



# Release Notes for Cisco CSR 1000v Series, Cisco IOS XE Denali 16.3

---

**Last Updated: May 7, 2021**

This release notes document provides information about Cisco CSR 1000v Series Cloud Services Routers operating with Cisco IOS XE Denali 16.3. You can find CSR1000v release notes for other versions of Cisco IOS XE at [Cisco CSR 1000v Release Notes](#).

- [Cisco CSR 1000v Series Cloud Services Routers Overview](#)
- [Migrating to Cisco IOS XE Denali 16.3](#)
- [Technologies Supported by a Platform](#)
- [System Requirements](#)
- [Features and Notes by Release](#)
- [Caveats](#)
- [Related Documentation](#)

## Cisco CSR 1000v Series Cloud Services Routers Overview

### Virtual Router

The Cisco CSR 1000v Cloud Services Router is a cloud-based virtual router deployed on a virtual machine (VM) instance on x86 server hardware. It supports a subset of Cisco IOS XE software features and technologies, providing Cisco IOS XE security and switching features on a virtualization platform.

When the Cisco CSR 1000v is deployed on a VM, the Cisco IOS XE software functions as if it were deployed on a traditional Cisco hardware platform. You can configure different features depending on the Cisco IOS XE software image.

### Secure Connectivity

The Cisco CSR 1000v provides secure connectivity from an enterprise network (such as in a branch office or data center) to the public or private cloud.



# Migrating to Cisco IOS XE Denali 16.3

Important information about migrating successfully from Cisco IOS XE 3S to Cisco IOS XE Denali 16.3.1 is in the Cisco IOS XE Denali 16.3 Migration Guide for Access and Edge Routers at:

<http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-16/products-installation-guides-list.html>.

For a list of caveats in this release, see [Caveats: Cisco IOS XE Denali 16.3.1](#).

## Technologies Supported by a Platform

A platform's product landing page lists technology configuration guides for Cisco IOS XE technologies that the platform supports.

In each technology configuration guide, a Feature Information table indicates when a feature was introduced to the technology. For some features, the table also indicates when additional platforms have added support for the feature.

To determine whether a particular platform supports a technology, view the list of technology configuration guides posted on the platform's product landing page.

## System Requirements

The following sections describe the system requirements for the Cisco CSR 1000v Series Cloud Services Routers.

- [Hardware Requirements](#)
- [Software Images and Licenses](#)

## Hardware Requirements

For hardware requirements and installation instructions, see the [Cisco CSR 1000v Series Cloud Services Router Software Configuration Guide](#).

## Software Images and Licenses

- [Cisco Smart Licensing](#)
- [Cisco CSR 1000v Evaluation Licenses](#)
- [Cisco CSR 1000v Software Licenses](#)
- [Software Image Nomenclature for OVA, ISO, and QCOW2 Installation Files](#)

## Cisco Smart Licensing

The Cisco CSR 1000v supports activation using Cisco Smart Licensing. To use Cisco Smart Licensing, you must first configure the Call Home feature and obtain Cisco Smart Call Home Services. For more information, see the [Cisco CSR 1000v Cloud Services Router Software Configuration Guide](#).

For a more detailed overview on Cisco Licensing, go to [cisco.com/go/licensingguide](http://cisco.com/go/licensingguide).

## Cisco CSR 1000v Evaluation Licenses

Evaluation license availability depends on the software version:

- Evaluation licenses valid for 60 days are available at the Cisco Software Licensing (CSL) portal: <http://www.cisco.com/go/license>

The following evaluation licenses are available:

- AX technology package license with 50 Mbps maximum throughput
- APPX technology package license with 10 Gbps maximum throughput

If you need an evaluation license for the Security technology package, or for an AX technology package with higher throughput, contact your Cisco service representative.

For instructions on obtaining and installing evaluation licenses, see the “[Installing CSL Evaluation Licenses for Cisco IOS XE 3.13S and Later](#)” section of the *Cisco CSR 1000v Software Configuration Guide*.

## Cisco CSR 1000v Software Licenses

Cisco CSR 1000v software licenses are divided into feature set licenses. Supported feature licenses depend on the release.

### Legacy License Types

Three legacy technology packages—**Standard**, **Advanced**, and **Premium**—were replaced in Cisco IOS XE Release 3.13 with the **IPBase**, **Security**, and **AX** technology packages.

### Current License Types

The following license types are supported in Cisco IOS XE Denali 16.3.1:

- IPBase: Basic Networking Routing (Routing, HSRP, NAT, ACL, VRF, GRE, QoS)
- Security: IPBase package + Security features (IP Security VPN, Firewall, MPLS, Multicast)
- AX: IPBase package + Security features + Advanced Networking features (AppNav, AVC, OTV and LISP)
- APPX Package: IPBase package + Advanced Networking features - Security features (IP security features not supported)

### Features Supported by License Packages

For more information about the Cisco IOS XE technologies supported in the feature set packages, see the overview chapter of the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

### Throughput

The Cisco CSR 1000v router provides both perpetual licenses and term subscription licenses that support the feature set packages for the following maximum throughput levels:

- 10 Mbps
- 50 Mbps
- 100 Mbps
- 250 Mbps

- 500 Mbps
- 1 Gbps
- 2.5 Gbps
- 5 Gbps
- 10 Gbps

Throughput levels are supported for different feature set packages in each version. For more information about how the maximum throughput levels are regulated on the router, see the [Cisco CSR 1000v Cloud Services Router Software Configuration Guide](#).

### Memory Upgrade

Beginning with Cisco IOS XE 3.11S, a memory upgrade license is available to add memory to the Cisco CSR 1000v. This license is available only for selected technology packages.

### Additional Information about Licenses and Activation

For more information about each software license, including part numbers, see the [Cisco CSR 1000v Router Datasheet](#). For more information about the standard Cisco IOS XE software activation procedure, see the [Software Activation Configuration Guide, Cisco IOS XE Release 3S](#).

## Software Image Nomenclature for OVA, ISO, and QCOW2 Installation Files

The Cisco CSR 1000v installation file nomenclature indicates properties supported by the router in a given release.

The following are filename examples for the 16.3.1 release:

```
csr1000v-universalk9.16.03.01.ova
csr1000v-universalk9.16.03.01.iso
csr1000v-universalk9.16.03.01.qcow2
```

[Table 1](#) lists the attributes and the release properties indicated.

**Table 1** OVA Installation Filename Attributes

Filename Attribute	Properties
Example: universalk9	Installed image package.
03.09.00a.S.153-2.S0a	Indicates that the software image is for the Cisco IOS XE 3.9.0aS release image (mapped to the Cisco IOS 15.3(2) release).
std or ext	Standard release or extended maintenance support release.  Every third release, an extended maintenance support release (16.3, 16.9, 16.12, ...) is planned.

# Features and Notes by Release

- [Features and Notes: Release Cisco IOS XE Denali 16.3.5](#)
- [Features and Notes: Release Cisco IOS XE Denali 16.3.1a](#)
- [Features and Notes: Release Cisco IOS XE Denali 16.3.1](#)

## Features and Notes: Release Cisco IOS XE Denali 16.3.5

### Notes

#### Recommended Release for Cisco IWAN

Cisco IOS XE Denali 16.3.5 is not recommended for Cisco IWAN due to the following bugs: CSCvf98783, CSCvg35332, and CSCvg05896. Instead, it is recommended to use [Cisco IOS XE Denali 16.3.5c](#) for Cisco IWAN, which provides a fix for these bugs. For more details on these bugs, please see [Cisco Bug Search Tool](#).

