# Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Everest 16.4

**First Published:** 2016-11-30

**Last Modified:** 2017-04-30

# 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.

# 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 16.4.1

No new hardware features were introduced for Cisco ASR 1000 Series in Cisco IOS XE Everest 16.4.1.

### New Software Features in Cisco IOS XE Everest 16.4.1

The following are the new software features introduced in Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Everset Release 16.4.1.

#### 18x1GE EPA Support in Modular platforms

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/routers/asr1000/install/guide/modular_linecard/asr1_mlc_hig/mlc_asr1_overview.html

#### 5 Tuple Hash Support for GEC Flow-based Load Balancing

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.html

#### 802.1X support on ISR 4K and Switch Modules

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4-8-port-ge-nim-guide.html

### Asymmetric Routing Serviceability

This feature provides support for displaying asymmetric flows on unknown, HTTP, and SSL traffic. It introduces the show ip nbar classification auto-learn top-asymmetric-sockets command. More information about this command is available at this link: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book/qos-s2.html.

### ASR1000: EPA 2x40G Support

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/routers/asr1000/install/guide/modular_linecard/asr1_mlc_hig/mlc_asr1_overview.html

### Bypass NAT functionality

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

### Cisco SSL 6.0 FOM

Cisco SSL 6.0 is used to upgrade openssl to 1.0.2 g. The security updates will be available for the next three years. From Cisco IOS XE Everest 16.4.1, RC4 and DES ciphers have been blocked and will no longer be supported as they are considered vulnerable.

### CLI for showing applications assigned to a specific traffic-class and business-relevancy

This feature provides support for matching two attribute/attribute-value combinations using the show ip nbar attribute command. More information about this command is available at this link: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book/qos-s2.html.

### DMVPN Multiple Tunnel Termination

For detailed information, see the following Cisco document:

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-mtt.html

### DNA SA Border Support

For detailed information, see the following Cisco document:

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

### ERSPAN with VLAN filtering

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.html

### FlexVPN Mixed Mode v6 over v4 transport

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-16/sec-sec-for-vpns-w-ipsec-xe-16-book/sec-ipsec-virt-tunnl.html

### L2&L3 EoGRE GW Support

For detailed information, see the following Cisco documents:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iwag/configuration/xe-16/IWAG_Config_Guide_BookMap.html

### LAN and WAN MACSec Interop

The LAN-WAN MACsec interoperability feature is supported on the following Cisco devices:

- Cisco ASR1001-X Router
- Cisco 4400 Intergrated Services Routers (With 2-port Wallander NIM)
- Cisco 4300 Intergrated Services Routers (With 2-port Wallander NIM)
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 4500-X Series Switch

The topology could be any two devices from the above list that are connected back-to-back (without any intermediate device). The working scenarios for this feature are as follows:

- MKA-MACsec with pre-shared key only for the P2P-port-based deployment model.
- MACsec Cipher Suites supported between ASR/ISR routers and C4500-X is GCM-AES-128 only.
- MACsec cipher suites supported between Cisco ASR 1000 Series Aggregation Services Routers or Cisco 4000 Series Integrated Services Routers and Cisco Catalyst 3850 Series Switches is GCM-AES-128 only. However, Cipher Suite GCM-AES-256 can also be used on some of the Cisco Catalyst 3850 Series Switches (depending on the ASIC used in the device), which do support this interoperability.

### MACSec ASR1001-HX Platform Enablement

Cisco ASR 1001-HX Router is a part of the Cisco ASR 1000 Series and offers a compact form factor that consumes less rack space and power while offering 60 Gbps forwarding throughput. Cisco ASR 1001-HX Router supports all general purpose routing and security features of Cisco ASR 1000 Series Aggregation Services Routers.

Effective with Cisco IOS XE Everest 16.4.1, MACsec is supported on Cisco ASR 1001-HX Router.

### MACSec Support 10X10GE EPA For Kahuna

Cisco ASR 1002-HX Router is a part of the Cisco ASR 1000 Series and offers a compact form factor that consumes less rack space and power while offering 100 Gbps forwarding throughput. Cisco ASR 1002-HX Router supports all general purpose routing and security features of Cisco ASR 1000 Series Aggregation Services Routers.

