Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Everest 16.5

First Published: 2017-04-14

Last Modified: 2018-03-28

About Cisco ASR 1000 Series Aggregation Services Routers

Note Come to the Content Hub at content.cisco.com, where, using the Faceted Search feature, you can accurately zoom in on the content you want; create customized PDF books on the fly for ready reference; and can do so much more...

So, what are you waiting for? Click content.cisco.com now!

And, if you are already experiencing the Content Hub, we'd like to hear from you!

Click the **Feedback** icon on the page and let your thoughts flow!

Cisco ASR 1000 Series Aggregation Services Routers are Cisco routers deployed as managed service provide 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.

Note Cisco IOS XE Everest 16.5.1b is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Everest 16.5 release series.

New Features and Important Notes

New and Changed Information

Note Before you dive into this release's features, we invite you to content.cisco.com to experience the features of the Cisco Content Hub. Here, you can, among other things:

- Create customized books to house information that's relevant only to you.
- Collaborate on notes and share articles by experts.
- Benefit from context-based recommendations.
- Use faceted search to close in on relevant content.

And, if you are already experiencing the Content Hub, we'd like to hear from you!

Click the **Feedback** icon on the page and let your thoughts flow!

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 16.5.1b

No new hardware features were introduced for Cisco ASR 1000 Series in Cisco IOS XE Everest 16.5.1b.

New Software Features in Cisco IOS XE Everest 16.5.1b

The following are the new software features introduced in Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Everest 16.5.1b.

ACI TrustSec Integration

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-16/sec-usr-cts-xe-16-book/cts-aci-intgn.html

Application Hosting

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/datamodels/configuration/xe-16/data-models-xe-16-book.html

Attack Surface Reduction: Display Active TCP Ports

To display all the open ports on a device, use the show ip ports all command in User EXEC or privileged EXEC mode. This command provides a list of all open TCP/IP ports on the system including the ports opened using Cisco networking stack.

The show ip ports all command was integrated into ASR 1000 Series Aggregation Routers for the Cisco IOS XE Everest 16.5.1 release.

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw_book/lsw_s1.html

Autonegotiation Support for SFP-GE-T and GLC-TE

Effective with Cisco IOS XE Everest 16.5.1b, autonegotiation is supported on 1000BASE-T SFP module (SFP-GE-T) and 1000BASE-T SFP module (GLC-TE).

Cisco TrustSec: Externalizing Operational Data (IP-SGT mapping & RBACL permission)

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-16/sec-usr-cts-xe-16-book/cts-exter-oper.html

CUBE Support for SRTP-SRTP and SRTP-RTP Interworking with NGE Cipher Suites

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/srtp-srtp-interworking.html

EEM Enhancements for Actions and Environment Variable Support in Python Policy

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/datamodels/configuration/xe-16/data-models-xe-16-book.html

ERSPAN-on-QinQ-sub-interface

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xe-16/lanswitch-xe-16-book/lnsw-conf-erspan.html

Fast Convergence Support in OSPFv2 and OSPFv3

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16/segrt-xe-16-book/seg-rout-trafc-engg.html

Gx Diameter Support for ISG Sessions

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/configuration/xe-16/isg-xe-16-book/isg-gx-dia-support.html

ICMP Inspection Improvement

With the Internet Control Message Protocol (ICMP) Inspection enhancement, after configuring the icmp unreachable allow command, the ICMP packets are passed through the zone-based firewall (ZBFW) even if the ICMP packets do not have Access Control List (ACL) to match ICMP of type 3.

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-16/sec-data-zbf-xe-16-book/fw-stateful-icmp.html

In Service Model Updates

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/datamodels/configuration/xe-16/data-models-xe-16-book.html

ISIS Segment Routing enhancement - TI LFA FRR, SR-LDP interworking, Adj SID

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16/segrt-xe-16-book/seg-rout-trafc-engg.html

Management & Control: Boot Integrity Visibility

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-16/fundamentals-xe-16-book/bt-it-vis.html

NAT: Port Parity, Range and Preservation

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book/iadnat-addr-consv.html

One Global CLI to Disable Firewall

You can enable or disable firewall on an interface with a single command. To disable the zone-based firewall configurations that have been applied on the interfaces, use the **platform inspect disable-all** command. To enable zone-based firewall on the interfaces, use the **no platform inspect disable-all** command.

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-16/sec-data-zbf-xe-16-book/sec-zone-pol-fw.html

Preboot Execution Environment (PXE) Client

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/datamodels/configuration/xe-16/data-models-xe-16-book.html

Provide the Capability to Select a VXLAN Source Port Range

For detailed information, see the following Cisco document:

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

Scripting: Python 2.7/3.0

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/datamodels/configuration/xe-16/data-models-xe-16-book.html

Segment Routing TE Feature

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16/segrt-xe-16-book/seg-rout-trafc-engg.html

SID-Redist-Default-optimize, SR-TE, SR-TE Static over ip unnumbered---- ISIS SR

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16/segrt-xe-16-book/seg-rout-trafc-engg.html

Smart Licensing

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/csa/configuration/xe-16/csa-xe-16-book/csa-smrt-license.html

Software License Solution

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/csa/configuration/xe-16/csa-xe-16-book/csa-sw-licse-sol.html

SR On Demand Next Hops (ODN) XE - L3 / L3VPN

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16/segrt-xe-16-book/seg-rout-trafc-engg.html

SR-TE Dynamic

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16/segrt-xe-16-book/seg-rout-trafc-engg.html

SR-TE IP Unnumbered support in OSPFv2

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16/segrt-xe-16-book/seg-rout-trafc-engg.html

SR-TE On demand LSP

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16/segrt-xe-16-book/seg-rout-trafc-engg.html

Support Multiple Static VXLAN Ingress-Replication Peers (One to Many Peers)

For detailed information, see the following Cisco document:

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

Tunnel QoS in load-Balancing Scenario

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/xe-16/isw-cef-xe-16-book/isw-cef-load-balancing.html

VFR Support on Default Zone

With Virtual Fragmentation Reassembly (VFR) now enabled on the default zones with Dynamic Multipoint VPN (DMVPN) tunnel and zone-based firewall, there is no drop of traffic when traffic is routed through the DMVPN tunnel.
For detailed information, see the following Cisco document:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-16/sec-data-zbf-xe-16-book/vrf-aware-fw.html

WebUI Behavior

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 the Web User Interface from Cisco IOS XE Everest 16.5.1b:

- Configuring Application Visibility—Enhanced to provide reports in a graphical representation format.
- Troubleshooting—Allows you to troubleshoot some of the basic features.

Important Notes

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

CUBE—SRTP Calls

Cisco IOS XE Everest 16.5.1b is not recommended for Cisco Unified Border Element deployment involving SRTP calls.

Yang Data Models

Effective with Cisco IOS XE Everest 16.5.1b, the Cisco IOS XE YANG models are available in the form of individual feature modules with new module names, namespaces and prefixes. Revision statements embedded in the YANG files indicate if there has been a model revision.

Navigate to *https://github.com/YangModels/yang > vendor > cisco > xe >1651*, to see the new, main cisco-IOS-XE-native module and individual feature modules attached to this node.

There are also XPATH changes for the access-list in the *Cisco-IOS-XE-acl.yang* schema.

The *README.md* file in the above Github location highlights these and other changes with examples.

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

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

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

  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 & 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.

SUMMARY STEPS

1. In your browser, navigate to the Cisco Bug Search Tool.
2. If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.
3. To search for a specific bug, enter the bug ID in the Search For field and press Enter.
4. To search for bugs related to a specific software release, do the following:
5. To see more content about a specific bug, you can do the following:
6. To restrict the results of a search, choose from one or more of the following filters:

DETAILED STEPS

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

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

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

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

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

b) In the Releases field, enter the release for which you want to see bugs.
The Cisco Bug Search Tool displays a preview of the results of your search below your search criteria.

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

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

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

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

Your search results update when you choose a filter.