## Features and Notes: Release Cisco IOS XE Denali 16.3.1a

### Notes

#### Amazon Web Services High Availability (AWS HA)

The method for monitoring AWS HA errors such as BFD peer down events has changed from using an EEM applet (in release Cisco IOS XE 3.16 or earlier) to using new Cisco IOS XE commands (for Cisco IOS XE Denali 16.3.1a or later) that include the **redundancy** command and sub-command **cloud provider [aws | azure] node-id**.

Use these commands to specify routing changes to the Route-table-id, Network-interface-id and CIDR in the event of an AWS HA error (for Cisco IOS XE Denali 16.3.1a or later).

The following verification commands are also available:

**show redundancy cloud provider [aws | azure] node-id** and  
**debug redundancy cloud [all | trace | detail | error]**.

For further information, see the “Configuring High Availability” section in [Cisco CSR 1000V Series Cloud Services Router Deployment Guide for Amazon Web Services](#).

## Features and Notes: Release Cisco IOS XE Denali 16.3.1

### Features

#### Hypervisor Support

The following hypervisors are either newly introduced or re-added for this release:- Citrix XenServer, Microsoft Hyper-V, Amazon Web Services and Microsoft Azure. (For Amazon Web Services, instance type C3 is no longer supported.)

**Snort-Powered IPS/IDS support on CSR**

The Snort IPS feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on Cisco CSR 1000v. This feature uses the open source Snort solution to enable IPS and IDS. For more information, see the *Security Configuration Guide: Unified Threat Defense*.

**VRF Support for IPS/IDS on CSR**

For detailed information, see the following documentation:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_utd/configuration/xr-16/sec-data-utd-xr-16-book/snort-ips.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xr-16/sec-data-utd-xr-16-book/snort-ips.html)

**DPDK for CSR**

DPDK (Dataplane Development Kit) is integrated into the dataplane of the CSR 1000v, using poll-mode drivers.

**URL Filtering Support on CSR**

Web Filtering enables the user to provide controlled access to Internet websites or Intranet sites by configuring the domain-based or URL-based policies and filters on the device. For more information, see the *Security Configuration Guide: Unified Threat Defense*.

**MVPN PE-PE Ingress Replication**

In Multicast VPN (MVPN) or Multipoint to Multipoint LDP (MLDP), multicast traffic received by an ingress provider edge (PE) router is replicated/copied and passes through the core to egress PE routers. State is maintained in the core and this may lead to some dynamic fluctuation of state in the service provider core routers. To improve upon this, when the new feature (PE to PE Ingress Replication (IR)) is used, multicast traffic received by an ingress PE router is replicated/copied and then tunneled over multiple unicast LSPs directly to egress PE routers. State is not maintained as the traffic passes through the core. For more information, see: BGP MVPN PE-PE Ingress Replication in the *IP Multicast: MVPN Configuration Guide*

**Citrix XenServer Support**

Support added for XenServer 6.5, 6.2 on Cisco CSR 1000v.

**Microsoft Hyper-V Support**

Support added for Windows Server 2012-R2 Hyper-V Mgr 6.3.9600.16384 on Cisco CSR 1000v.

**BGP IPv6 Admin Distance**

For detailed information, see the following documentation:

[www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_bgp/configuration/xr-16/irg-xr-16-book/bgp-ipv6-adm-distance.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xr-16/irg-xr-16-book/bgp-ipv6-adm-distance.html)

**ECMP load balance with tunnel visibility**

For detailed information, see the following documentation:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch\\_cef/configuration/xr-16/isw-cef-xr-16-book/isw-cef-ecmp-loadbalance-with-tunnel-visibility.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/xr-16/isw-cef-xr-16-book/isw-cef-ecmp-loadbalance-with-tunnel-visibility.html)

**Class-based traffic shaping**

For detailed information, see the following documentation:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos\\_mqc/configuration/xe-16/qos-mqc-xe-16-book/3-level-user-defined-queuing-policy-support.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xe-16/qos-mqc-xe-16-book/3-level-user-defined-queuing-policy-support.html)

### **3-level user-defined queuing policy support**

For detailed information, see the following documentation:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos\\_mqc/configuration/xe-16/qos-mqc-xe-16-book/3-level-user-defined-queuing-policy-support.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xe-16/qos-mqc-xe-16-book/3-level-user-defined-queuing-policy-support.html)

### **PPPoE over BDI**

For detailed information, see the following documentation:

[http://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/iproute/iri-xe-3s-asr920-book/iri-xe-3s-asr920-book\\_chapter\\_011.html](http://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/iproute/iri-xe-3s-asr920-book/iri-xe-3s-asr920-book_chapter_011.html)

### **PKI Trustpool Enhancements**

Effective with Cisco IOS XE Denali 16.3.1, the way PKI Trustpools are managed have changed. The PKI Trustpool Enhancements feature is used for authentication of HTTPS connections built from the router. Common features that leverage this feature include, but not exhaustive, Plug and Play (PnP), Cisco Web Security (CWS), Cisco Umbrella Branch. If you are upgrading to this release, please review the changes to the feature at the following Cisco document:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_pki/configuration/xe-16/sec-pki-xe-16-book/sec-pki-trustpool-mgmt.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-16/sec-pki-xe-16-book/sec-pki-trustpool-mgmt.html)

### **BFD over DMVPN**

For detailed information, see the following documentation:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book/sec-conn-dmvpn-bfd-support.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book/sec-conn-dmvpn-bfd-support.html)

### **VxLAN GPE Tunnel**

For detailed information, see the following documentation:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xe-16/ce-xe-16-book/vxlan-gpe-tunnel.html>

### **EVPN VxLAN L3**

For detailed information, see the following documentation:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xe-16/ce-xe-16-book/evpn-vxlan-l3.html>

### **set ip next-hop unchanged/next-hop-unchanged allpaths IPv4/IPv6**

For detailed information, see the following documentation:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_bgp/configuration/xe-16/irg-xe-16-book/bgp\\_next\\_hop\\_unchanged.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/bgp_next_hop_unchanged.html)

### **BGP IPv6 Dynamic Neighbor Support and VRF Support**

For detailed information, see the following documentation:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_bgp/configuration/xe-16/irg-xe-16-book/bgp-dynamic-neighbors.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/bgp-dynamic-neighbors.html)

**NAT support on BDI interface**

For detailed information, see the following documentation:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr\\_nat/configuration/xe-16/nat-xe-16-book/iadnat-dynamc-hsrp.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book/iadnat-dynamc-hsrp.html)

**Allow use of same ACL/router-map on multiple NAT statements**

For detailed information, see the following documentation:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr\\_nat/configuration/xe-16/nat-xe-16-book/iadnat-dynamc-hsrp.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book/iadnat-dynamc-hsrp.html)

**Cisco Unified Border Element (CUBE) Features**

The following CUBE features are supported on Cisco CSR 1000v platforms running Cisco IOS XE Denali 16.3.1:

**Multitenancy Call Routing and Scaling Enhancements for CUBE**

For detailed information, see the following documentation:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-multi-vrf.html>

**Consumption of Forked 18X Responses with SDP for CUBE**

For detailed information, see the following documentation:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-forked-18x-responses.html>

**Support for Voice Quality Monitoring**

For detailed information, see the following documentation:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-voice-quality-monitoring.html>

**Support for multi-tenants on SIP Trunks on Cisco IOS XE Denali 16.3.1**

For detailed information, see the following documentation:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-multi-tenants.html>

**Support for Multi-VRF on Cisco IOS XE Denali 16.3.1**

For detailed information, see the following documentation:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-multi-vrf.html>

**Support for session-ID on Cisco IOS XE Denali 16.3.1**

For detailed information, see the following documentation:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-session-id.html>

**Support for Video Suppression on Cisco IOS XE Denali 16.3.1**

For detailed information, see the following documentation:



<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-audio-force-d.html>

### **CVP Survivability TCL support with High Availability on Cisco IOS XE Denali 16.3.1**

For detailed information, see the following documentation:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-cvptcl-ha.html>

For more information on CUBE support in Cisco IOS XE, see:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/read-me-first.html>

## **Notes**

### **Memory Requirements when vCPUs Spread across Two Sockets (NUMA Nodes)**

In this release, if the CSR 1000v is configured to have vCPUs spread across two sockets (NUMA Nodes), then you must use 5 GB memory (not 4 GB).