Effective Cisco IOS XE Everest 16.4.1, MACsec is supported on Cisco ASR 1002-HX Router in the 10-Port 10 Gigabit Ethernet Port Adapter (EPA-10X10GE).

### Nginx/HTTP - Web Security Features for 16.4

For detailed information, see the following Cisco document:

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

### QoS: DMVPN per-tunnel QoS over aggregate GEC

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xe-16/qos-mqc-xe-16-book/aggregate-etherchannel-quality-of-service.html

### QoS: Tunnel pre-classify uses internal address for fair-queue distribution

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xe-16/qos-mqc-xe-16-book/qos-apply.html

### Security (ACL) enhancements

For detailed information, see the following Cisco document:

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

### Security (ARP/NDP cache entries) enhancements

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/xe-16/arp-xe-16-book/arp-config-arp.html

### Security (punt policing) enhancements

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

### MACSec Support

For detailed information, see the following Cisco document:

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

### Site to Site IPSEC VPN for WEBUI

- Site-to-Site VPN—A Virtual Private Network (VPN) allows you to protect traffic that travels over lines that your organization may not own or control.VPNs can encrypt traffic sent over these lines and authenticate peers before any traffic is sent. Site-to-Site VPN feature allows you to create a VPN network connecting two routers.
- Cellular Interface—The Cellular Interface feature supports the Fourth Generation (4G) Long-Term Evolution (LTE) and its primary application is Cellular WAN connectivity, which functions as a primary or backup data link for critical data applications.
- Configuring Application Visibility—Enhanced to include Application Signatures identifier based on NBAR engine version 28. NBAR engine version changes if you update the protocol package.

### Support for EPA-1X100GE

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/routers/asr1000/install/guide/modular_linecard/asr1_mlc_hig/mlc_asr1_overview.html

#### TrustSec SGACL monitor mode on routers (ASr1K, ISR4K, CSR)

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/sec-cts-sgacl.html

#### Type 4 PWE VLAN rewrite

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l2_vpns/configuration/xe-16/mp-l2-vpns-xe-16-book.html

#### ZBFW - Per-filter stats enhancement

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.html

### New Hardware Features in Cisco IOS XE Everest 16.4.2

No new hardware features were introduced for Cisco ASR 1000 Series in Cisco IOS XE Everest 16.4.2.

### New Software Features in Cisco IOS XE Everest 16.4.2

No new software features were introduced for Cisco ASR 1000 Series in Cisco IOS XE Everest 16.4.2.

## Important Notes

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

### 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 16.4.1

### Open Caveats—Cisco IOS XE Everest 16.4.1

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

| Caveat ID Number | Description |
|---|---|
| CSCvc16686 | AVC/ezPM Incorrectly Reports PfRv3 Smart-Probe Statistics |
| CSCvc14951 | CSR crashes cpp_mma_policy_isd_free_exmem_entry |
| CSCvc19074 | AWS : CSR crashes with t2 instances running for long |
| CSCuz51603 | multicast crashed with invalid leaf pointer |
| CSCvb94718 | TC is being tried to be deleted unsucessfully from a PFR/VRF routine in a 3925 router |
| CSCvb66420 | PFR Sync Issues between MC and Border router ,active probes are missing on border router randomly |
| CSCvb87341 | Ping to ASR1k with a MTU of 10000 Bytes and record option set fails |
| CSCvc08339 | ISR 4331 + NIM-1MFT-T1/E1 + Frame-relay circuit does not come up |
| CSCvb62115 | cman_fp CPUHOG Traceback during FP Switchover |
| CSCvb98483 | add ipsla timstamping support to asr1001hx |
| CSCvc09950 | NBAR performance drop on Kahuna platform |
| CSCvc11012 | PFR continuously Path Changed due to UNREACHABLE Received |
| CSCvb89732 | memory leak in MPE when signature amount reaches amount using the Dynamic DB |
| CSCvc03290 | RP3/ESP100 and ISRs not scaling to known targets for NAT44 PAT |
| CSCvb98210 | ASR1001-X Polaris image PfR provisioning failed with channel-unreachable-timer for PfR MC |
| CSCvc01982 | PFRV3: Crashed at Segmentation fault(11), Process = CENT-MC-vrf106 |
| CSCvc13224 | Local Unreachable TCA not processed by master causing traffic switch on routing converge |
| CSCvc13442 | PFRV3: Transit MC crashed @be_cent_ipc_site_pfx_origin_delete |
| CSCvc06521 | Intermittent EPA-18X1GE and EPA-10x10GE repeated crash on stop/start with traffic |
| CSCvb67886 | rp2/rp3: fsck and format harddisk fails when rtr booted from harddisk |
| CSCvb71160 | ASR 1013: Imagefamily mismatching |
| CSCvb78101 | XE313: Incorrect Active flows showing up in flow monitor |
| CSCvc00703 | Polaris : ASR1k EPC PPS limit functionality not working as required. |