Caveats in Cisco IOS XE Everest Release 16.5.1b

Open Caveats—Cisco IOS XE Everest Release 16.5.1b

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

Caveat ID Number	Description
CSCvb80572	ASR1000-6TGE : Byte counters reported from physical interface and child subinterface don't match
CSCvd23920	ASR1001-X crashed when add QoS config
CSCvd16970	Packet reordering due to “platform qos port-channel-aggregate”
CSCvd30843	crash @ in __intel_security_check_cookie mcprp_ifdev_oper_up
CSCvc05143	Downlink packet loss observed post RPSO across multiple streams with churn
CSCvd42370	CUBE sRTP-RTP Call failures during bulk calls
CSCvb76594	CT3 SPA controllers not coming UP sometimes after wr erase and reload
CSCvd46418	crash after reload CPE with 255 EID prefix
CSCvc56422	XE316:Prince interface flaps after soft OIR
CSCvc95223	Looped multicast packets on dense-proxy-register border router

Resolved Caveats—Cisco IOS XE Everest Release 16.5.1b

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

Caveat ID Number	Description
CSCvc59128	No kernel core when punt-keepalive crash and “no platform punt-keepalive disable-kernel-core”
CSCuu16717	Speedracer, Kahuna and Nighster images do not support “show software authenticity”
CSCvc07319	Random Netclock error messages appearing on console

Caveat ID Number	Description
CSCvc39890	Applying ACL under ERSPAN session: Port matching using ‘eq’ doesn’t occur
CSCvb56056	MACSEC capable 1G interfaces with CU-SFP mka could not recover when reload router
CSCvc23622	ASR1001x - Fiber SFP LED status remains amber even though line status is up and line protocol is up
CSCvc57589	Source IP of RST from ZBFW due to invalid ACK not translated to PAT IP when inter VRF configured
CSCui24809	“TestErrorCounterMonitor Skipped” diagnostic error on ASR1006
CSCvc47681	Increase Number of Supported DSP Conference Profiles
CSCvb75726	IOS-XE Always Reporting “Returned to ROM by reload”
CSCvd29093	cpp-mcplo-ucode crash decrypting 3821 - 3839 byte ipsec packet
CSCvd04210	IKEV2 Tunnels are flapping, rekey request received from PD, lifetime kilobytes configured
CSCvc06760	ICMP TTL messages not returned properly with NAT
CSCvc71183	ASR1K ESP100 - Both ESP crashing due to cpp_bqs_srt_yoda_place_child_internal: failed to grow tree
CSCvc86594	cpp_cp process crashed cpp_bqs_srt_yoda_destroy_tree
CSCvc83373	cpp_cp process crashes due to sw wdog expiring while creating a queue
CSCvc80135	Crash when bandwidth remaining percent <#> is removed then re-added to a class-map
CSCvc74759	Dual QFP Crash triggered by removing service policy from interface with mixed shaper feature enabled
CSCvd23034	Multiple Parent Events Per Node lead to a crash
CSCvd47310	Secondary SUP keep crashing @ CPP Client process failed
CSCvc79819	ESP100 crashes after manual failover
CSCvc68778	Platform switchport svi command not supported on NIM UCSE
CSCvc76954	“bootup e-lead off” behavior like "no bootup e-lead off”

Caveats in Cisco IOS XE Everest 16.5.2

Open Caveats—Cisco IOS XE Everest Release 16.5.2

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

Caveat ID Number	Description
CSCvf73689	"delay-start" command ignore after "delay-start vrf" command
CSCvf15937	3850 16.3.3 not replying to CoA when connecting to CWA SSID
CSCvd69608	Asr1k crashes at PPP process on pushing 4 or more per-user static ipv6 routes
CSCvd97229	Framed-IPv6-Route attribute is not working for IPv6 full route with leading zeros
CSCve00087	Line-by-Line sync verifying failure on command: client test01 server-key 0 Password
CSCve90164	Observing incorrect server state in BINOS
CSCve96308	Observing memory leak in AAA_MALLOC_LITE
CSCve90160	Observing memory leaks in AAA_STRDUP_GREEN_PARSER_SG_NAME1
CSCvf83231	Cat3650 RADIUS Dynamic VLAN assignment fails for default VLAN
CSCvd90018	PPPoA: NULL LCP Magic value in LCP echo reply
CSCvf41295	Recommit CSCvf09355 - OBFL data not restored for ESP after router reload
CSCvd18432	btelnet consumes 100% CPU
CSCvc21471	kernel: fsid server error fileid changed
CSCux20847	R0/0: kernel: bullseye_i2c_master_xfer Error Repeats Every Hour
CSCve33266	To fix diag counters processing for RP and FP slots
CSCvf92881	cpu got hiked up 100% after scaling 350 sxp connections with 50 IP-SGT bindings in ASR.
CSCvd67775	SGACL does not enforce policy on Virtual Access interfaces
CSCve53263	Configured Speed/Duplex are not supported on Mgmt Eth port
CSCvf59830	ASR1001-HX/ ASR1002-HX/ MIP-100 not able to send dot1q packet in EoMPLS.
CSCuz84374	SPA modules on ASR1002-x show "missing" under show platform

Caveat ID Number	Description
CSCvb64301	ASR1000-6TGE: Too many "Interface TenGigabitEthernet4/0/0, link down due to local fault" logs
CSCvc89102	ASR1000 doesn't send PPP ECHO Reply
CSCvd63476	Changing autoneg setting on ASR1K cause link failure on subsequent link flap (connected to 2960XR)
CSCvc39443	router may crash with ZBFW ACL modification
CSCvd10362	Deletion of channel-group failed on QFP when FR encaps set on associated Serial Int.
CSCvf65522	ESP crashed - double_exception_has_occured - malformed PIM packet over GRE tunnel & ERR_DTL_INV_ADDR
CSCvc88274	ASR1004 -3.16.4aS: Continuous IKE error messages and 2000 BGP session goes down
CSCvc92936	Crypto map decrypts transit ESP traffic in IOS-XE
CSCvb86438	IOS-XE IPSec serviceability - Conditional droptype debug not working consistently
CSCvf80163	ASR1K crashes due to crypto microcode with no corefile/crashinfo
CSCvf81650	ASR1K encryption processor cores written to tracelogs
CSCvf81695	ASR1K encryption processor trace file is not valid
CSCvf89430	IOS shim free obj id AVL DB loop causing watchdog crash
CSCvc83900	MIB counter, ipIfStatsHCOutOctets, does not show correct value
CSCvf90614	ASR1k Regarding ifHCInBroadcastPkts value decreasing
CSCvd18323	AVC Server Response Time Reports Negative Values Occasionally
CSCvb46429	QFP ucode crash on ISR4300 with IWAN
CSCvc15571	ISR4K:applying MPLS-TE command on an interface stops traffic completely
CSCvc83037	ESP crash while doing NAT ALG
CSCve10486	Inbound H323 call fails
CSCvd95309	Incorrect IP NAT translations
CSCvf49912	NAT stops working for virtual interface
CSCve32391	Ports are not freed for non-EDM mapping when EDM mapping also exists

Caveat ID Number	Description
CSCvd91379	Router crashes when NAT is moved from CGN mode to normal node.
CSCvd90446	ASR1K - NBAR causing memory allocation failures leading to Pending-Objects
CSCve62696	NBAR control-plane crash while reloading corrupted protocol-pack
CSCvf91587	CPP ucode crash in FNF fia
CSCvf02240	Crash seen with FNF feature
CSCvf28977	ESP Crash with FP Switchover
CSCvf36888	IOS-XE DMVPN Per-tunnel QoS not working on CSR1k without AX license
CSCvf84673	Traceback: ASR1001-X BUILT-IN-2T+6X1GE might go Out of Service after a reload
CSCvd30543	ASR900 Traffic drop seen in MLDP partition MDT with core interface flap
CSCvf60961	BGP scanner crashed with add/remove command bgp mpls-local-label
CSCvf56274	BGP VRF route redistribution into global routing table fails after a VRF route flap
CSCvf63541	BGP w/global import/export crashes when several nbrs deleted simultaneously
CSCvd15140	Router crashes using show BGP commands
CSCvb55711	variable 'i' is incremented both in the loop header and in the loop body
CSCvd89159	FPI leak observed when ISDN call gets forwarded to voicemail thru BACD
CSCvf98838	CME SIP Segmentation Fault crash occurs on calls to VHG with Shared Lines
CSCvd54525	SIP Can not add participants to the Ad-hoc conference if SCCP is Ad-hoc conference creator
CSCve11792	CME GUI changes for 11.6 release
CSCvf18145	Crash seen in Blind Transfer video call
CSCvd49732	User receives "Transfer to is busy" when transferring calls to an Octo-line
CSCve91511	Call queue notification delay with SIP phones
CSCvf62310	CME SIP: call-forward Unregister fails when shared-line enabled on DN
CSCve18549	CME/BE4000 Intermittently Crash when making configuration changes
CSCvf95739	Remove "dns-vrf-aware" CLI and make DNS vrf aware by default.