### **Web User Interface**

The 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 for Cisco IOS XE Denali 16.3:

- Software Upgrade
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Network Address Translation (NAT)
- Virtual Routing and Forwarding (VRF)
- Application Visibility and Control (AVC)
- Custom Application
- Serial Interface

## **Limitations and Restrictions in Cisco IOS XE Denali 16.3.1**

### **REST API Management Container Images Compatible with Denali 16.3.1**

- When using the Cisco IOS XE REST API with the router, note the following limitation: If the router is operating with Cisco IOS XE Denali 16.3.1, use the latest REST API management container image. Attempting to use a REST API container image released prior to Cisco IOS XE Denali 16.x may cause the router to crash repeatedly.

## **Limitations and Restrictions in Cisco IOS XE Denali 16.3.11**

- Cisco CSR1000V Release 16.3.11 does not support the 6.4.3f-b4.2 image. If you upgrade your Cisco CSR1000V instance to release 16.3.11, the router moves to an offline state.

# Caveats

See open and resolved caveats in the following sections:

- [Caveats: Cisco IOS XE Denali 16.3.9](#)
- [Caveats: Cisco IOS XE Denali 16.3.8](#)
- [Caveats: Cisco IOS XE Denali 16.3.7](#)
- [Caveats: Cisco IOS XE Denali 16.3.6](#)
- [Caveats: Cisco IOS XE Denali 16.3.5](#)
- [Caveats: Cisco IOS XE Denali 16.3.4](#)
- [Caveats: Cisco IOS XE Denali 16.3.3](#)
- [Caveats: Cisco IOS XE Denali 16.3.1a](#)
- [Caveats: Cisco IOS XE Denali 16.3.1](#)

## Overview

Caveats, or “bugs,” describe unexpected behavior. Severity 1 caveats are the most serious. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. This section includes severity 1, severity 2, and selected severity 3 caveats.

## Terminology

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

[http://docwiki.cisco.com/wiki/Category:Internetworking\\_Terms\\_and\\_Acronyms\\_\(ITA\)](http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA))

## Bug Search Tool

If you have an account on Cisco.com, you can also use the Bug Search Tool (BST) to find select caveats of any severity. To reach the Bug Search Tool, log into Cisco.com and go to <https://tools.cisco.com/bugsearch/search>.

If a defect that you have requested cannot be displayed, it may be because the defect number does not exist or the defect does not have a description available.

You can use to the [Bug Search Tool](#) to view new and updated caveats: <https://tools.cisco.com/bugsearch/search>.

## For Best Bug Search Tool Results

For best results when using the Bug Search Tool:

- In the **Product** field, enter Cisco Cloud Services Router 1000v.
- In the **Releases** field, enter one or more Cisco IOS XE releases of interest. The search results include caveats related to any of the releases entered in this field.

The tool provides autofill while you type in these fields to assist in entering valid values.

Releases beginning with **3.x** have an equivalent release number beginning with **15.x**, as shown in the following table. Include the **15.x** equivalent to ensure that all relevant caveat results are displayed.

Releases for Cisco IOS XE Denali 16.x, such as Cisco IOS XE Denali 16.3.1 do not have equivalent 15.x releases; for example a search using release number **16.3.1** should find the caveats for Cisco IOS XE Denali 16.3.1.

**Table 2** Release Number Equivalents for Cisco IOS XE 3S Releases

For...	...search using the following equivalent release numbers
3.14	3.14 and 15.5(1)
3.15	3.15 and 15.5(2)
3.16	3.16 and 15.5(3)
3.17	3.17 and 15.6(1)

**Field Notices**

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

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

**Caveats: Cisco IOS XE Denali 16.3.9****Open Caveats—Cisco IOS XE Denali 16.3.9**

Caveat ID Number	Description
<a href="#">CSCvi28402</a>	Stateful features enhancement for big flow (Elephant flow) -CFT infra dependency
<a href="#">CSCvn03502</a>	SR: CFLOW input intf index is 0xffffffff for Service-engine DSP module interface
<a href="#">CSCvn78961</a>	Subscribers cannot re-login due to CoA time-out (lite-sessions in routed mode)
<a href="#">CSCvo20934</a>	FMAN crash due to Flexible Netflow (fnf)
<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="#">CSCvp86216</a>	Router ucode crash with NAT with interface flap

**Resolved Caveats—Cisco IOS XE Denali 16.3.9**

Caveat ID Number	Description
<a href="#">CSCvb22637</a>	nginx crashes when username containing formatted string logs into WebUI
<a href="#">CSCve47826</a>	Memory leak Crypto IKEv2 at ikev2_ios_psh_set_route_info
<a href="#">CSCvf25402</a>	Incorrect handling of SIGVTALRM (signal 26)
<a href="#">CSCvh11088</a>	Crash on OPF_CSR32_OPF_LOGIC_ERR_LEAF_INT__INT_START_OF_BURST_MARKER_ERR
<a href="#">CSCvj28921</a>	High CPU due to Alignment Corrections - SMEF & IWAN

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvk17998</a>	Rekey Timer are same for both the Server and Client
<a href="#">CSCvk53405</a>	Router crash - AFW_application_process
<a href="#">CSCvm51112</a>	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys
<a href="#">CSCvn00104</a>	Software crash due to memory corruption after packet trace was enabled.
<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="#">CSCvn37237</a>	ASR1002-HX crashed after huge traffic is transmitted over it
<a href="#">CSCvn53969</a>	Memory leak in SMD process due to AAA Idle-timer not being freed
<a href="#">CSCvn78349</a>	FlexVPN with password encryption - keyring aaa LIST password 6 xxxxx encrypted again upon reload
<a href="#">CSCvo03458</a>	PKI "revocation check crl none" does not fallback if CRL not reachable
<a href="#">CSCvo27553</a>	PKI incorrect fingerprint calculation during CA authentication
<a href="#">CSCvo42379</a>	ASR1000 / ISR4300 Console Hang with line speed set to 115200 in 16.3
<a href="#">CSCvo43897</a>	ISR 4331, wrongly adding to Port to subscriber field after translation.
<a href="#">CSCvo46127</a>	MaxSusRate is not working with service class
<a href="#">CSCvo47866</a>	Crash at Process = SCCP Auto Config
<a href="#">CSCvo66216</a>	IPSec-Session count in "show crypto eli" reaches max causing VPN failure
<a href="#">CSCvo67856</a>	in.telnetd process consumes 100% CPU in show process cpu platform sorted
<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="#">CSCvo94468</a>	%PERF_MON_ASYNC-3-MEM: Memory cleanup failed - ssrc db cache results in PMI not created on BR
<a href="#">CSCvo99156</a>	Unexpected reload in btrace routines due to division by NULL.
<a href="#">CSCvp00579</a>	bqs may select an inaccurate rate
<a href="#">CSCvp59848</a>	ASR1001-x crash while configuring policy-map
<a href="#">CSCvp63616</a>	Crash due to too many DSPs
<a href="#">CSCvp92334</a>	Crash after Media monitor look up.

