEK9 license
<a href="#">CSCvh60871</a>	show platform software adjacency oce <ID> crashing router

## Caveats in Cisco IOS XE Everest Release 16.6.2

### Open Caveats—Cisco IOS XE Everest 16.6.2

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

Caveat ID Number	Description
<a href="#">CSCus83515</a>	Unable to verify files on stby-bootflash: filesystem.
<a href="#">CSCvg38872</a>	Crash observed while sending 40K 4Kb packet size html session with ETA configured on ESP 100
<a href="#">CSCux20847</a>	R0/0: kernel: bullseye_i2c_master_xfer Error Repeats Every Hour
<a href="#">CSCuz84374</a>	SPA modules on ASR1002-x show "missing" under show platform
<a href="#">CSCvc59505</a>	Member link of Port channel gets removed on doing a SSO on the peer end
<a href="#">CSCvc80822</a>	OSPF SRTE: Invalid primary paths and metric seen with SRTE autoroute announce with metric option
<a href="#">CSCvd04871</a>	Crash after IWAN does a recalculation in the RIB
<a href="#">CSCvd65197</a>	IOSd crashed when dialer disconnect the ISDN call
<a href="#">CSCvd96815</a>	Enhancement: Un-controlled TC in DISCARDED state is dropped instead of RIB-routed
<a href="#">CSCve01479</a>	e2e ping is failed after configuring profiles qos-de and aaaauth1

Caveat ID Number	Description
<a href="#">CSCve18549</a>	CME/BE4000 Intermittently Crash when making configuration changes
<a href="#">CSCve32330</a>	%UTIL-6-RANDOM: A pseudo-random number was generated twice in succession
<a href="#">CSCve53263</a>	Configured Speed/Duplex are not supported on Mgmt Eth port
<a href="#">CSCve54914</a>	NDSSO vrf ha table to be populated correctly
<a href="#">CSCve60276</a>	Crash in ADSL SNMP code
<a href="#">CSCve64341</a>	920 : Mid Point LSP creation failure after reload with latest polaris Image
<a href="#">CSCve75919</a>	In-dialog options ping received post ACK (call completion) cause cube to change codec and no audio
<a href="#">CSCve78446</a>	[1661]- Switch number is missing in stack merged logs.
<a href="#">CSCve78802</a>	Overlord: GLC-TE SFP module cannot up after OIR during traffic
<a href="#">CSCvf16626</a>	iwan router crash while updating pmi policy
<a href="#">CSCvf28977</a>	ESP Crash with FP Switchover
<a href="#">CSCvf33947</a>	CUBE can't handle mid-call re-invite when midcall-signalling passthrough mediachange is configured
<a href="#">CSCvf39868</a>	[UniScale]isr4431 crashes while verifying IPv6 CEF scalability
<a href="#">CSCvf43271</a>	Traceback: Stack master crash at dot1x authentication
<a href="#">CSCvf50723</a>	Packet-tracer error message % Error: Failed to collect packet info
<a href="#">CSCvf53573</a>	ISR4K 4400 fail to boot up on 3.13.8S 3.12.3s 3.11.4s 3.10.9s (4300 fail to boot up on 3.13.8S)
<a href="#">CSCvf65079</a>	ASR CUBE 1K reloaded with reason: RG-application reload on voice-b2bha RG
<a href="#">CSCvf68261</a>	Crash when printing IPSEC anti-replay error
<a href="#">CSCvf70383</a>	Crash in SDP Passthru when T.38 as 1st mline in mid-call SDP
<a href="#">CSCvf71066</a>	Router crash due to memory corruption in PKI
<a href="#">CSCvf74334</a>	mSATA SSD inventory is missing after module stop/start/reload
<a href="#">CSCvf84349</a>	Router crash on polling cEigrpPeerEntry
<a href="#">CSCvf86185</a>	NIM-SSD: Inventory of disk0 and disk1 are interchanged on Polaris 16.x
<a href="#">CSCvf87904</a>	IWAN Performance degradation on PI32 images
<a href="#">CSCvf88231</a>	Watchdog crash during file copy operation
<a href="#">CSCvf89399</a>	Flexible NetFlow crash