Caveat ID Number	Description
CSCvd47657	Router crashed in afw application
CSCvf28564	Show details soft key is not functioning in a conference call
CSCuy40939	Trust List / Toll Fraud Feature vulnerability on CME
CSCvf95746	When Overlaping IP address is conifgured on BE4K with VRF , phone doesn't register on TCP
CSCvf77411	Static when initiating conference from CME on ISR 4k
CSCvf53724	Crash when delete an interface on CSR1000v
CSCvf51814	AWS CSR redundancy fails to create bfd client if AWS redundancy conf'd prior to BFD intf coming up.
CSCvf92239	Failing to collect router info via netconf
CSCvf80757	NETCONF-YANG/RESTCONF edit config fails silently, subsequent get config reports false-positive
CSCvd80837	Crash observed in DHCP SIP
CSCvf76512	option 82 circuit-id-tag restricted by 6 bytes
CSCvf94367	SNMP poll on cDhcpv4ServerSubnetTable is not returning subnet mask
CSCve15249	IP domain lookup with source interface takes over 20 mins for a invalid query
CSCvf80807	query for NS record does not return A record in additional section
CSCuy65547	Auth-fail vlan feature does not work
CSCvf67319	EIGRP - Update from Hub to Spoke not send in DMVPN
CSCve76947	Eigrp hmac-sha-256 secret string changes when show running-config is executed
CSCvf12203	Router crashes while running EIGRP due to double free condition
CSCvf53573	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)
CSCve78802	Overlord: GLC-TE SFP module cannot up after OIR during traffic
CSCut94180	Router incorrectly displays the Serial number for an on-board module
CSCvb01800	ISR4000 - Change defaults for TDM clocking commands
CSCvd07066	ISR4451 fails to power 8851 phones after a reload

Caveat ID Number	Description
CSCvf68261	Crash when printing IPSEC anti-replay error
CSCvf33373	Packet drop with CERM_DP-4-DP_TX_BW_LIMIT seen without HSECK9 (steady traffic rate)
CSCvf79008	Voice-port shut down but PRI is still UP.
CSCvc59505	Member link of Port channel gets removed on doing a SSO on the peer end
CSCve14828	"show track" does not display Embedded Event Manager applet name on IOS-XE
CSCvc98571	EEM applet will not release the Config Session Lock if it ends when CLI is in configuration mode
CSCvc17346	ASR1K ping failed after 'medium p2p' removed from interface config
CSCvf33489	ISIS FRR : FRR ReOpt Issue, FRR state pointing to Label backup even with primary link up
CSCvf36440	Enable "mtu" config in flow exporter
CSCvf89399	Flexible NetFlow crash
CSCvd42829	Revert FNF UT fixes done in previous commit that break ASR1K polaris_dev build
CSCvf28410	Observing tracebacks after ISSU @ NETWORK_RF_API-3-ISSU_START_NEGO_SES
CSCvd81828	IKEv1 IPsec HA: ISAKMP Fails When Multiple HSRP Interfaces Configured in Same Subnet
CSCve05976	RSP3C - Memory leak @ httpc_iox_resp_data_alloc
CSCve13491	Router might crash due watchdog when creating a new swidb at if_index_allocate_index
CSCvf81966	FTP Write Process crash at process_add_wakeup
CSCve47826	Memory leak Crypto IKEv2 at ikev2_ios_psh_set_route_info
CSCva91559	3850 03.06.04.E software clean force verbose command authz fails
CSCvf87415	IP Admission doesn't work if enabled on two LAN interfaces in Active-Active Mode
CSCvd63496	ISR4k Timer corruption in auth component
CSCvf44287	Webauth not releasing allocated IDs from hash table for sockets with no data on INIT timer expiry
CSCvf12322	ART Server Bytes not exported correctly by ezPM

Caveat ID Number	Description
CSCvf76535	B2B NAT HA: Stale NAT translations stuck on primary router after communication loss with standby
CSCvf52049	FTP disconnection after failover on NAT BtoB
CSCvc46894	icmp.id becomes 0x0 in ICMP reply
CSCvd96532	ISR4k NAT selectively translating H323 payload
CSCvc39783	ISR4K:ARP entry disappeared after delelte one of static port NAT entry
CSCvc87535	NAT PAT Local High mapped to Local Low
CSCvd45710	Crash seen in IOSXE-RP Punt Service Process
CSCvf50723	Packet-tracer error message % Error: Failed to collect packet info
CSCvd23989	ASR1k B2B HA active crashes when standby is reloaded
CSCvd70318	BGP dampening commands causes crash
CSCvd11951	High CPU utilization due to Virtual Exec process
CSCvf92565	Invalid Static routes exist in VRF ip route
CSCvd58820	Need API for ip best source address for given outgoing interface
CSCvc64601	ROUTE-MAP--system deletes the first prefix-list while deleting no existing access-list
CSCvc35399	3900E not able to handle ospf peerings after the spokes cross 300 numeric count in dual hub design.
CSCux65265	Crash during the show interface CMD while a multicast tunnel goes down
CSCvf81817	Call drop with cause code 47 when call is put on hold after signaling forking
CSCvc84378	Cannot connect a TLS session on an interface that contains a VRF that also uses a redundancy group
CSCvd97803	CUBE doesn't Update the codec in UPDATE in signal forking early media renegotiation scenarios.
CSCvf92057	CUBE is unable to send PRACK to Skype server for inbound calls
CSCvd46963	CUBE isn't sending 200 OK during consulting transfer
CSCvf95352	CUBE sends 488 When Codec Changed after Mid-call Invite with Midcall-Signaling commands

Caveat ID Number	Description
CSCvf51917	dns-a-override CLI not working due to breakage since 16.4 IOS
CSCvf70475	High CPU on ASR1001 when "media stats-disconnect" command is enabled.
CSCvd17104	massive garbage output when video call is made on ASR1004
CSCvf93129	Mid-call failure because all available Crypto is not Offered in SDP
CSCvc42383	One-way recoring issue with media forking.
CSCvf97230	RE-INVITE and OPTIONS Glare not handled by CUBE
CSCvc88068	Voice Class Tenant Bind Statement Fails in VRF
CSCvf81579	ASR1K: IOSd crash in kmi_initial_check on null map dereference
CSCvf82376	Crash when removing "crypto map ipv6" and then related IPv6 ACL
CSCvb08960	ezvpn client config dissapears from dialer int when pppoe session flaps
CSCvc84053	IKEv2 CREATE_CHILD_SA REKEY_SA may fail with specific transfrom order and INVALID_KE_PAYLOAD
CSCvf96294	MIB counter for IPSec tunnels does not decrement under high tunnel scale and churn
CSCuv14856	WATCHDOG timeout crash during IPSEC phase 2
CSCvd90553	After CRL expiry, reauth-msg isn't sent
CSCvf89894	GETVPN // Primary KS sending rekey first to GM's and then to Secondary KS via scheduled rekey.
CSCvf88705	Malformed GETVPN message %GDOI-4-COOP_KS_UNAUTH
CSCvc35196	Behavior difference between XE3.17 and Polaris
CSCve16269	IKEv2 CoA does not work with ISE
CSCvf37371	IKEv2 CoA does not work with ISE- unknown attributes should be ignored.
CSCvc49350	IKEv2 CREATE_CHILD_SA REKEY_SA does not properly handle multiple DH transforms
CSCvd08600	IKEv2 Frag: "debug cry ikev2" should display payload contents for received fragments
CSCvd74953	IKEv2 IETF Frag: IPV6 Ikev2 incorrect Frag MTU used when set to default
CSCvc97368	IKEv2 IETF Frag: Tunnel negotiation fails in IKE AUTH with lower value of MTU