## Caveats: Cisco IOS XE Denali 16.3.8

### Resolved Caveats—Cisco IOS XE Denali 16.3.8

Caveat ID Number	Description
<a href="#">CSCva46032</a>	FlexVPN: Hostname in DHCP is incorrect when using AnyConnect
<a href="#">CSCvi01558</a>	iBGP dynamic peer using TTL 1
<a href="#">CSCvi65958</a>	Standby RP crashes due to shortage of memory when running OSPF
<a href="#">CSCvi74088</a>	link local multicast packets are received when the SVI is in down state
<a href="#">CSCvj91448</a>	PKI:-IP address parsing issue while printing the subject name if classless IP is used in Trustpoint
<a href="#">CSCvj95351</a>	OSPF SR uloop : After issuing "clear ip ospf process". ospf process crashed.
<a href="#">CSCvk12152</a>	Unable to remove command 'ip nat inside destination'
<a href="#">CSCvk16771</a>	ISIS for IP is enabled/installing routes in the RIB while IP routing is disabled
<a href="#">CSCvk41664</a>	CSR1000v: crash at mempool_add_region when adding memory
<a href="#">CSCvk42631</a>	CSR1000v running inside Citrix XenServer 7.0 crashed
<a href="#">CSCvk45884</a>	BGP 'address-family ipv4' sub-configuration is not shown in the running configuration
<a href="#">CSCvm19399</a>	CRL file is getting overwritten when PKI server turns up after reload
<a href="#">CSCvm65384</a>	SNMP OID conflict.Trap being generated with wrong oid 6999.it should be 854
<a href="#">CSCvm74894</a>	PKI authentication should proceed even if GetCACaps return any http failure
<a href="#">CSCvm76452</a>	IPSec background crash while sending SNMP trap
<a href="#">CSCvn41467</a>	Recommit of CSCvm99778 - eca/ewlc/qwlc/mewlc Sanity : AP join failed.

## Caveats: Cisco IOS XE Denali 16.3.7

### Open Caveats—Cisco IOS XE Denali 16.3.7

Caveat	Description
<a href="#">CSCva00765</a>	crash after no ipv4 multicast multitopology command
<a href="#">CSCvh23735</a>	CSR1000v HA vCUBE IP-4-DUPADDR detected after Active router goes down.
<a href="#">CSCvi35960</a>	VRF aware CUBE fails to send OOD OPTIONS pings
<a href="#">CSCvj72854</a>	Router crash due to NHRP process Segmentation fault(11)
<a href="#">CSCvj90089</a>	Crash while doing a conference call
<a href="#">CSCvk07838</a>	CUBE is using wrong source IP address to send SIP error
<a href="#">CSCvk10633</a>	bgp crash while running show command and same time bgp peer reset
<a href="#">CSCvk22449</a>	BGP Traceback/Crash seen with 20k IPv4 BGP scale after reload/clearing bgp

## Resolved Caveats—Cisco IOS XE Denali 16.3.7

**Table 3**

<b>Caveat</b>	<b>Description</b>
<a href="#">CSCvd04871</a>	Crash after IWAN does a recalculation in the RIB
<a href="#">CSCvd14310</a>	IP TUNNELS: Overlapping Loopback Interface Causes Incorrect Forwarding Decision with AppNav and PfR
<a href="#">CSCve56437</a>	Router runs Denali 16.3.x may crash with AFW_application_process when sip call disconnect
<a href="#">CSCvf84349</a>	Router crash on polling cEigrpPeerEntry
<a href="#">CSCvg05452</a>	IOS-XE router crash from memory corruption during CCB cleanup
<a href="#">CSCvg09010</a>	KS merge fails for groups with TBAR due to PST update failure on primary KS
<a href="#">CSCvg30991</a>	IOS-XE routers: Memory leak observed on process ivr: peer_item_t in AFW_application_process
<a href="#">CSCvg34731</a>	IOS-XE MOS scores always show 4.x even with massive packet loss.
<a href="#">CSCvg94908</a>	Mgig stack keeps crashing while configuring with Radius commands
<a href="#">CSCvg95562</a>	CENT: branch MC crashed @ cent_pdp_msg_send_from_pickexit after CSCup19724
<a href="#">CSCvg97010</a>	load-balance advanced moving traffic to fallback path when primary path are not over utilized
<a href="#">CSCvh14715</a>	CVLA crash on memory merge scan task
<a href="#">CSCvh85788</a>	Local LAN-only prefix present in master route-import table but not present in site prefix DB
<a href="#">CSCvi01745</a>	cpp_cp_svr crashes, causing reload
<a href="#">CSCvi02816</a>	ZBF not able to identify the WAAS optimized flow and drops ACK
<a href="#">CSCvi11065</a>	Router cpp_cp_svr process crashes at cpp_qm_event_parent_event_create
<a href="#">CSCvi12657</a>	BQS pending deferred is stuck
<a href="#">CSCvi13062</a>	FP cpp_cp_svr crash @cpp_bqs_srt_yoda_place_child
<a href="#">CSCvi32156</a>	Router crashes when DMVPN tunnel moves across ports
<a href="#">CSCvi56463</a>	Unexpected Reset, Crypto IKMP Segmentation fault with IPsec AAA Configuration
<a href="#">CSCvj03263</a>	H225 gatekeeper request dropping under "ALG_PARSER" with ZBF
<a href="#">CSCvj27172</a>	Crash during Generic Call Filter Module cleanup
<a href="#">CSCvj70568</a>	FlexVPN    DHCP entries not flushing for ikev2 timed out reconnect sessions

## Caveats: Cisco IOS XE Denali 16.3.6

### Open Caveats—Cisco IOS XE Denali 16.3.6

*Table 4*

Caveat	Description
<a href="#">CSCvf80757</a>	NETCONF-YANG/RESTCONF edit config fails silently, subsequent get config reports false-positive
<a href="#">CSCvg05452</a>	IOS-XE router crash from memory corruption during CCB cleanup
<a href="#">CSCvg94600</a>	crash with "debug platform condition ipv4 access-list "
<a href="#">CSCvh47124</a>	NextHop is wrong in route-import table on branch when delete WAN interface and reconfigure it

### Resolved Caveats—Cisco IOS XE Denali 16.3.6

*Table 5*

Caveat	Description
<a href="#">CSCUw85826</a>	Evaluation of Cisco IOS and IOS-XE1 for NTP_October_2015
<a href="#">CSCux86075</a>	Unexpected crash during SSH operation
<a href="#">CSCva46459</a>	SSH session hangs if it is not closed properly
<a href="#">CSCva92216</a>	BGP session is reset when unrecognized capability received in OPEN message
<a href="#">CSCvb34443</a>	IKEv2 fragmentation not working with aes-gcm encryption - hmac failure
<a href="#">CSCvb53469</a>	Ephone-DN remains in down state when restart all is given in telephony-service
<a href="#">CSCvb65024</a>	LDAP authentication reuses old TCP connection
<a href="#">CSCvc18534</a>	Incorrect Radius Server Status when locally defined user called in tester command
<a href="#">CSCvc26134</a>	self-generated packets sent fail over PMIP-MUDP tunnel in LMA
<a href="#">CSCvc61653</a>	Polaris: polaris memory leak in btrace thread deletion: cli_agent.
<a href="#">CSCvc63958</a>	SIP CME relays out "Authorization: header" received from IP Phone.
<a href="#">CSCvc77378</a>	Glare condition exists for mid call DO INVITE when CUBE receives in-dialogue SIP OPTIONS message
<a href="#">CSCvd11419</a>	Configuring Packet tracer on IOS-XE triggers a crash intermittently
<a href="#">CSCvd16501</a>	High CPU due to SNMP ENGINE when polling mplsTunnelHopEntry
<a href="#">CSCvd64670</a>	SCEP enrollment failing with HTTP/1.1 500 Internal Error
<a href="#">CSCvd80837</a>	Crash observed in DHCP SIP
<a href="#">CSCve09104</a>	Command "segment-routing mpls" under router isis 1 not getting NVGEN'd
<a href="#">CSCve54486</a>	Crash when attempting to assign nonexistent/shutdown VLAN to 802.1x port