Caveat ID Number	Description
<a href="#">CSCvf90614</a>	ASR1k Regarding ifHCInBroadcastPkts value decreasing
<a href="#">CSCvf93129</a>	Mid-call failure because all available Crypto is not Offered in SDP
<a href="#">CSCvf96762</a>	[Amur-MR8] SM-X reload after configuring channel-group 18 on an interface
<a href="#">CSCvf97434</a>	3650/3850: neconf return if-index value as 0
<a href="#">CSCvg01760</a>	Traceback-CPUHog seen on the device
<a href="#">CSCvg03683</a>	ASR1K CGN NAT ASR1K ESP100 crashed with clear ip nat translation *
<a href="#">CSCvg05452</a>	IOS-XE router crash from memory corruption during CCB cleanup
<a href="#">CSCvg05554</a>	3800 Access points failing 802.1x authentication, sending wrong EAP Parameters
<a href="#">CSCvg06512</a>	Host name with . as last character is handled incorrectly on 6800 platforms
<a href="#">CSCvg07428</a>	List Header leak with Pfr enabled
<a href="#">CSCvg08471</a>	OSPF; process ospf segmentation fault when shut and no shut is performed in active RP.
<a href="#">CSCvg09010</a>	KS merge fails for groups with TBAR due to PST update failure on primary KS
<a href="#">CSCvg15158</a>	DMVPN session get stuck in NHRP and UP-NO-IKE state without active IKEv2 session until rekey
<a href="#">CSCvg16357</a>	Copying file larger than 2GB to FTP destination fails with "Invalid argument" (revisit CSCug41449)
<a href="#">CSCvg18107</a>	ZBFW Misclassifying and Dropping Traffic on Ingress/Egress
<a href="#">CSCvg19204</a>	Unable to establish OSPF neighbor when got more than 1500 intra-routes
<a href="#">CSCvg19259</a>	MPLSoFlexVPN: Hub doesn't forward resolution req when default route is advertised to spokes
<a href="#">CSCvg19491</a>	ASR1k losing VXLAN NVE Peer
<a href="#">CSCvg22515</a>	After upgrade of IOS, SSH passwords longer than 25 characters do not work
<a href="#">CSCvg23820</a>	CTS PAC download fails with VRF config on non-management interface
<a href="#">CSCvg26073</a>	QFP Memory leak in 'cpp_cp_svr' with 'CPP List Hdr Chunk'
<a href="#">CSCvg30928</a>	Management ARP Entry Disappears After A Period of Time
<a href="#">CSCvg31373</a>	SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for ASR1000 SPA TDL
<a href="#">CSCvg33403</a>	Incoming call fails with 'Lower layer disconnected call cause=47' error
<a href="#">CSCvg33941</a>	Netflow does not count the amount of traffic correctly

Caveat ID Number	Description
CSCvg34034	Te0/0/0 shows up/up without cable
CSCvg34685	IKEv1 Stuck Virtual-access interface&RRI 15.4(3)s6
CSCvg34783	Voice-port command compand-type is remove during a reboot
CSCvg34819	Crash on RTCP Packet ingress with FNF and Multicast configured.
CSCvg34889	IKEv2 VPN tunnel does not establish when destination ip address changes during the AUTH exchange.
CSCvg35550	Netflow cannot add anymore cache entries after some events
CSCvg36289	dot1x-err : Dot1x authentication already running for<MAC>with different handle
CSCvg38313	both ESP100 crashed when the ATM interface input QOS configure is applied
CSCvg38587	Crash while SNMP invokes TTY trap

### Resolved Caveats—Cisco IOS XE Everest 16.6.2

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

Caveat ID Number	Description
CSCuv47069	DHCP crashed when configure a manual binding in an interface
CSCux22473	IPv6 Tracking for route learned from IBGP neighbor is down
CSCvb11664	ASR1k:16.3_MR smd crash in FIPS Mode
CSCvc78492	DMVPN: IOS-XE - Unable to pass traffic if spoke to spoke fails to build in phase 2
CSCvd11419	Configuring Packet tracer on IOS-XE triggers a crash intermittently
CSCvd16501	High CPU due to SNMP ENGINE when polling mplsTunnelHopEntry
CSCvd80715	ASR1k IOSD crash due to memory corruption in aaa accounting
CSCve00909	16.6: Ping failure on re-add of ip address to Dialer Interface.
CSCve07263	IPSec Tunnel stuck in Up/Down state after shut/no-shut - VPN interop
CSCve09104	Command “segment-routing mpls” under router isis 1 not getting NVGEN'd
CSCve10917	IPsec crash on ASR1k router while processing KMI
CSCve13491	Router might crash due watchdog when creating a new swidb
CSCve15722	The second and later Pfrv3 VRF configs are missing after reload
CSCve20850	ASR1k unable to recover from the tunnel flapping at scale for IKEv2
CSCve23090	16.6 OBS: Local LFA is used incorrectly when TI-LFA Node Protection enabled