Caveat ID Number	Description
CSCve78226	IKEv2 responder terminates negotiation if NAT-T is disabled (even if no nat is detected)
CSCvd22385	IKEv2 when key-config key is lost, type 6 pre-shared key encrypted form is sent as pre-shared key
CSCvc45949	"clear crypto sa peer <crypto peer name>" does not work on IOS
CSCve38376	Cisco IOS IKEv1 commencing deprecation for RSA encrypted nonces
CSCvb94392	Cisco IOS and IOS XE System Software SNMP Subsystem Denial of Service Vulnerability
CSCve68213	Network monitoring tool is reporting a duplicate IPv6 HSRP virtual address.
CSCvf03898	Crash on call establishment with 'isdn autodetect' enabled on BRI NIM
CSCvb65892	ISDN process crashed unexpectedly
CSCvf67269	IS-IS support for mult-instance redistribution for IPv6.
CSCvd81370	ISIS SRTE: traceback when autoroute is configured or removed from explicit path SRTE tunnel.
CSCvb27004	OSPF SID Conflict: even after conflict detected the SID used in ospf rib
CSCvf88730	ISRG2+EHWIC-4ESG High cpu due to process "dx_mrvl_find_vidx"
CSCve60276	Crash in ADSL SNMP code
CSCvf92460	show gtp parameters causes RP to crash
CSCvc62468	Incorrect "last status change time" seen in show L2VPN VC detail
CSCvf63717	VPLS does not go up after ISSU upgrade
CSCve97383	CSR1000v crashes when "ip ldap source-interface" command is entered
CSCvb94470	AR: disabling eth map-server should clear all AR entries
CSCvb44664	LISP LIG: lig should display when it has rejected a map-reply
CSCvf71850	prefix missed in map-cache output
CSCvf71701	show ip lisp database keeps reachable although threre are no routes to EID Prefix
CSCvb84068	igmp ssm-map in VRF does not use the VRF name-server
CSCvf69272	SNMP ENGINE high CPU usage observed with 1.3.6.1.2.1.185.1.1.1(mgmdHostInterfaceEntry)

Caveat ID Number	Description
CSCvd20054	Polaris 16.4: Traceback @mpls_ldp_cfg_interface while enabling isis
CSCvc18884	ISR4321 LSMPI-4-INJECT_FEATURE_ESCAPE: Egress IP packet delivered via legacy inject path
CSCvd99555	AAA Acct sessions memory held up for LMA bindings even after cleanup
CSCvc90685	Accounting Stop not sent for PMIPv6 tunnel in LMA
CSCvd28966	MAG crash with traffic on and home interface config is removed
CSCvf40039	ISR4k: Parser remembers Cellular interface commands after changing slots
CSCvd51482	Traffic loss seen in endpoint_sso_after_path_protection_trigger Flex-LSP script RSP3, v165
CSCvd65474	ISIS/OSPF SRTE: dynamic tunnel not coming up after dest prefix SID removed and tunnel shut/no shut.
CSCvc93793	OSPF SRTE: Even after OSPF is shut, verbatim SRTE tunnels are still up .
CSCvd03170	MRCPv2 response fails with NULL string in middle of packet
CSCve47576	IPSec traffic may be classified as 'unknown' by NBAR
CSCvf14771	NBAR incorrectly classifies RTP-AUDIO as Cisco-Jabber
CSCvf38142	NBAR not classifying Citrix traffic when Citrix tags are used.
CSCve36302	NBAR Not Recognizing Netapp Snapmirror Traffic
CSCvf39811	[IOS] Evaluation of CVE-2017-7529 (NGINX) for IOS Software
CSCvd46821	Dreamliner: flowcontrol receive command on L2 ports does not take effect
CSCve42763	ISR4k with Two NIM-ES2 HSRP VIP not reply after reloading
CSCvd60596	Mandatory lookup yields a path in another cloud
CSCvd20857	3850 Stack may reload when making config changes
CSCve45461	After disabling NTP device drops all mode 6 NTP packets due to 'MODE_CONTROL ratecontrol'
CSCuz92785	Evaluation of all for NTP June 2016
CSCvc23569	Evaluation of all for NTP November 2016
CSCve65442	sys_leap variable(used for ntp status) is not updating properly when leap bit set

Caveat ID Number	Description
CSCvf83313	ASR900 drops incoming MPLS encapsulated OSPF packets (Virtual link)
CSCvc73961	OSPF BGP LS: When seg mpls is disabled on the nbr, the unnumbered links not withdrawn from LSLIB.
CSCve30867	OSPF SR TE: with multicast-intact option,handling of inter area prefixes incorrect in some scenerios
CSCve63821	OSPF SR: OSPF External Routes with non zero FWD Address - LRIB original (native) Paths/route missing
CSCvc80822	OSPF SRTE: Invalid primary paths and metric seen with SRTE autoroute announce with metric option
CSCva04919	TILFA: "node prot reqd" not working for intra routes hosted on ASBR
CSCur13623	ENH: PKI, warn if trailing spaces are present in certificate map config
CSCvf82643	Implementation for GetNextCACert in PKI Rollover on IOS needs to be changed
CSCvc71330	IOS CA Server unable to read CRL file accessed over ftp/tftp after CRL file reaches a certain size
CSCvd31250	Restored IOS CA Server Doesn't Start Without Reload
CSCve90221	Observing memory leak in command handler after CoA reauth
CSCvf19274	Observing memory leaks in AAA_MALLOC_LITE after scale test
CSCve57788	Web authentication clients do not receive redirect URL and HTTP Intercept, Invalid appl_id error smd
CSCvc88922	ppp ms-chap refuse don't work
CSCve23483	VTCP generated packet drop by punt inject infra
CSCvf24928	QFP exmem memory leak in cpp_fm_sce_result_chunk
CSCvf74499	ISR4K: RP crash seen @ bm_get_next_hqf_packet with CTS/DMVPN enabled
CSCvc79628	ISR4000 ZBF crash
CSCvb79182	IPSec GRE tunnel path-mtu-discovery does not work
CSCvf18885	Crypto-DP preventive fix for GETVPN TBAR clock drift
CSCvd32350	INFRA-3-INVALID_GPM_ACCESS error with ipv4_nat_set_appl_type_on_stby
CSCvc80792	Reboots constantly after adding Static NAT statement

Caveat ID Number	Description
CSCvg00248	ASK1k running polaris encountered a ucode crash
CSCvf05494	Traffic shaping not working with percent command
CSCvf26851	CBQOS MIB returns random value for value greater than 4.2Gbps/2Gbps
CSCvf77213	3850 CTS manual encrypted sap pmk causes stack to reload due to config parsing error
CSCvd27271	Crash during after IPSLA/IPPM frees packet store information
CSCve10619	Crash while deleting an ip sla scheduler group attached to a live probe
CSCvf02131	IP SLA can trigger crash when used with MPLS probe
CSCvf85737	rttMonEchoAdminTargetDomainName is not reflecting in SNMP as in CLI command
CSCvf66860	IOS crash in SOCK TCP Test Server process
CSCvf35507	Crash in SSH Process due to SCP memory corruption
CSCvf38253	ASR1K - %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0)
CSCvf57047	ISG ASR1k Traceback %AAA-6-BADHDL: invalid hdl AAA
CSCvb72458	Router repeatedly crashing with "%UTIL-3-TREE: Data structure error"
CSCvg00014	Chance of crash when exiting a TCL script thread
CSCvc44167	show dial-peer voice summary not showing server groups
CSCvb82446	voice-class busyout/Busyout monitor command removed after reload
CSCvf80101	CM JM procedure is not triggered on dm814x
CSCvf84340	IOS crash when logging rx dsp ctrl message out_of_sequence count syslog
CSCvf93892	If Pcm-dump caplog FFF is assigned to a h323 Dial-peer, hold/resume result in one way audio
CSCvc56866	ISR4xxx router crashed due to voice IVR script - AFW_application_process
CSCvd17146	Add plc configuration CLI for tdm voice and dspfarm
CSCvd22910	Hung Transcoder sessions in complex call flows
CSCvd79313	Invaild Session-ID header in ACK for Authentication
CSCvd98991	Path header not included in 2nd REGISTER with authorization