**Table 5** (continued)

<b>Caveat</b>	<b>Description</b>
<a href="#">CSCve55089</a>	BGP crashes at bgp_ha_sso_enable_ssomode
<a href="#">CSCve57506</a>	IPv6 ESP traffic incorrectly dropped after decryption by IPv6 interface access-list
<a href="#">CSCve59906</a>	router crash with "param long-dur-action disconnect"
<a href="#">CSCve74806</a>	Standby Router crash when there is a m-line shrink case within the dialog.
<a href="#">CSCve75919</a>	In-dialog options ping received post ACK (call completion) cause cube to change codec and no audio
<a href="#">CSCvf05864</a>	BGP RR changes tunnel parameters for bgp evpn route type 3
<a href="#">CSCvf16338</a>	voiprtp_register_transport_port_manager_and_reserve: Alloc ports failed, min: 8000, max: 48199 248
<a href="#">CSCvf16448</a>	No all IPv6 GRE crypto tunnels may come up or recover from flapping at scale
<a href="#">CSCvf24607</a>	Ipsec Session Fail After Up/down Link Between Dmvpn Tunnel
<a href="#">CSCvf24928</a>	QFP exmem memory leak in cpp_fm_sce_result_chunk
<a href="#">CSCvf31368</a>	router crash after EEM-wanfailover script triggered
<a href="#">CSCvf33947</a>	CUBE can't handle mid-call re-invite when midcall-signalling passthrough mediachange is configured
<a href="#">CSCvf35507</a>	Crash in SSH Process due to SCP memory corruption
<a href="#">CSCvf36269</a>	Cisco IOS and IOS XE Software Plug-and-Play PKI API Certificate Validation Vulnerability
<a href="#">CSCvf36888</a>	IOS-XE DMVPN Per-tunnel QoS not working on Cisco CSR 1000v without AX license
<a href="#">CSCvf39474</a>	GETVPN: TBAR sync "timer is not running" after KS upgrade causing anti-reply drops and GM outages
<a href="#">CSCvf43271</a>	Traceback: Stack master crash at dot1x authentication
<a href="#">CSCvf48159</a>	Router crash during T38 fax bitrate negotiation
<a href="#">CSCvf60862</a>	Cisco IOS and IOS XE Software IOS daemon Cross-Site Scripting Vulnerability
<a href="#">CSCvf63269</a>	After on the vnic edit on the fly changes - LAN-SRIOV sub interface ping fails after Reboot of ISRv
<a href="#">CSCvf63541</a>	BGP w/global import/export crashes when several nbrs deleted simultaneously
<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="#">CSCvf74829</a>	CRL download fails due to "failed to create getcacert message"
<a href="#">CSCvf80495</a>	IPv6 BGP network advertized not seen in the peer
<a href="#">CSCvf89608</a>	Missing ip route to cellular interface after router reload or modem power cycle
<a href="#">CSCvf89894</a>	GETVPN // Primary KS sending rekey first to GM's and then to Secondary KS via scheduled rekey.
<a href="#">CSCvf95077</a>	Stale Mac entry in MLRIB
<a href="#">CSCvf96035</a>	ISIS redistribute connected not working for IPV6 routes
<a href="#">CSCvg02533</a>	router crashed after triggers with debug



**Table 5** (continued)

<b>Caveat</b>	<b>Description</b>
<a href="#">CSCvg05896</a>	IWAN EIGRP SAF - seq number mismatch after branch reload
<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="#">CSCvg20200</a>	Polaris: Crash observed while client association with key-wrap enabled in controller.
<a href="#">CSCvg21440</a>	Memory leak with DMVPN tunnel protection ipsec
<a href="#">CSCvg28395</a>	Crash when doing snmp walk for ipAddressEntry
<a href="#">CSCvg31493</a>	Stale Mac entry in MLRIB additional fix
<a href="#">CSCvg45247</a>	Site-prefix learning: Unexpected Reboot in 'IP RIB Update' Process after 'no domain default'
<a href="#">CSCvg52560</a>	Traceback: OCSP creates a large number of lists and triggers a memory problem
<a href="#">CSCvg60288</a>	Device IP address AV pair replaced with 192.168.1.5
<a href="#">CSCvg74048</a>	PKI: All SCEP requests fail with "Failed to send the request. There is another request in progress"
<a href="#">CSCvg75380</a>	Polaris 16.3.5: Unexpected Reboot with Device Classifier enabled
<a href="#">CSCvg76912</a>	CFD: pnp config upgrade failed when IFS returns size 0 for all TFTP files
<a href="#">CSCvg84039</a>	Traceback: Crash on WAAS menu prompt for WAN Interface
<a href="#">CSCvg85879</a>	BGP sets the wrong Local Preference for routes validated by RPKI server
<a href="#">CSCvg90226</a>	Crypto Traceback: Router crash at 'Crypto Support' segmentation fault
<a href="#">CSCvg92437</a>	AToM: MSPW VC Down with Reason as No VC Remote Label Binding Received on RP SSO
<a href="#">CSCvg94978</a>	CUBE Router crashed - Critical software exception, Process = CCH323_CT
<a href="#">CSCvg98890</a>	IOS-XE GM router might crash after the rekey method is changed from unicast to multicast
<a href="#">CSCvh00038</a>	Device IP address AV pair replaced with 192.168.1.5
<a href="#">CSCvh05611</a>	IOSd crash while applying dial peer configuration
<a href="#">CSCvh17481</a>	PKI: Device crash during crl download with multiple CDP URI
<a href="#">CSCvh24315</a>	Memory leak for CCSIP_TCP_SOCKET and CCSIP_UDP_SOCKET on CUBE
<a href="#">CSCvh47443</a>	Spoke-to-spoke site-prefix reachability checking should be removed
<a href="#">CSCvh53691</a>	FP crash with scaled IKE sessions.
<a href="#">CSCvh60525</a>	CLI 'aaa common-criteria' not available on IPBASEK9 license

## Caveats: Cisco IOS XE Denali 16.3.5

### Open Caveats—Cisco IOS XE Denali 16.3.5

*Table 6*

<b>Caveat</b>	<b>Description</b>
<a href="#">CSCvf81695</a>	ASR1K encryption processor trace file is not valid
<a href="#">CSCvf60961</a>	BGP scanner crashed with add/remove command <code>bgp mpls-local-label</code>
<a href="#">CSCvg05896</a>	IWAN EIGRP SAF - seq number mismatch after branch reload
<a href="#">CSCvd11419</a>	Configuring Packet tracer on IOS-XE triggers a crash intermittently
<a href="#">CSCvg09010</a>	KS merge fails for groups with TBAR due to PST update failure on primary KS
<a href="#">CSCuz16455</a>	ISIS SR: Subtract 3 instead of 2 from PD maximum label support for TILFA
<a href="#">CSCvg03683</a>	ASR1K CGN NAT ASR1K ESP100 crashed with clear ip nat translation *