| Caveat ID Number | Description |
|---|---|
| CSCvb35300 | Reload boot time is longer than expected on GoldBeach P2 and Juno |
| CSCvb77131 | clear ipv6 neighbor makes stby out of sync for the ND cache entries |
| CSCvc24833 | Per interface ND limit stops working post RP switchover |
| CSCuy17600 | Getting of_irq_parse_pci() failed with rc=-22 on reloading of Argus EPA |
| CSCva49710 | ASR1k: serdes bad packet count increases in "sh plat hard slot F< 0\|1 > serdes stat" |
| CSCvb39392 | serdes bad byte counter increase in "sh plat hard slot 0\|1 serdes stat" |
| CSCvb94838 | Traceback outputs in Standby-RP. cause:show license standby |
| CSCvc26641 | Core file and ping fails while configuring sonet interface |

## Resolved Caveats—Cisco IOS XE Everest 16.4.1

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

| Caveat ID Number | Description |
|---|---|
| CSCvb95069 | FTP Passive mode: NAT door limit being exceeded |
| CSCvb62767 | NATed packets are dropped by ALG_PROCESS_TOKEN_FAIL due to NAT door limit being exceeded |
| CSCvb95663 | NIM-2GE-CU-SFP : Cannot ping GLBP Gateway IP |
| CSCvb91834 | CPP crash with enchenced+None SF combination |
| CSCvb18256 | PfRv3 Channels Not Deleted Once TC is Removed |
| CSCvb17379 | PFRv3 border will learn master prefix When the package is fragments. |
| CSCvb82048 | Dual QFP Crash triggered by removing service policy from interface with mixed shaper feature enabled |
| CSCvb77550 | PfR channels Unreachable with quick monitor and quick monitor probes to 1 in 10 secs |
| CSCvc05272 | SFF crashes when redirect interface on the same subnet as SF |
| CSCva72274 | PfRv3: BR May Crash due to Channel Creation/Modification and Next-Hop State |

# Caveats in Cisco IOS XE Everest 16.4.2

## Open Caveats—Cisco IOS XE Everest 16.4.2

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

| Caveat ID Number | Description |
|---|---|
| CSCvc21471 | kernel: fsid server error fileid changed |
| CSCvc42059 | tracelogs/punt_debug.log* missing when punt keepalive timeout / crash occurs |
| CSCvb64301 | ASR1000-6TGE: Too many "Interface TenGigabitEthernet4/0/0, link down due to local fault" logs |
| CSCve09829 | ISSU: 16.3.4 <-> 16.5.1 Config_Sync@lacp rate fast after Loadversion in RP2 platforms |
| CSCvc99951 | Input errors on glc-ge-100fx |
| CSCvd15140 | Router crashes using show BGP commands |
| CSCvd47657 | Router crashed in afw application |
| CSCvc65935 | ISR4451-X/K9 -16.3.2 crash when configure NAT66 reason:LocalSoftADR |
| CSCvc08361 | Crash in XE3.17 in TCP-TLS B2B call scenario |
| CSCvc33794 | CSR1000v HA Checkpointing Broken for Video Calls with SDP Pass-Thru |
| CSCuy91126 | POLARIS: IPSec FlexVPN PSK does not scale on asr1013/RP2/ESP100 |
| CSCvc35196 | Behavior difference between XE3.17 and Polaris |
| CSCvb94852 | IKEV2 Default Proposal Reset After Reload |
| 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 |
| CSCvb57376 | RSP3:standby router crashes due to parser return error |
| CSCvb92701 | OSPF SR SID Conflict: two prefixes have the same sid and no conflict is detected. |
| CSCvd89428 | ASR1002-HX crash on configuring mpls-lsp-monis-lsp-monitor |
| CSCvb79683 | OSPF SID Conflict: when SR disabled on OSPF inst other inst sids affecte |