Caveat ID Number	Description
<a href="#">CSCve35209</a>	Kernal errors
<a href="#">CSCve35247</a>	ASR1K smd crash while copying config onto console
<a href="#">CSCve47826</a>	Memory leak at crypto IKEv2
<a href="#">CSCve51657</a>	Slow convergence with scale after a core link flaps
<a href="#">CSCve54486</a>	Crash when attempting to assign nonexistent/shutdown VLAN to 802.1x port
<a href="#">CSCve57788</a>	Web authentication clients do not receive redirect URL and HTTP Intercept
<a href="#">CSCve62846</a>	“kernel: nfs: server xx not responding, timed out” message output when reinserting ASR1000-RP2
<a href="#">CSCve66119</a>	Router crash due to process “Crypto Support” segmentation fault
<a href="#">CSCve68911</a>	Nested enhanced route refresh requests triggers stale prefixes
<a href="#">CSCve70876</a>	Crypto device microcode hangs and crashes on ASR1k routers
<a href="#">CSCve76827</a>	Large NAT policy-map takes long time to download
<a href="#">CSCve76945</a>	XE16.7.1:Router crashed when a “sh bgp” command was executed
<a href="#">CSCve77011</a>	SSL handshake failure when validating certification with name-constraints
<a href="#">CSCve81985</a>	Subscriber session not synced to standby while assigning static ip in DHCP
<a href="#">CSCve89668</a>	XE16.7.1:Router crashed when “clear ip bgp vpnv4 u update-group” command was run
<a href="#">CSCve94399</a>	Router crash when importing BGP routes - EVPN
<a href="#">CSCve95243</a>	Internal interface missing from L2FIB output list
<a href="#">CSCve97061</a>	Unable to remove “mpls tp” configuration from router
<a href="#">CSCve98056</a>	ESP ucode crash with ALG for PPTP traffic and PAP is enabled
<a href="#">CSCve98223</a>	Two PW-Group switchover notifications are triggered for a single event
<a href="#">CSCvf02131</a>	IP SLA can trigger crash when used with MPLS probe
<a href="#">CSCvf05616</a>	Traffic drop, on reconfiguring L2VPN sessions after SSO on peer
<a href="#">CSCvfl1237</a>	Memory leak seen @crypto_init_show_instance
<a href="#">CSCvfl1721</a>	ASR1k netflow crash
<a href="#">CSCvfl1776</a>	VRRPv3 with VRRS remains NOT READY after shutdown Port-channel IF
<a href="#">CSCvfl1991</a>	Crash when layer 2 switching packet
<a href="#">CSCvfl6448</a>	No all IPv6 GRE crypto tunnels may come up or recover from flapping at scale

Caveat ID Number	Description
CSCvf18162	Crash observed in MLPP-BACD scenario
CSCvf18470	IOS-XE CUBE HA crash
CSCvf24607	IPsec session fail after up/down link between DMVPN tunnel
CSCvf24713	Stale path message for that prefix is noticed when dampening is configured
CSCvf27072	NBAR not working on 16.5.1a in switch if name-server is configured
CSCvf29213	PFRv3: Site Prefix shows unreachable after removing and adding the specific route for the prefix
CSCvf30703	Watchdog crash when executing the “show run” command
CSCvf33570	Crash while BGP-RR Unconfiguration
CSCvf34835	IOS-XE GETVPN KS crashes while sending cgmGdoiKeyServerRegistrationComplete trap after GM reg
CSCvf35507	Crash in SSH Process due to SCP memory corruption
CSCvf42300	ISIS SR: segmentation fault in ISIS when “no seg mpls” command is given.
CSCvf44638	Numbered extended IP ACLs break config sync
CSCvf51341	Crash after “show ip ospf database summary” command
CSCvf52877	Memory leak under cpp_cp_svr process
CSCvf54314	Crash due to a null pointer dereference on HTSP structure
CSCvf59923	DNS: Split DNS reg-expression issue
CSCvf62777	CSR router restarts whenever no pass-through config is passed
CSCvf62916	Router crashes when doing “show ip bgp neighbor” on a flapping BGP neighborship
CSCvf63541	BGP w/global import/export crashes when several nbrs deleted simultaneously
CSCvf65643	Unicast ping stops working when “ip pim sparse-mode” removed from SVI
CSCvf68602	e1r2-Cas is not working when adding “invert-abcd 1 0 0 0”
CSCvf69272	SNMP ENGINE high CPU usage observed
CSCvf74154	SGACL: Crash during CFM EDIT request
CSCvf74829	CRL download fails due to “failed to create getcacert message”
CSCvf76512	Option 82 circuit-id-tag restricted by 6 bytes
CSCvf76535	B2B NAT HA: Stale NAT translations stuck on primary router after communication loss with standby