## Resolved Caveats—Cisco IOS XE Denali 16.3.5

**Table 7**

<b>Caveat</b>	<b>Description</b>
<a href="#">CSCvf01501</a>	NBAR data-plane crash for DNS TXT query with an additional record
<a href="#">CSCvc58538</a>	BGP crashes when removing advertise-map
<a href="#">CSCvd90251</a>	Duplicate BGP prefixes are not dropped
<a href="#">CSCve68911</a>	Nested Enhanced Route Refresh requests triggers Stale Prefixes
<a href="#">CSCuz20869</a>	RFC: BGP sending error sub-code: '8' instead of '4'
<a href="#">CSCvf62916</a>	Router crashes when doing "show ip bgp neighbor" on a flapping BGP neighborship
<a href="#">CSCve51657</a>	Slow convergence with scale after a core link flaps
<a href="#">CSCvf24713</a>	stale path message for that prefix is noticed when dampening is configured
<a href="#">CSCvd19860</a>	OSPFv3 AUTH breaks IPv6 traffic intermittently
<a href="#">CSCve83012</a>	CSR 1000v: Core Files during extended operation - 1vCPU CSR 1000v ESXI vSwitch
<a href="#">CSCvb86484</a>	wrong EIGRP redistribution statement in startup config breaks BGP settings after router reload
<a href="#">CSCvf81579</a>	ASR1K: IOSd crash in kmi initial_check on null map dereference
<a href="#">CSCve10917</a>	IPSec crash on ASR1K router while processing KMI
<a href="#">CSCvd99474</a>	IPsec: For sVTI after rekey old SAs are not getting deleted
<a href="#">CSCvf11237</a>	Memory leak seen@crypto ainit_show_instance
<a href="#">CSCve87898</a>	Session coming up late after RP failover due to PD delay in polaris
<a href="#">CSCvc78492</a>	DMVPN : IOS-XE - Unable to pass traffic if spoke to spoke fails to build in phase 2
<a href="#">CSCvf34835</a>	IOS-XE GETVPN KS crashes while sending cgmGdoiKeyServerRegistrationComplete trap after GM reg
<a href="#">CSCve20850</a>	ASR1K is unable to recover from the tunnel flapping at scale for IKEv2 dmVPN/BGP
<a href="#">CSCvb75167</a>	Crash in Crypto IKEv2 process
<a href="#">CSCvd54358</a>	Dynamic routes don't get propagated if old session is present in In-Active state.
<a href="#">CSCvc78694</a>	Ikev2 SA INIT queue CLI : Fix default behavior
<a href="#">CSCve07263</a>	IPSec Tunnel stuck in Up/Down state after shut/no-shut - VPN Interop
<a href="#">CSCuz15131</a>	dqueue not empty prior to destruction crashes ipv4fib_les_switch_wrapper
<a href="#">CSCvd97524</a>	Fixed versions for CSCuz15131 crash when traffic with maximum size is on wire
<a href="#">CSCuy09470</a>	ISIS hello stops to be sent after RSP switchover
<a href="#">CSCvd21785</a>	ISIS RIB and Global RIB out of sync resulting in complete traffic loss
<a href="#">CSCve47374</a>	Assert stop processing leaks memory
<a href="#">CSCvd72530</a>	ASR1K configured as PxTR crashes when booted with 16.5.1 image at LISP fwd background process
<a href="#">CSCvd47567</a>	Unexpected reboot with NAT and Multicast configured

**Table 7** (continued)

<b>Caveat</b>	<b>Description</b>
<a href="#">CSCve98696</a>	Interoperability issue of 16.3.4 with other releases
<a href="#">CSCve86613</a>	IOSXE-RP Punt Service Process crash @ __be_fmm_flow_int_table_entry_compare
<a href="#">CSCve61713</a>	PfRv3: Crash in Route-Control Process
<a href="#">CSCve14782</a>	PfRv3: Crash Observed While Checking/Modifying Channel Prefixes
<a href="#">CSCve43611</a>	PfRv3: Multiple TCAs Logged Simultaneously May Lead to Crash
<a href="#">CSCvf29213</a>	PFRV3: Site Prefix shows unreachable after removing and adding the specific route for the prefix
<a href="#">CSCve80719</a>	Site-prefix learning: Prefix withdrawal not working for hub-> branch on 16.6
<a href="#">CSCve92511</a>	Site-prefix of Peer BR is not synchronized after shut/no shut BR border
<a href="#">CSCve15722</a>	The second and later PfRv3 VRF configs are missing after reload
<a href="#">CSCvf51341</a>	Crash after show ip ospf database summary command
<a href="#">CSCvd48206</a>	OSPF TILFA SCALE: On reopt or clearing OSPF process, no. of protected prefixes goes down drastically
<a href="#">CSCvd73491</a>	OSPF TILFA SCALE: with 2K Inter-area Prefix Scale, some non-ECMP routes are not getting protected
<a href="#">CSCvd40276</a>	OSPF: Not able to remove ospfv3 config under Virtual-Template
<a href="#">CSCvd38714</a>	OSPF: When anycast present in two areas, when one area is removed, rout not getting installed in RIB
<a href="#">CSCvd67254</a>	Crash during CRL fetch failure
<a href="#">CSCvd38619</a>	EST client pki authentication request goes out to default URL always
<a href="#">CSCve29882</a>	EST client pki simpleenroll request goes out to default URL always
<a href="#">CSCve53984</a>	ISR 4300 crashed while importing certificate
<a href="#">CSCvd69749</a>	PKI Server: "Rollover RA Certificate" Becomes "Rollover ID Certificate" After Reload of Router
<a href="#">CSCve52258</a>	Both ESP crash on changing COS type on ATM VC
<a href="#">CSCve42512</a>	Both ESP crash on changing shaper rate under port-channel
<a href="#">CSCve48009</a>	cpp_cp_svr crash seen on ASR1002-X and device keeps rebooting with 16.5.1b
<a href="#">CSCve49596</a>	fp crash while changing port-channel from vlan based mode to LACP
<a href="#">CSCve40432</a>	Yoda: Collapse HQF Aggregation Node
<a href="#">CSCve76827</a>	large NAT policy-map takes long time to download
<a href="#">CSCvf74154</a>	SGACL: cpp_sp_svr crash during CFM EDIT request with reseq_enable = TRUE
<a href="#">CSCvd72277</a>	[UniScale]asr1k peers crashed while unconfiguring testbed devices in IPSEC IPv6 Ikev2/SCM
<a href="#">CSCve08943</a>	QFP sorter interrupts related to REAL_DISTANCE are fatal when they should be informational
<a href="#">CSCve98056</a>	ESP ucode crash with ALG for PPTP traffic and PAP is enabled.
<a href="#">CSCva28875</a>	NAT ALG fails on Multipart SIP Header

**Table 7** (continued)

<b>Caveat</b>	<b>Description</b>
<a href="#">CSCvf18162</a>	Crash observed in Mlpp-Bacd scenario
<a href="#">CSCve71893</a>	ISR4K - Hoot and Holler multicast replication issue
<a href="#">CSCve21448</a>	multiple ISR4K VGW's crashed with Segmentation fault(11), Process = DSMP
<a href="#">CSCut98625</a>	ASSERTION FAILED : ..vtsp.c: vtsp_cdb_assert: then crash
<a href="#">CSCuy68013</a>	Switch crashed after add "ip wccp 61 global" command during traffic

## Caveats: Cisco IOS XE Denali 16.3.4

### Open Caveats—Cisco IOS XE Denali 16.3.4

**Table 8**

<b>Caveat</b>	<b>Description</b>
<a href="#">CSCve09469</a>	CSR 1000v Crash due to length inconsistency
<a href="#">CSCvd69608</a>	ASR 1000v crashes at PPP process on pushing 4 or more per-user static IPv6 routes
<a href="#">CSCvc58538</a>	BGP crashes when removing advertise-map
<a href="#">CSCve32217</a>	Crash due memory corruption in AFW
<a href="#">CSCve44393</a>	ASR 1006 crashes due watchdog in the DHCP client process
<a href="#">CSCve13491</a>	Router might crash due watchdog when creating a new swidb at if_index_allocate_index
<a href="#">CSCur42069</a>	CUBE crashed when "sh sip-ua calls br" command entered
<a href="#">CSCve08418</a>	IPsec/IKEv2 Installation Sometimes Fails With Simultaneous Negotiations
<a href="#">CSCvd06688</a>	Traceback: loop in Crypto ACL creates CPUHOG then crash at large scale
<a href="#">CSCvc46230</a>	PfRv3: Unexpected Reload While Evaluating/Moving TC's Between Channels
<a href="#">CSCve59906</a>	Router crashes with "param long-dur-action disconnect"