# Resolved Caveats—Cisco IOS XE Everest 16.4.2

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

| Caveat ID Number | Description |
|---|---|
| CSCvc01133 | ASR 1000 router crash while updating ogacl statistics |
| CSCvb78833 | Router crashes when RF/PPPoE link goes down |
| CSCvc49148 | Harddisk is not accessible from IOS sometimes after router reload |
| CSCvc06453 | As1k @ CFM traffic frames being sent with 2 dot1q tags |
| CSCvb30256 | ASR1000-2T+20X1GE: More than 1Gbps traffic is reported on 1GE port |
| CSCvb49832 | ASR1k-ELC- XCVR disabled after router reload and interface is down |
| CSCvc06521 | EPA-18X1GE and EPA-10x10GE reloads unexpectedly with traffic and EPA OIR |
| CSCvb01450 | IP/ARP connection failed between two direct-connected interfaces |
| CSCvc23830 | Vlan Oversubscription packets are not working. |
| CSCvc14951 | CSR crashes cpp_mma_policy_isd_free_exmem_entry |
| CSCvb36753 | Ingress Unicast traffic not received on the BDI. |
| CSCvc91743 | Platform does not trigger license release when the port moves into error disable state |
| CSCvc26824 | AN: ACP is not getting created after save & reload in some specific scenario |
| CSCvb62685 | AN: Channel/Nbr flap during bootstrap in ASR903 with standby RSP. |
| CSCuz85280 | AN: Standby reload due to config-sync failure at CISCO_AN_IPSEC_PROFILE |
| CSCvc42729 | Autonomic Networking Infrastructure Adjacency Discovery DoS Vulnerability |
| CSCvc42717 | Autonomic Networking Infrastructure Registrar Device Reload |
| CSCvc89965 | After reload route policy processing not re-evaluate with route-map using match RPKI |
| CSCvd09584 | eVPN PMSI VNI decoding / encoding as MPLS label |
| CSCvb85945 | Router crash @ IP RIB Update while deleting bgp config |
| CSCvb75286 | RP crash @ BGP router with "import l2vpn evpn re-originate" |
| CSCvb53469 | Ephone-DN remains in down state when restart all is given in telephony-service |