Caveat ID Number	Description
CSCvc81130	QSIG call redirection fails when using session server-group in dial-peer
CSCvd49153	SIPREC XML metadata is missing on the INVITE if the session target is domain name
CSCvf70383	Crash in SDP Passthru when T.38 as 1st mline in mid-call SDP
CSCvd91120	Hung sccp and rtp session when media failure reported for transcoding call
CSCvd96104	Standby processor config-sync failure and reload while adding BGP neighbor under 'scope vrf'
CSCvf90066	ASR1K RP2 crash due to CPUHOG occourred by arp input process infinite loop
CSCvf73552	VRRP non-zero authentication data on 16.3.3
CSCvc95168	ASR1001-X 1G GigE Ports do not Link up with RevB L1 PHY
CSCve71674	WCCP bypassed packets dropped by ACL on WAN interface
CSCvc75614	%SCHED-3-THRASHING after running cellular commands

Resolved Caveats—Cisco IOS XE Everest Release 16.5.2

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

Caveat ID Number	Description
CSCve31698	3650 / 3850 Login Block "Quite Mode" ACL not Working on MGMT Port
CSCve54313	Crash in ALPS SNMP code
CSCvb05362	RP crashed - UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ANCP HA
CSCvc77706	[DT]Crash oberseved while sending ANCP port up
CSCvd73062	PPPoE crash: due to invalid dlidx while Virtual Access Interface is not yet attached to Dialer.
CSCve62846	"kernel: nfs: server xx not responding, timed out" message outputed when re-inserted "ASR1000-RP2"
CSCvf09355	OBFL data not restored for ESP after router reload
CSCvf58757	Recommit CSCvf41295/CSCvf09355 - OBFL data not restored for ESP after router reload
CSCvf48876	CRIT LED behavior difference during IOS XE version

Caveat ID Number	Description
CSCvc49148	Harddisk is not accessible from IOS sometimes after router reload
CSCvc16495	Power supplies showing "ps fail" when they function fine
CSCve09906	Show plat hard slot R0 sensor producer all not works fine with 13RU(RP3).
CSCvf13960	Incorrect status in show facility-alarm status after Gi0 no shut
CSCvc48365	ASR1000-6TGE/2T+20X1GE:- Chunk corruption in XLIF pending process
CSCve57465	Recommit of CSCvd90801 - EPA-18x1GE/GLC-TE/ Ping failure at different speed settings
CSCve25878	ASR1001-X: dot3StatsDuplexStatus gives unknown for tengig and gig interfaces
CSCve53205	ASR1k 3.16 - ASR1k-ELC- XCVR disabled after router reload and interface is down
CSCve25890	CPAK-100G-SR10 V03 doesn't come up with ios images.
CSCvd62780	CPAK-100GE-EPA sends out pause frames continuously when pause frames are received
CSCvf50756	ASR1001-X crashes on smc_msg_send_fragment
CSCve09829	ISSU: 16.3.4 <-> 16.5.1 Config_Sync@lacp rate fast after Loadversion in RP2 platforms
CSCve44236	ISR4K crashes after assert failure in PA packet-buffer infrastructure
CSCvd85992	Volume based rekey, old SA deleted 30 sec after soft-expiry regardless of new SA creation
CSCve70876	Crypto device microcode hangs and crashes on ASR1k routers
CSCvb46508	IOS-XE Router Experiences Crash in "cpp_cp_svr" Process Due to "Double Free" of Buffer Used by MMA
CSCvd29248	Egress Backbone PE does not decrement TTL correctly for mpls pop operation
CSCve08344	Crash due to FNF while collecting and adding entries to cache
CSCvf05057	SPA-1XCHSTM1/OC3 : IDB Mismatch between Active & Standby RPs in ASR1k
CSCvc99951	Input errors on glc-ge-100fx
CSCvb78322	input frame and CRC counter increasing on administratively down Tengi interface
CSCvc91743	Platform does not trigger license release when the port moves into error disable state

Caveat ID Number	Description
CSCvc69594	PVC configuration missing on p2p subinterfaces
CSCvd37112	bfd dampening disappears after reload
CSCve07503	RSP crashes seen in dampening code.
CSCvc89965	After reload route policy processing not re-evaluate with route-map using match RPKI
CSCvc12039	ASR903/RSP1B&RSP3C 3sec to 10sec loss on RSP switchover when SSO enabled
CSCvc99820	BGP crashed configuring different update-source interface with v6 LL peering
CSCvc58538	BGP crashes when removing advertise-map
CSCvd90251	Duplicate BGP prefixes are not dropped
CSCve48453	eBGP vrf next-hop setting behaviour is changed by CSCuv07111.
CSCvd09584	eVPN PMSI VNI decoding / encoding as MPLS label
CSCvd16828	High CPU due to periodic route refresh to VPN peers using rtfilter AF
CSCve68911	Nested Enhanced Route Refresh requests triggers Stale Prefixes.
CSCvd02623	Prefixes were not imported to Global BGP table
CSCve94399	router crash when importing BGP routes - EVPN
CSCvf62916	Router crashes when doing "show ip bgp neighbor" on a flapping BGP neighborship
CSCvc47855	RT Filter peer sometimes unable to receive vpnv4 or vpnv6 nets
CSCve51657	Slow convergence with scale after a core link flaps
CSCvf24713	stale path message for that prefix is noticed when dampening is configured.
CSCvc75887	Support of RFC7432 EVPN route type 4 of originating router IPv4/IPv6 address
CSCvc11613	SYS-2-CHUNKSIBLINGS: when deleting vrf
CSCvd48039	UUT failed to send vpnv4/v6 routes to peer
CSCvd47126	vrf blue doesnt receive type 7 croute
CSCvd43437	Wrong Source IP Selection for eBGP in EVN/VNET environment
CSCvf06059	XE16.7.1:sh bgp <AF> u all summ shows double the route count after clear ip bgp *

Caveat ID Number	Description
CSCve57697	Crash in Bstun SNMP code
CSCva75833	Huge Memory Holding and MALLOCFAIL Tracebacks seen while Churning PTA
CSCvd63393	Policy-map name 'policy-map PIN-G3/1/3.8' causes TB and subsequent RP Crash on Policy deletion/add.
CSCut87808	Crash While Accessing CallManager XML Config
CSCve32055	ISR SIP CME crashes when "reset" command is used or after a reload
CSCvf01181	8845/8865/8821 registered to CME do not show call recents under Settings menu and VM button fails
CSCvd03961	CME Local Directory fails blank page or XML error on IOS-XE platforms
CSCve38080	CME SIP: User Busy on Shared Line due to Call Leak
CSCve32217	Crash due memory corruption in AFW
CSCvc46119	One way audio in conference when using voice-class codec in SIP CME
CSCvd09948	sip phones are not notified when sccp phone answers the call (mixed shared line)
CSCve50088	CME SIP: Crash occurs when invalid SNR extension and debugs are enabled
CSCve49376	Can't create multiple nodes for Azure HA
CSCvd58830	AWS: CSR1000v cannot be deployed in 10.0.3.0 network if using csr_mgmt container for HA
CSCve19384	climgr crashes on reload
CSCve74804	CSR AWS HA Fail
CSCve83012	CSR1000V: Core Files during extended operation - 1vCPU CSR1000V ESXI vSwitch
CSCvc94202	DP Stats Caching is not Debuggable
CSCve67856	CSR Crashed During Normal Operation
CSCvd35120	CSR Transparent VLAN broken for CSR 16.x Releases
CSCve71400	CSR1000v - GE interface output - Input queue "drops" counter miscalculation
CSCvd30843	CSR1000v crash after vNIC interface command error message
CSCvd40809	Traffic is not excluded from role-based permissions when enforcment is disabled on interface