### Resolved Caveats—Cisco IOS XE Denali 16.3.4

**Table 9**

<b>Caveat</b>	<b>Description</b>
<a href="#">CSCus85486</a>	CSR1000v Default Licence of 0.1Mbps blocking running IWAN on CML
<a href="#">CSCvc14951</a>	CSR 1000v crashes cpp_mma_policy_isd_free_exmem_entry

**Table 9**

Caveat	Description
<a href="#">CSCvd58678</a>	CSR 1000v configured with large mtu crashes during sweeping ping
<a href="#">CSCvc33794</a>	CSR 1000v HA Checkpointing Broken for Video Calls with SDP Pass-Thru
<a href="#">CSCvd47757</a>	CSR 1000v is not able to poll CISCO-IPSEC-FLOW-MONITOR-MIB
<a href="#">CSCvd31118</a>	Reduce impact of fingerprinting code on NVRAM access
<a href="#">CSCvb21929</a>	ping fail under pppoe configuration
<a href="#">CSCvd61632</a>	"distance bgp 255 0 0" getting conf under IPv6 AF after some sequence of steps
<a href="#">CSCvc89965</a>	After reload route policy processing not re-evaluate with route-map using match RPKI
<a href="#">CSCvc99820</a>	BGP crashed configuring different update-source interface with v6 LL peering
<a href="#">CSCvd09584</a>	eVPN PMSI VNI decoding / encoding as MPLS label
<a href="#">CSCvd16828</a>	High CPU due to periodic route refresh to VPN peers using rtfiler AF
<a href="#">CSCvd15140</a>	Router crashes using show BGP commands
<a href="#">CSCvd43437</a>	Wrong Source IP Selection for eBGP in EVN/VNET environment
<a href="#">CSCvb20224</a>	Router crashes on configuring bandwidth on the Dialer interface
<a href="#">CSCuy27746</a>	CDP packet causes switch to crash due unexpected exception to CPUvector
<a href="#">CSCvd58678</a>	CSR1000v configured with large mtu crashes during sweeping ping
<a href="#">CSCvc96709</a>	Crash using EIGRP and DVTI with IKEv2
<a href="#">CSCvc65604</a>	VNET global vrf neighbor is down after an interface flap
<a href="#">CSCvc14385</a>	Missing FIB subblock causes crash when configuring vrf
<a href="#">CSCvd58820</a>	Need API for ip best source address for given outgoing interface
<a href="#">CSCvc35453</a>	ISATAP Server feature broken on ASR1K
<a href="#">CSCuz63888</a>	Crash in "show ipc all" @ ipc_print_ports_internal
<a href="#">CSCvc66912</a>	CUBE Ent crashes when Diversion header received with no user portion and 'history-info' enabled
<a href="#">CSCvc34235</a>	"crypto ipsec fragmentation before-encryption" command disappears after reload
<a href="#">CSCvd40880</a>	Modifying crypto ACL leads to a removal of crypto map config
<a href="#">CSCvc09368</a>	Crash at update of context nhrp
<a href="#">CSCvc35196</a>	Behavior difference between XE3.17 and Polaris
<a href="#">CSCvc59750</a>	IKEv2 Aggregate-auth Timing Issue
<a href="#">CSCvd69373</a>	IKEv2: Unable to initiate IKE session to a specific peer due to 'in-neg' SA Leak
<a href="#">CSCvd39741</a>	IOS IKEv2 profile NVgen local auth is rejected from startup configuration upon reload
<a href="#">CSCvd25106</a>	2nd isis instance crashes after configuring new connected-prefix-sid-map due to no instance PDB
<a href="#">CSCvc51408</a>	ISIS route oscillation due to ldp sync and interface max metric
<a href="#">CSCvc15923</a>	L2TP Account accuracy: SSS disconnect ACKs are not received for few sessions
<a href="#">CSCvc17525</a>	complete traffic drop with DATA MDTs with latest polaris_dev

Table 9

Caveat	Description
<a href="#">CSCvd58678</a>	CSR 1000v configured with large mtu crashes during sweeping ping
<a href="#">CSCvc33794</a>	CSR 1000v HA Checkpointing Broken for Video Calls with SDP Pass-Thru
<a href="#">CSCvd47757</a>	CSR 1000v is not able to poll CISCO-IPSEC-FLOW-MONITOR-MIB
<a href="#">CSCvd31118</a>	Reduce impact of fingerprinting code on NVRAM access
<a href="#">CSCvb21929</a>	ping fail under pppoe configuration
<a href="#">CSCvd61632</a>	"distance bgp 255 0 0" getting conf under IPv6 AF after some sequence of steps
<a href="#">CSCvc89965</a>	After reload route policy processing not re-evaluate with route-map using match RPKI
<a href="#">CSCvc99820</a>	BGP crashed configuring different update-source interface with v6 LL peering
<a href="#">CSCvd09584</a>	eVPN PMSI VNI decoding / encoding as MPLS label
<a href="#">CSCvd16828</a>	High CPU due to periodic route refresh to VPN peers using rfilter AF
<a href="#">CSCvd15140</a>	Router crashes using show BGP commands
<a href="#">CSCvd43437</a>	Wrong Source IP Selection for eBGP in EVN/VNET environment
<a href="#">CSCvb20224</a>	Router crashes on configuring bandwidth on the Dialer interface
<a href="#">CSCCuy27746</a>	CDP packet causes switch to crash due unexpected exception to CPUvector
<a href="#">CSCvd58678</a>	CSR1000v configured with large mtu crashes during sweeping ping
<a href="#">CSCvc96709</a>	Crash using EIGRP and DVTI with IKEv2
<a href="#">CSCvc65604</a>	VNET global vrf neighbor is down after an interface flap
<a href="#">CSCvc14385</a>	Missing FIB subblock causes crash when configuring vrf
<a href="#">CSCvd58820</a>	Need API for ip best source address for given outgoing interface
<a href="#">CSCvc35453</a>	ISATAP Server feature broken on ASR1K
<a href="#">CSCCuz63888</a>	Crash in "show ipc all" @ ipc_print_ports_internal
<a href="#">CSCvc66912</a>	CUBE Ent crashes when Diversion header received with no user portion and 'history-info' enabled
<a href="#">CSCvc34235</a>	"crypto ipsec fragmentation before-encryption" command disappears after reload
<a href="#">CSCvd40880</a>	Modifying crypto ACL leads to a removal of crypto map config
<a href="#">CSCvc09368</a>	Crash at update of context nhrp
<a href="#">CSCvc35196</a>	Behavior difference between XE3.17 and Polaris
<a href="#">CSCvc59750</a>	IKEv2 Aggregate-auth Timing Issue
<a href="#">CSCvd69373</a>	IKEv2: Unable to initiate IKE session to a specific peer due to 'in-neg' SA Leak
<a href="#">CSCvd39741</a>	IOS IKEv2 profile NVgen local auth is rejected from startup configuration upon reload
<a href="#">CSCvd25106</a>	2nd isis instance crashes after configuring new connected-prefix-sid-map due to no instance PDB
<a href="#">CSCvc51408</a>	ISIS route oscillation due to ldp sync and interface max metric
<a href="#">CSCvc15923</a>	L2TP Account accuracy: SSS disconnect ACKs are not received for few sessions
<a href="#">CSCvc17525</a>	complete traffic drop with DATA MDTs with latest polaris_dev