Caveat ID Number	Description
<a href="#">CSCvf80163</a>	ASR1K crashes due to crypto microcode
<a href="#">CSCvf80495</a>	IPv6 BGP network advertized not seen in the peer
<a href="#">CSCvf80757</a>	NETCONF-YANG/RESTCONF edit config fails silently, subsequent get config reports false-positive
<a href="#">CSCvf81579</a>	ASR1K: IOSd crash on null map dereference
<a href="#">CSCvf81695</a>	ASR1K encryption processor trace file is not valid
<a href="#">CSCvf84482</a>	ASR1001-X 10GE built-in ports cannot be enabled using Smart Licensing
<a href="#">CSCvf86462</a>	ASR1006-X memory leak after sending ARP entries
<a href="#">CSCvf88590</a>	After disabling http server/https server on netconf, IP-Adm-V4-Int-ACL-global delete
<a href="#">CSCvf89608</a>	Missing IP route to cellular interface after router reload or modem power cycle
<a href="#">CSCvf92057</a>	CUBE is unable to send PRACK to Skype server for inbound calls
<a href="#">CSCvf95077</a>	Stale Mac entry in MLRIB
<a href="#">CSCvf95141</a>	ZBF crashes on standby
<a href="#">CSCvf96035</a>	ISIS redistribute connected not working for IPv6 routes
<a href="#">CSCvg08979</a>	Martian check for “distance” command needs to be removed
<a href="#">CSCvg13049</a>	ISRG2: dot1p marking fails if service-policy applied on the Dialer
<a href="#">CSCvg31493</a>	Stale Mac entry in MLRIB additional fix
<a href="#">CSCvg31495</a>	NMR calculation is wrongly considering eid-record of 0.0.0.0/0 in SDA
<a href="#">CSCvf98863</a>	MMA crash observed on Hub Router in IWAN setup

## Caveats in Cisco IOS XE Everest Release 16.6.1

### Open Caveats—Cisco IOS XE Everest 16.6.1

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

Caveat ID Number	Description
<a href="#">CSCvf23886</a>	Link goes down due to local fault in an ASR1K plugged to 3850 switch running OSPF
<a href="#">CSCve62846</a>	“kernel: nfs: server xx not responding, timed out” message outputted when re-inserted “ASR1000-RP2”
<a href="#">CSCvf28315</a>	ASR1006-X memory leak in linux_iosd-imag and fman_rp after sending 1000000 ARP entries
<a href="#">CSCux20847</a>	R0/0: kernel: bullseye_i2c_master_xfer Error Repeats Every Hour