Caveat ID Number	Description
CSCvd37502	ASR1k - Crash within IOSd due to Segfault in DHCPD Timer
CSCvd80715	ASR1k IOSD crash due to memory corruption in aaa accounting
CSCuw77959	Cisco IOS and IOS XE Software DHCP Remote Code Execution Vulnerability
CSCve61344	DHCP NAK is observed with Rebind request
CSCve82129	Different behavior seen in DHCP Init Reboot scenario
CSCvf41666	ISG: IWAG-GTP has conflicting lease-time value in DHCPOFFER versus DHCPACK
CSCve81985	Subscriber session not synced to standby while assigning static ip in DHCP
CSCvb19688	SUP7 DHCP snooping statistics incorrect drop untrusted port counter
CSCvf53750	Delay in DNS resolve after network flap
CSCvf59923	DNS : Split DNS reg-expression issue in IOS-XE (16.x)
CSCvf54983	ngDNS : "restrict authenticated" in dns view-list does not work in IOS-XE (16.x)
CSCvc96709	Crash using EIGRP and DVTI with IKEv2
CSCvf17241	EIGRP Segmentation Fault When Removing VPNV4 LFA
CSCve43573	Large EIGRP SAF updates close to max size may induce stale condition
CSCvc65604	VNET global vrf neighbor is down after an interface flap
CSCve90812	ISR4431 drops all received packets due to CRC error after power off/on
CSCve78101	Inconsistent Behavior on Link states with different SFP's plugged into the module
CSCvf03810	ISR4221 boot loop when Gig0/0/0 up
CSCve64508	ISR4451-X : CWDM-SFP-1530 SFP Rx power flutuates for built-in ports
CSCvf04211	Privilege Escalation from level 15 to binos/root using picocom
CSCve62353	Startup-config missing after power outage
CSCve78027	Polaris crash in ADSL SNMP code
CSCve15383	Random Early Detection is too aggressive on ISR4Ks and CSR
CSCvd81843	Tracebacks seen during transcoding calls with dspfarm on ISR4k

Caveat ID Number	Description
CSCve46937	Disconnect with remote when deleted VPLS configuration
CSCve33337	Policy suspension failed
CSCvd88737	ASR920 reload at fib_chain_remove (Part 4)
CSCve44819	LISP Multicast software forwarding doesn't work
CSCve39622	ISR4431/ISR4451 CPP CP/SP/HA/FMAN FP process exits (rc 255) without producing core file
CSCvd31118	Reduce impact of fingerprinting code on NVRAM access
CSCvf29760	3850 crash with "IOSXE_INFRA-4-NO_PUNT_KEEPALIVE" when mgmt port down/not connected
CSCvd14825	IOSXE - ucode crash in abort from utd_chk_proto
CSCvc61899	static route is not getting redistributed into RIP database
CSCvf55306	Static route of which next-hop intf is GRE tunnel remains even if the tunnel is down
CSCvf65643	Unicast ping stops working when "ip pim sparse-mode" removed from SVI
CSCvf45112	[AVC]context with name longer than 15 chars assignment fails
CSCvd13306	"no default-information originate" doesnt work unless "default-information originate" is added first
CSCuz63888	Crash in "show ipc all" @ ipc_print_ports_internal
CSCve68771	Crash in TCL/AFW processes
CSCvd90900	CUBE sends two wsapi notifications for audio to fax-pthru esc and desc
CSCvd30171	SIP Profile does incorrect modification - the variable name is added in signalling
CSCve71700	[Media flow around] One way audio after call resumed from hold
CSCvf72841	FlexVPN Client not starting immediately after router is reloaded
CSCve20522	"show crypto map" displays incorrect wildcard mask for crypto access-list
CSCve10917	IPSec crash on ASR1k router while processing KMI
CSCvd99474	IPsec: For sVTI after rekey old SAs are not getting deleted
CSCvf11237	Memory leak seen@crypto_init_show_instance

Caveat ID Number	Description
CSCvf16448	No all IPv6 GRE crypto tunnels may come up or recover from flapping at scale
CSCve87898	Session coming up late after RP failover due to PD delay in polaris
CSCvc78492	DMVPN : IOS-XE - Unable to pass traffic if spoke to spoke fails to build in phase 2
CSCvf34835	IOS-XE GETVPN KS crashes while sending cgmGdoiKeyServerRegistrationComplete trap after GM reg
CSCvc93605	lifetime mismatch after outage of primary key server
CSCve20850	asr1k is unable to recover from the tunnel flapping at scale for IKEv2 dmVPN/BGP
CSCvd40554	IKEv2: IOS cannot parse INV_SPI notification with SPI size 0 - sends INVALID_SYNTAX
CSCvd69373	IKEv2: Unable to initiate IKE session to a specific peer due to 'in-neg' SA Leak
CSCvd39741	IOS IKEv2 profile NVgen local auth is rejected from startup configuration upon reload
CSCve07263	IPSec Tunnel stuck in Up/Down state after shut/no-shut - VPN Interop
CSCvd10126	Call Admission Control active ISAKMP SA leak when ISAKMP SA deleted immediately after MM6
CSCvb90985	ISAKMP SA entries are not getting deleted
CSCve62464	Locally generated traffic may be dropped in a GETVPN over DMVPN setup
CSCvb14640	Cisco IOS and Cisco IOS XE Software IPv6 SNMP Message Handling Denial of Service Vulnerability
CSCve14060	IPV6 alias: Shim the local route registries of ipv6_nd alias changes
CSCve23090	16.6 OBS: Local LFA is used incorrectly when TI-LFA Node Protection enabled
CSCvd25106	2nd isis instance crashes after configuring new connected-prefix-sid-map due to no instance PDB
CSCvd72585	Binding of strict-sid does not honor maximum-paths
CSCvd59518	incorrect flag in redist rib for connected routes causes mpls ping to fail
CSCvf06972	ISIS BGP LS: When we configure same BGP LS inst id to 2 ISIS instances, it accepts without error msg
CSCuy09470	ISIS hello stops to be sent after RSP switchover
CSCvc55484	isis redist rib not getting cleared after disabling segment-routing

Caveat ID Number	Description
CSCvd03354	ISIS removing all connected ipv6 prefixes when removing 1 ipv6 scope
CSCvd21785	ISIS RIB and Global RIB out of sync resulting in complete traffic loss
CSCvc51408	ISIS route oscillation due to ldp sync and interface max metric
CSCvf42300	ISIS SR: segmentation fault in ISIS when "no seg mpls" command is given.
CSCvd12333	ISIS: FRR with unnumbered interface leads to traffic loss until TI-LFA repair path is removed
CSCve04263	ISIS: when trying to change cost, "no fibidb for backup interface - ifnum 34" msg appears on the log
CSCvc92664	prefix SID missing in Redist rib during prefix conflict
CSCvc80516	sh isis ip rib command(cli) is broken
CSCvc98524	source router address for prefix does not get updated correctly
CSCvb58643	Traceback @__be_isis_age_one_lsp_chain when we un-configure NET-ID after site bridge-domain bringup
CSCvc15923	L2TP Account accuracy: SSS disconnect ACKs are not received for few sessions
CSCvd63640	l2tp Sessions goes to dead state while disconnecting
CSCvd60080	Radius attribute Acct-Terminate-Cause - 49 difference
CSCve66328	Router acting as LAC adds an extra byte to DSL line attribute Remote-ID
CSCve20813	Corrupt event trace output in AToM with CEM AC
CSCvf05616	Traffic drop, on reconfiguring l2vpn sessions after sso on peer
CSCve20493	TU_AIS Alarm gets clear after SSO with TU_AIS condition by doing Tug Shut in PE.
CSCve38585	4K UCI Phase2: Crash @ lisp_dyn_eid_instance_route_update when changing to default vrf
CSCvd21509	Cat3k: High CPU and Memory utilization seen after deleting eid-table on fabric edge node
CSCvf68059	Dynamic-eid: 5.1.0.21 was not found in lisp dynamic-eid summary
CSCve17435	ipv6 lisp etr map-server key xxx hash-function sha2 is lost from cpe config upon reload
CSCvb35616	LISP assert after disabling "ip routing"