**Table 9**

Caveat	Description
<a href="#">CSCvc82325</a>	Crash after the MPLS LDP neighbor flap in the NSR scenario
<a href="#">CSCvd01488</a>	Running command "show policy-map interface" or "show tech nbar" can cause crash
<a href="#">CSCvd41270</a>	Crash on IWAN Hub when TC is uncontrolled and current channel is present
<a href="#">CSCvd36813</a>	Memory Leak due to cent_rt_eigrp_nh_convert
<a href="#">CSCvd29705</a>	PfR Monitoring do not display VRF101 data and reports FVRF incorrectly
<a href="#">CSCvc62532</a>	HTTP connection may fail when IPv6 address is configured on any interface
<a href="#">CSCvc65670</a>	NTP leap second addition/deletion for consecutive leap months not working properly
<a href="#">CSCvc19234</a>	Old Constrained Node Sid not getting deleted from MPLS forwarding table on changing SID
<a href="#">CSCvc12420</a>	OSPF SRTE: CSTR path is not installed in some cases properly.
<a href="#">CSCvc71872</a>	OSPF: IPFRR repair path computation stopped after receiving type 10 opaque EPL lsa.
<a href="#">CSCvc54359</a>	SRTE: Single hope tunnel doesn't install any repair path.
<a href="#">CSCvc23238</a>	SRTE: when i/f address is removed, traceback is seen and adj-sids not destroyed.
<a href="#">CSCvc54211</a>	Tunnel & repair path continuously flapping on disabling SR on next node from head-end.
<a href="#">CSCvd58884</a>	During PKI enrollment, Cisco router rejects CA/RA reply containing HTTP 500 "Internal Server Error"
<a href="#">CSCvd69397</a>	Crash on vtcp parsing in Extended Processing Path for the FIA.
<a href="#">CSCva31708</a>	SR:RSP2:Object download failure(EOS object)error seen randomly
<a href="#">CSCvd68050</a>	CHUNKBADREFCOUNT crash
<a href="#">CSCuz52528</a>	Evaluation of all for OpenSSL May 2016
<a href="#">CSCvb48683</a>	Evaluation of all for Openssl September 2016
<a href="#">CSCvb72458</a>	Router repeatedly crashing with "%UTIL-3-TREE: Data structure error"
<a href="#">CSCvb27784</a>	Router crashes when running the csim start command
<a href="#">CSCvd18792</a>	ISR4K - Hoot and Holler E&M port cannot be co-located with multicast hub

## Caveats: Cisco IOS XE Denali 16.3.3

### Open Caveats—Cisco IOS XE Denali 16.3.3

**Table 10**

Caveat	Description
<a href="#">CSCvc46230</a>	PfRv3: Crash occurs while evaluating/moving TC's between channels.
<a href="#">CSCvc78492</a>	Unable to pass traffic if spoke to spoke fails to build in phase 2.



Table 10

Caveat	Description
<a href="#">CSCvd04871</a>	Crash occurs after IWAN recalculates in the RIB.
<a href="#">CSCvd06688</a>	Traceback: loop in the Crypto ACL process creates a CPUHOG message and then a crash occurs—for a large scale crypto tunnel.

## Resolved Caveats—Cisco IOS XE Denali 16.3.3

Table 11

Caveat	Description
<a href="#">CSCvc13015</a>	AWS CSR: High Availability fails if redundancy is configured before the tunnel interface.

## Caveats: Cisco IOS XE Denali 16.3.1a

### Open Caveats—Cisco IOS XE Denali 16.3.1a

Table 12

Caveat	Description
<a href="#">CSCvc13015</a>	AWS CSR: High Availability fails if redundancy is configured before the tunnel interface.

### Resolved Caveats—Cisco IOS XE Denali 16.3.1a

Table 13

Caveat	Description
<a href="#">CSCuz64902</a>	AWS: CSR csr_mgmt container fails to learn default route
<a href="#">CSCvb29204</a>	BenignCertain on IOS and IOS-XE
<a href="#">CSCvb19326</a>	NTP leap second addition is not working during leap second event

## Caveats: Cisco IOS XE Denali 16.3.1

### Open Caveats—Cisco IOS XE Denali 16.3.1

Table 14

Caveat	Description
<a href="#">CSCuz50549</a>	CSR 1000v may boot with its default configuration because the startup-config fails to be read properly
<a href="#">CSCuz64902</a>	AWS: CSR csr_mgmt container fails to learn default route
<a href="#">CSCuz76369</a>	AWS: CSR crashes, loses connectivity after detaching PMAP interface
<a href="#">CSCva07535</a>	AWS: CSR Crashed after copying configuration file using kron-policy
<a href="#">CSCva11162</a>	CSR 1000v loses configuration after either adding a new interface or deleting an existing interface for VMware ESXi
<a href="#">CSCva20296</a>	CSR 1000v linux_iosd_vxe core seen after Qcow install
<a href="#">CSCva45347</a>	PCIe pass-thru w/ ixgbe driver causes MaxTu drops due to TCP reassembly
<a href="#">CSCuw78735</a>	subsys diff between polaris and MCP_DEV 2015 0615 image
<a href="#">CSCuz09519</a>	CSR Ingress over-subscription not represented by “show controllers”
<a href="#">CSCuz16548</a>	CSR UP performance degrades on ipsec tests (Cisco IOS XE 3.17 to 16.3.1) VMware ESXi vmxnet3
<a href="#">CSCuz16813</a>	CSR1000v performance degradation on several QOS features
<a href="#">CSCuz25548</a>	CSR1000v lost config after reload w read of NVRAM contents failed
<a href="#">CSCuz58508</a>	CSR interfaces do not support user settable MTU
<a href="#">CSCuz58877</a>	1vCPU CSR Perf: ucode_ctl_rx thread hogs
<a href="#">CSCuz64672</a>	Resource service-plane-heavy not take effective with 8vCPU
<a href="#">CSCuz94912</a>	UniScale CSR loses startup config and picks up gw hostname after crash
<a href="#">CSCuz96475</a>	1vCPU CSR scale degradation on 5/28 vs 5/21 Cisco IOS XE Denali 16.3
<a href="#">CSCva13262</a>	AWS: All CSR interfaces are mapped to eth0
<a href="#">CSCva27661</a>	VASI subsystems are not packaged in ipbasek9 image for CSR1K platform
<a href="#">CSCva61456</a>	ENCS - ISRV interface sometimes failed to be brought up
<a href="#">CSCva65218</a>	RestAPI/LICENSE: 500 is returned to use /api/v1/license
<a href="#">CSCva65638</a>	RestAPI/LICENSE: udi in restapi response is different with CLI
<a href="#">CSCva66675</a>	RestAPI/idtoken: wrong expiry-time when POST idtoken
<a href="#">CSCva72743</a>	AWS: CSR 1000V takes long boot time after reload when NTP is configured
<a href="#">CSCva72822</a>	RUN images fails to boot for small and medium option
<a href="#">CSCva74083</a>	RUN images fails to boot for small and medium option
<a href="#">CSCva74176</a>	CSR configured with 8vCPUs, 4GB RAM and 2 NUMA nodes crashes

## Resolved Caveats—Cisco IOS XE Denali 16.3.1

**Table 15**

Caveat	Description
<a href="#">CSCuw34077</a>	ASR1K: FP crash due to poor handling of mem allocation failure in IFDB
<a href="#">CSCuw99060</a>	CSR1000V: log notification on reload when migration from CSL to SL
<a href="#">CSCuw17158</a>	Performance degradation on IPSec, NAT, FW, HQos with RHEL 7.1
<a href="#">CSCuz52914</a>	Openstack: CSR goes in grub mode if Hard Reset

## Related Documentation

For information about the Cisco CSR 1000v Series and associated services, see:  
[Documentation Roadmap for Cisco CSR 1000v Series, Cisco IOS XE 16.](#)

---

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012-2016 Cisco Systems, Inc. All rights reserved.