Caveat ID Number	Description
<a href="#">CSCve45753</a>	R0/0: kernel: i2c_master_xfer (line 276): port 0, addr 19, len 1 c2w master failed to send data
<a href="#">CSCve53263</a>	Configured Speed/Duplex are not supported on Mgmt Eth port
<a href="#">CSCvf13960</a>	Incorrect status in show facility-alarm status after Gi0 no shut
<a href="#">CSCuz84374</a>	SPA modules on ASR1002-x show “missing”/“out of service” under show platform
<a href="#">CSCvd63476</a>	Changing autoneg setting on ASR1K cause link failure on subsequent link flap (connected to 2960XR)
<a href="#">CSCvf08550</a>	Netflow Export over aggregate port-channel is Nil
<a href="#">CSCve95037</a>	Traceback found for PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT part 2
<a href="#">CSCvf26158</a>	SPA-1X10GE-L-V2 may not power up on insertion in ASR1001-X
<a href="#">CSCvf07683</a>	ASR1k crash when enabling FNF in a tunnel interface
<a href="#">CSCvf11721</a>	ASR1k netflow crash at flow_def_field_list_copy_with_callback
<a href="#">CSCvf02875</a>	Reducing the memory utilized by ISR-WAAS-200
<a href="#">CSCve45274</a>	A Cisco router may crash when issuing the ‘show dmvpn detail   in Virtual-Access.+ is up/down INTF’
<a href="#">CSCvf23190</a>	IPSec install failing with dynamic crypto map scale
<a href="#">CSCuv90519</a>	Map doesn't get updated with socket change on local address change
<a href="#">CSCvf14771</a>	NBAR incorrectly classifies RTP-AUDIO as Cisco-Jabber
<a href="#">CSCvf16626</a>	iwan router crash while updating pmi policy
<a href="#">CSCvc46230</a>	PfRv3: Unexpected Reload While Evaluating/Moving TC's Between Channels
<a href="#">CSCvf02356</a>	ASR1002-X Router crashed on “Parent still holding tunnel subblocks after delete”
<a href="#">CSCvf21718</a>	ASR1K crash when running ‘show ip nhrp vrf ... detail’
<a href="#">CSCve99492</a>	DMVPN Ph-2: spoke to spoke traffic drops, NHRP entry incomplete, if crypto session fails to come up
<a href="#">CSCve89450</a>	ASR1001X silent reload “Critical process fman_fp_image fault on fp_0_0 (rc=154)”
<a href="#">CSCve69182</a>	Logs filled with conn_array_empty messages
<a href="#">CSCve85635</a>	Restconf GET /restconf/data?depth=1&content=nonconfig results in malformed JSON(missing closing “}”)
<a href="#">CSCve85617</a>	Restconf query parameters fields and depth doesn't work properly together

Caveat ID Number	Description
<a href="#">CSCve85645</a>	Restconf “fields” query param - malformed JSON and setting value to leaf from different model
<a href="#">CSCve69764</a>	“default interface <name>” config command reports different vty then actually executed the command
<a href="#">CSCve29602</a>	CDB does not sync after OIR of slot/subslot components
<a href="#">CSCve97572</a>	MKA-PSK: Need support for CKN length of all values between 1 and 32 range
<a href="#">CSCve87995</a>	Site prefix splitting redesign due to the new site prefix learning from rib feature

### Resolved Caveats—Cisco IOS XE Everest 16.6.1

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

Caveat ID Number	Description
<a href="#">CSCvd19860</a>	OSPFv3 AUTH breaks IPv6 traffic intermittently
<a href="#">CSCve71068</a>	"show platform software cerm-information" no longer showing statistics information
<a href="#">CSCve47826</a>	Memory leak Crypto IKEv2 at ikev2_ios_psh_set_route_info
<a href="#">CSCve20522</a>	"show crypto map" displays incorrect wildcard mask for crypto access-list
<a href="#">CSCve10917</a>	IPSec crash on ASR1k router while processing KMI
<a href="#">CSCvfl1237</a>	Memory leak seen@crypto_init_show_instance
<a href="#">CSCve63482</a>	Phase1 comes up and DPDs being exchanged even if the tunnel interface is shut d
<a href="#">CSCvf22394</a>	ASR1001 memory leak in the "Crypto IKE Dispa" process
<a href="#">CSCve07263</a>	IPSec Tunnel stuck in Up/Down state after shut/no-shut - VPN Interop
<a href="#">CSCvc79296</a>	Redundancy inter-device is not working with "security ipsec"
<a href="#">CSCve66119</a>	Router crash due to process "Crypto Support" segmentation fault
<a href="#">CSCvd97524</a>	Fixed versions for CSCuz15131 crash when traffic with maximum size is on wire
<a href="#">CSCve14080</a>	Error message "LID: Handle 0x0 is invalid" filling console logs
<a href="#">CSCve77011</a>	SSL handshake failure when validating certification with name-constraints
<a href="#">CSCve74862</a>	Crash due to memory corruption when using PNP feature
<a href="#">CSCve76827</a>	large NAT policy-map takes long time to download
<a href="#">CSCve98056</a>	ESP ucode crash with ALG for PPTP traffic and PAP is enabled.

## Related Documentation

### Platform-Specific Documentation

For information about associated services and modules in Cisco ASR 1000 Series Aggregation Services Routers, see: [Documentation Roadmap for Cisco ASR 1000 Series](#), [Cisco IOS XE 16.x Releases](#).

### Communications, Services, and Additional Information

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

### Cisco Bug Search Tool

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