Caveat ID Number	Description
CSCve03563	LISP to OSPF redistribution failing
CSCvc09919	UCI-4k: Lisp Assert @ lisp_os_rib_watch_start with vrf delete and traffic loss with re-config
CSCve47374	assert stop processing leaks memory
CSCvd47567	Unexpected reboot with NAT and Multicast configured
CSCvc82325	Crash after the MPLS LDP neighbor flap in the NSR scenario
CSCve31547	ICMP Time exceed dropped due to uRPF on the MPLS PE (per-ce label) [PE-CE is eBGP]
CSCvd02153	router crash due to mpls/ospf config on interface
CSCvd16501	High CPU due to SNMP ENGINE when polling mplsTunnelHopEntry
CSCvc63145	OSPF SRTE: When mpls traffic engii is not configured on the neighbor node, the tunnel is still UP.
CSCvc95477	OSPF SRTE: When mpls traffic engineering is uncftged from i/f, tunnel not getting re-calculated.
CSCve97061	Unable to remove 'mpls tp' configuration from Router.
CSCve19361	681985688 - CPP ucode crashes at ESP20 / 16.03.02
CSCvf71734	Custom Nbar protocol is classifying traffic incorrectly.
CSCvf27072	NBAR not working on 16.5.1a
CSCvf20676	"speed" config is not display in show run
CSCve99492	DMVPN Ph-2: spoke to spoke traffic drops, NHRP entry incomplete, if crypto session fails to come up
CSCve45486	NHRP registration request non-compulsory experimental extension gets dropped
CSCve29356	16.6: Ospf neighbor failure in GigabitEthernet sub interface
CSCvc94053	165: Stale entry in BGP LS topo when ospf interface is shut with 2 ABRs
CSCvd34271	BGP LS: numbered point to point interfaces not given to LSLIB if SR or TE not enabled.
CSCvf51341	Crash after show ip ospf database summary command

Caveat ID Number	Description
CSCvc75440	MFI_LABEL_BROKER-3-INVALID_PARAM Traceback message on change of unnumbered to numbered IP address
CSCvd34128	On unshutting one of the ECMP link, packets starts puting to ROUTING THROTTLE Q due to INCOMP ADJ.
CSCvd27968	OSPF allocates extra size when sending HELLO's with cryptographic authentication enabled.
CSCve05936	OSPF FRR: repair path programming in FRR is wrong when we unconfigure L2 medium p2p from the i/f.
CSCve14426	OSPF IPFRR: cost of Ext2 external route repair path is wrong when node protection is enabled
CSCvd28737	OSPF IPFRR: default policy not applied when all configured tiebreak policies are deleted
CSCvb96911	OSPF NSSA Translator ABR does not Translate Type 7 to 5 with only VRF Superbackbone as non-NSSA area
CSCvc93519	OSPF P-adj: segmentation fault in OSPF, when we unconfigure the IP address and ospf parameters.
CSCvd28559	OSPF P-ADJ: When i/f is removed and added from the area, the p-adj sid is not getting created.
CSCvc84110	OSPF P-ADJ: When protection disabled and enabled, p-adj sid comes up with repair path.
CSCvd28411	OSPF P-ADJ: When SR is disabled and re-enabled on NBR, p-adj sids are created without repair path.
CSCve18476	OSPF PADJ: p-adj sid is not getting created when OSPF route becomes best route in RIBv4.
CSCve00964	OSPF retransmit behaviour issues
CSCvd90920	OSPF RLFA: when i/f is shut, "%OSPF-3-INTERNALERR: Internal error: Stale release node is referenced"
CSCva74756	OSPF Rogue LSA with maximum sequence number vulnerability
CSCvc99243	OSPF SID Conflict: Even after mapping server uncfed, SRMS entries shown in OSPF database.
CSCvc41975	OSPF SID Conflict: Reworking translation logic

Caveat ID Number	Description
CSCvd08433	OSPF SR ADJ: When i/f changed from unnumbered to numbered, MFI_LABEL_BROKER-3-INVALID_PARAM error
CSCvc33266	OSPF SR SID Conflict: SRMS entries are not installed in the local advertising router.
CSCvb92701	OSPF SR SID Conflict: two prefixes have the same sid and no conflict is detected.
CSCve42876	OSPF SR: ECMP routes not programmed in MPLS Forwarding table whenever there are Non-Tunnel paths
CSCvd58489	OSPF SR: Extended Prefix Opaque LSA is not added to contributing list
CSCve06489	OSPF SR: Local prefix DB entry created for translated EPL not deleted in certain scenarios
CSCvf64410	OSPF SR: Stale srgb handle used after changing the SRGB range
CSCvd22538	OSPF SR: When intra prefix is changed to inter prefix, the prefix resolution happening wrongly.
CSCvd04000	OSPF SR: When the neighbor is not SR enabled, OSPF should not install SR label path for nbr prefix.
CSCvd87404	OSPF SRTE : InterArea routes handling - No Native Paths marked by OSPF in LRIB.
CSCve01206	OSPF SRTE : OSPF External Routes handling - No Native paths marked by OSPF in LRIB.
CSCvc29492	OSPF SRTE: Not all the paths are given to SRTE after "clear ip ospf process"
CSCvc93491	OSPF SRTE: Once nsr is enabled, OSPF does not provide TE parameters to standby SRTE process.
CSCvc31353	OSPF SRTE: prefix resolution when more than 4 ECMP paths is not provided properly to SRTE.
CSCvc28022	OSPF SRTE: Send LLS loc intf ID for all link types and ELL loc rmt ID TLV for P2P numbe and unnumbe
CSCvc64977	OSPF SRTE: When i/f type changed from numbered to unnumbered, link info not given to SRTE properly.
CSCvf49340	OSPF SRTE: when SRTE tunnel is down, CSTR flag is not removed from RIB at certain scenerios.
CSCvc49095	OSPF SRTE: When the prefix is not the best route in the RIB, OSPF does not provide prefix to SRTE

Caveat ID Number	Description
CSCvc63458	OSPF SRTE: with multi area adjacency, the tunnels not coming up to the multi area instance.
CSCvd34432	OSPF SRTE; When SRTE tunnel changed to RSVP TE tunnel with forwarding adja, links not advt by OSPF.
CSCvf75000	OSPF TI LFA: when we have TILFA tunnel with more than 1 segment, label not calculated correctly.
CSCvd48206	OSPF TILFA SCALE: On reopt or clearing OSPF process, no. of protected prefixes goes down drastically
CSCvd73491	OSPF TILFA SCALE: with 2K Inter-area Prefix Scale, some non-ECMP routes are not getting protected
CSCvc85129	OSPF TILFA: inter-route withdrawn, no repair path for Ext2 computed
CSCvc81881	OSPF TILFA: Micro-loop avoidance is not enabled by default when TI-LFA is enabled
CSCvf14031	OSPF TILFA: post convergence flag and PRIMARYPATH property not set for some repair paths.
CSCvc71872	OSPF: IPFRR repair path computation stopped after receiving type 10 opaque EPL lsa.
CSCvc59255	OSPF: mapping server entries used after route replaced in RIB.
CSCvd40276	OSPF: Not able to remove ospfv3 config under Virtual-Template
CSCvd38714	OSPF: When anycast present in two areas, when one area is removed, rout not getting installed in RIB
CSCvb62808	TILFA : repair path not created for NSSA learnt external routes.
CSCvc78398	3.18.1.SP modem/s stuck in reject(pk) with PKI-3-CERTIFICATE_INVALID log message
CSCvd67254	Crash during CRL fetch failure
CSCve87458	CSR 1000v router goes offline with polaris image when WCM creates self signed cert for router
CSCvd58884	During PKI enrollment, Cisco router rejects CA/RA reply containing HTTP 500 "Internal Server Error"
CSCvd38619	EST client pki authentication request goes out to default URL always
CSCve29882	EST client pki simpleenroll request goes out to default URL always

Caveat ID Number	Description
CSCve53984	ISR 4300 crashed while importing certificate
CSCva44291	OCSP SHA2 signature algorithms verification fails
CSCvd69749	PKI Server: "Rollover RA Certificate" Becomes "Rollover ID Certificate" After Reload of Router
CSCvd67772	PKI unable to enable PKI debugs immediately after system boot
CSCve77011	SSL handshake failure when validating certification with name-constraints
CSCve74862	Crash due to memory corruption when using PNP feature
CSCvd50282	"password encryption aes" may break redundancy
CSCvd05280	DBM Crash on Active Switch while changing DCA channels
CSCvb11664	ASR1k:16.3_MR smd crash in FIPS Mode
CSCvf44896	NAT YANG model: Static NAT with VRF and route-map results in incorrect CLI order
CSCvc55197	MTU of the PPPoE Dialer interface resets to 1492 while doing any change in the MTU config
CSCvf47767	PPPoE client uses RFC4638 tag of last PADO instead of selected PADO
CSCvd82881	16.6: ASR1K: RP crash seen @cpp_bqs_rm_yoda_init_or_save_child.
CSCve52258	Both ESP crash on changing COS type on ATM VC
CSCve42512	Both ESP crash on changing shaper rate under port-channel
CSCvd70453	Changing speed and negotiation causes crash
CSCve48009	cpp_cp_svr crash seen on ASR1002-X and device keeps rebooting with 16.5.1b
CSCvd68301	Crash when interface with multiple tunnels sourced comes up
CSCve49596	fp crash while changing port-channel from vlan based mode to LACP
CSCvd40077	omit a shaped GE from platform qos optimize-rate-ratios
CSCvf01098	SUP crash @ cpp_bqs_rm_yoda_proc_pend_fc_cb
CSCve72213	Un-configuring and re-configuring QoS class-map post ISSU results in FP reload
CSCve40432	Yoda: Collapse HQF Aggregation Node