| Caveat ID Number | Description |
|---|---|
| CSCvc63958 | SIP CME relays out "Authorization: header" received from IP Phone. |
| CSCvb51806 | Router crash when removing EIGRP |
| CSCvd04210 | IKEV2 Tunnels are flapping, rekey request received from PD, lifetime kilobytes configured |
| CSCvc55378 | ASR1k crashed while unconfiguring Netflow |
| CSCvc32062 | Evaluation of IOS XE BinOS component for Openssl September 2016 |
| CSCvc26134 | self-generated packets sent fail over PMIP-MUDP tunnel in LMA |
| CSCva05558 | IKEv2 IPv6 GRE IPSec fails to stabilize on asr1k on 16.3 |
| CSCvd40880 | Modifying crypto ACL leads to a removal of crypto map config |
| CSCvc59750 | IKEv2 Aggregate-auth Timing Issue |
| CSCvc99738 | IKEv2 tunnel fails to come up b/w Cisco routers post upgrading one router to 15.5(3)S5, 15.5(3)M5 |
| CSCvd69373 | IKEv2: Unable to initiate IKE session to a specific peer due to 'in-neg' SA Leak |
| CSCvd47757 | csr1000v is not able to poll CISCO-IPSEC-FLOW-MONITOR-MIB |
| CSCvc51408 | ISIS route oscillation due to ldp sync and interface max metric |
| CSCvb58857 | LDP NSR : Remote Side VCs stays up even with local access interface shut after SSO |
| CSCvb49730 | VFI is down after provisioning a new new VFI to the existing |
| CSCvc35325 | MK51-UCI, Mcast trafic is blackholing on ISSU CV while upgrading from FC5 to FC6 |
| CSCvc17525 | complete traffic drop with DATA MDTs with latest polaris_dev |
| CSCvc90685 | Accounting Stop not sent for PMIPv6 tunnel in LMA |
| CSCvc54049 | Ignore home address is broken in MAG/LMA |
| CSCvd28966 | MAG crash with traffic on and home interface config is removed |
| CSCvc03651 | SSH / Telnet / Console freezes while bringing up PMIPv6 tunnel interface |
| CSCvc21452 | ASR903:ISIS routes are set with Max Metric due to IGP LDP Sync |
| CSCva44687 | ASR 1K Running IOS-XE 3.16S w/ MPLS Crashes on 'clear ip route *' |

| Caveat ID Number | Description |
|---|---|
| CSCvb88373 | MRCP V2 logging tag support |
| CSCvc99925 | ASR 1k NHS Fallback fails for NHRP on secondary path |
| CSCva70115 | ISR4331 crash due to NHRP running 03.16.03.S |
| CSCva97469 | VA stuck in protocol down state after failing to establish IPSec session |
| CSCvc19234 | Old Constrained Node Sid not getting deleted from MPLS forwarding table on changing SID |
| CSCvb34173 | OSPF SR SID Conflict: SID is not installed for route via virtual-link |
| CSCvc12420 | OSPF SRTE: CSTR path is not installed in some cases properly. |
| CSCvc19844 | SID conflict: Even after an area is removed from topology, SID database does not remove the area. |
| CSCvc54359 | SRTE: Single hope tunnel doesn't install any repair path. |
| CSCvc23238 | SRTE: when i/f address is removed, traceback is seen and adj-sids not destroyed. |
| CSCvc54211 | Tunnel & repair path continuously flapping on disabling SR on next node from head-end. |
| CSCvb96706 | Client auth and enroll to subca fails |
| CSCvc33707 | crash after multiple renew |
| CSCvd58884 | During PKI enrollment, Cisco router rejects CA/RA reply containing HTTP 500 "Internal Server Error" |
| CSCvb73018 | PKI: Cannot import RSA SubCA signed by ECDSA |
| CSCvd82881 | 16.6: ASR1K: RP crash seen @cpp_bqs_rm_yoda_init_or_save_child. |
| CSCvc55747 | ASR1K ESP100 - Both ESP crashing due to cpp_bqs_srt_yoda_place_child_internal: failed to grow tree |
| CSCvc71183 | ASR1K ESP100 - Both ESP crashing due to cpp_bqs_srt_yoda_place_child_internal: failed to grow tree |
| CSCvc48813 | BQS unable to resume processing leading to pending objects constantly increasing |
| 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 |
| CSCvd68301 | Crash when interface with multiple tunnels sourced comes up |

| Caveat ID Number | Description |
|---|---|
| CSCvb82048 | Dual QFP Crash triggered by removing service policy from interface with mixed shaper feature enabled |
| 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 |
| CSCvb87341 | Ping to ASR1k with a MTU of 10000 Bytes and record option set fails |
| CSCva31708 | SR:RSP2:Object download failure(EOS object)error seen randomly |
| CSCvb44207 | CTS/SGT across GRE p2p tunnel broken when doing inline tagging |
| CSCvc26599 | ASR crashes when attempting SRTP/TLS call |
| CSCvb48683 | Evaluation of all for Openssl September 2016 |

# 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.