Caveat ID Number	Description
CSCve15807	Yoda: Collapse HQF Aggregation Node
CSCvf74154	SGACL: cpp_sp_svr crash during CFM EDIT request with reseq_enable = TRUE
CSCvf38445	CPP DRV: propagate CSCvc08848 to cbr-8
CSCve01564	CPP DRV: Transit Entrenched Recycle Path Does Not Enforce Packet Order
CSCve18870	CPP DRV: Transit Entrenched Recycle Path Does Not Enforce Packet Order (cBR-8)
CSCve08943	QFP sorter interrupts related to REAL_DISTANCE are fatal when they should be informational
CSCve94555	PCP-IKE-IND are rate-limited too aggressively due to unbalanced hashing
CSCvf52877	Memory leak under cpp_cp_svr process
CSCve37593	ASR1K ESP crash when creating QoS bind
CSCve04836	service policy removed from multilink interface after reload
CSCve56006	FIB has extra prefix when BGP and OSPF receive the same route
CSCvf59046	tunnel interface missing in frr-manager
CSCvf20607	ASR1K RSP crash when command 'show ip rsvp sender detail' was executed
CSCvc56422	XE316:NIM serial interface flaps after soft OIR with traffic
CSCtz29340	7600 ISSU: Traceback at sisf_issu_xmit_transform
CSCub30497	BT state not sync when interface shut/no-shut before switchover
CSCus60440	C6880 crashes when dot1x device moved across a client stack
CSCus19794	Cisco IOS and IOS XE IPv6 SEND Denial of Service Vulnerability
CSCuo04400	Cisco IOS and IOS XE IPv6 Snooping Denial of Service Vulnerability
CSCul21314	Crash seen @ sisf_internal_error with scaled ipv6 client
CSCue74708	destination-glean recovery not shown in show snoop policy command
CSCug92091	Enh: Drop message misleading
CSCue51747	Exec/Standby service handler process Traceback @sisf_internal_error
CSCuc43160	fhs-ask1k dynamic Binding Table number not include dhcp prefix entry

Caveat ID Number	Description
CSCtn50909	FHSv6: Sdby reloads for RPR due to config-sync failure and ISSU_INCOMPAT
CSCvd82104	IPv6 neighbor binding table not updated || 2960x
CSCue13287	LDRA not processing the packet received on the server facing interface
CSCua93136	LDRA: Switch crashes when sending v6 packet with "ipv6 snooping" enabled
CSCua72199	NG3K-7.65: IPv6 (internal)RAs forwarded as mcast RAs to Wireless clients
CSCue49808	PTA router crashes on configuring unclassifed mac-address
CSCun33490	SISF-3-INTERNAL: Set filter failed for 3333::/64 port Vl2 vlan 2 mac any
CSCub84903	sisfv4: SISF should accept moving more trusted entry when DOWN
CSCue18812	sisf_internal_error Traceback observerd in standby
CSCut14048	TB@sisf_mac_fsm_clean upon triggering dot1x/mab authentication
CSCua87944	Texel: fix SISF CLI (limited brd, device_role, prefix_list)
CSCub17251	Texel:DHCPv6 binding entries are not synced after switchover
CSCua87794	Texel:Inadequate IPv6 FHS behavior on private VLANs
CSCub12935	Texel:IPv6 FHS causes switch to come up in RPR mode
CSCub50593	Texel:IPv6 Snooping counter not reporting DHCP drops
CSCub21486	Texel:Policy info should be displayed in "show ipv6 nd suppress policy"
CSCvc29233	validate-xml of sh ipv6 snoop policy and counters fail with some special sub-options set
CSCvd29898	DNS probes are failing with type cname in the dns response
CSCvc31435	OID for average jitter in ASR920 Y.1731 returning zero values
CSCvf30703	Watchdog crash at sla_resp_config_command when executing the "show run" command
CSCve05026	Fatal Alignment Error Crash Due to Corrupted PC with SMEF
CSCvd90888	"snmp-server ifindex persist" is not work for virtual port
CSCvc74968	3850 "snmp-server queue-length" Value Back to Default 10 after Reload
CSCvd68050	CHUNKBADREFCOUNT crash

Caveat ID Number	Description
CSCvd12371	SSH logs showing empty username on successful authentication
CSCvc72602	3.16.4 : Prepaid feature not installed if applied on service-stop evt
CSCve66658	Crash in TN3270E-RT-MIB code
CSCve60402	Crash in Voice DNIS SNMP code
CSCvf18162	Crash observed in Mlpp-Bacd scenario
CSCvf12424	DSPRM-3-DSPALARMINFO: DSP (4/1) Host GIGE ack failed when calls invoke transcoding
CSCvd86245	fax relay t30 all-level-1 debug broken
CSCvd71879	ISR 4451-X crashed with "Segmentation fault(11), Process = DSMP"
CSCvd18792	ISR4K - Hoot and Holler E&M port cannot be co-located with multicast hub
CSCve71893	ISR4K - Hoot and Holler multicast replication issue
CSCvd80733	ISR4K: Hung Inactive SCCP session in transcoder/MTP required call flow
CSCvd03571	MGCP Gateway sends RTCP packet after T.38 switchover
CSCve21448	multiple ISR4K VGW's crashed with Segmentation fault(11), Process = DSMP
CSCvc81563	IOS-XE software crash observed mid-call when receiving Port 4000 and a=sendonly - SRTP
CSCvc91091	Code change for CLI "bootup e-lead on/off" for NIM-4E/M port
CSCvf54314	Crash due to a null pointer dereference on htsp structure
CSCve05179	removed DC from NIM-FXO card and SM-X-FXS/FXO
CSCut98625	ASSERTION FAILED : ..vtsp.c: vtsp_cdb_assert: then crash
CSCvd72693	Hairpin call to PSTN fails
CSCvd16863	2951 crash due to Null Pointer Dereference
CSCvb97638	CCSIP_SPI_CONTROL memory usage leads to crash - SIP subscribe messages
CSCvc99971	Cisco Router 2921 sending cisco-rtp payload 121 for RFC2833 (rtp-nte) instead of 101.
CSCve20335	Crash while localhost CLI disabled with Options keepalive

Caveat ID Number	Description
CSCvc80620	CUBE-161: S3: 639020025: Multiple SIP/SDP Spurious Crashes//2951//15.5(1)T3
CSCvf18470	IOS-XE CUBE HA crash
CSCve56437	ISR4351 running denali 16.3.3 crashes in AFW_application_process
CSCvc47166	One-way audio on held-resumed calls after 20 mins
CSCva22819	Processor pool leak due to CCSIP_SPI_CONTROL
CSCve64076	SIP Timer Expires gets into 0 unexpectedly
CSCve52491	DSL line info attributes Upstream and downstream not converted to bps
CSCvf11776	VRRPv3 with VRRS remains NOT READY after shutdown Port-channel IF.
CSCve29367	Packet drops seen between AppNav 694 and ASR1001X
CSCvf27566	OpenDNS local-domain bypass on ISR4k stop working after reboot

Caveats in Cisco IOS XE Everest 16.5.3

Resolved Caveats—Cisco IOS XE Everest Release 16.5.3

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

Caveat ID Number	Description
CSCvf36269	Cisco IOS and IOS XE Software Plug-and-Play PKI API Certificate Validation Vulnerability
CSCvf60862	Cisco IOS and IOS XE Software IOS daemon Cross-Site Scripting Vulnerability
CSCvg41950	Cisco IOS XE Software Diagnostic Shell Path Traversal Vulnerability
CSCvh04233	Crash after configuring ERSPAN on a ASR1001-HX
CSCvh61384	16.6: vfr related drops are not observed in CSR platfrom

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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.