Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Gibraltar 16.10.x

First Published: 2018-12-03

About Cisco ASR 1000 Series Aggregation Services Routers

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

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

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

ROMmon Release Requirements

For more information on ROMmon support for Route Processors (RPs), Embedded Services Processors (ESPs), Modular Interface Processors (MIPs), and Shared Port Adapter Interface Processors (SIPs) on Cisco ASR 1000 Series Aggregation Services Routers, see https://www.cisco.com/c/en/us/td/docs/routers/asr1000/rommon/asr1000-rommon-upg-guide.html.

New Features and Important Notes

New and Changed Information

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

New Software Features in Cisco IOS XE Gibraltar 16.10.1a

The following are the new software features introduced in Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Gibraltar 16.10.1a

- RIB/CEF Routing: Improvements to Show Tech Routing command. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/command/isg-cr-book/isg_m1.html#wp3145726977.
- BNG: Add disconnect summary and history of subscribers in show tech subscriber. For detailed information, see the following Cisco document: :https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/command/isg-cr-book/isg_m1.html#wp3145726977
- SpaceX: MPLS over DMVPN. For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16-10/sec-conn-dmvpn-xe-16-10-book/sec-conn-dmvpn-xe-16-10-book_chapter_010000.html
- L3 routed dual-stake IPoE sessions support. For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/configuration/xe-16-10/isg-xe-16-10-book/isg-acess-ip-sess.html
- Smart Licensing. For further information, see the following Cisco document:. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/smart-licensing/qsg/b_Smart_Licensing_QuickStart.html

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.
- Segment Routing OSPFv2 Remote uLoop support. For further information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16-10/segrt-xe-16-10-book/ospfv2-microloop-avidance.html
- Hashing algorithms enhancements for LAG. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/xe-16-10/isw-cef-xe-16-10-book/isw-cef-ecmp-loadbalance-with-tunnel-visibility.html
- OSPF: Statistics per OSPF Neighbor. For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/command/ipv6-cr-book/ipv6-s5.html.
- NAT CLI simplification: simplify on-the-box data collection without having the user knowing architecture. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book.html.
- ASR1K : show interfaces transceiver (CSCvh67402). For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book.html
- Optimized APM for Assurance monitoring. For further information, see:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/media_monitoring/configuration/xe-16-10/mm-xe-16-10-book.html.
- PfRv3 Fallback timer. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16-10/pfrv3-xe-16-10-book/pfrv3.html
- Direct Cloud Access Phase 2. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16-10/pfrv3-xe-16-10-book/pfrv3.html
- Boot: Boot statement check before reload.

  When upgrading their IOS software image, customers might sometimes delete their old image without updating the boot statement. This could result in the router entering the ROMMON (ROM Monitor)

mode. To recover from the ROMMON mode, the following enhancements are supported for different use cases:

1. Reload the router with default config-reg configuration -- Before reloading, the router checks if the first boot statement points to an image that exists and verifies it. If the image is missing or invalid, you are prompted for confirmation to proceed with reload of the router.
2. Reload the router with config-register 0x2102 - auto boot – The router checks if the boot variable is set properly, and accordingly prompts you to proceed with caution.
3. Reload the router with config-register 0x2102 - auto boot and the boot variable (bootvar) is set, but there is no image in bootvar set path – The router checks if the bootvar is properly set and if there is any image set in the bootvar path. If there is no image in the bootvar path (hard disk/bootflash/flash, and so on), then the reload is aborted with a warning message, and you are prompted to correct the boot statement or copy the image to hard disk.
4. Auto boot and boot variable is set – If the image is present in the bootvar path, then the router reload is allowed.

- Add support for NAT46—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16-10/nat-xe-16-10-book/iadnat-46.html.
- BGP: Display the time at which route was installed in bgp table—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/command/irg-cr-book/bgp-s1.html.
- BGP: add a peak watermark output along with a timestamp of when the peak occurred on a per neighbor basis to the show ip bgp neighbor command—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/command/irg-cr-book/bgp-s1.html.
- BGP: Improve the Show tech BGP command. For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/command/irg-cr-book/bgp-s1.html.
- VXLAN GPE P2MP Tunnels Support. For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xe-16-10/ce-xe-16-10-book/vxlan-gpe-p2mp-tunnel.html.
- DHCP-Radius-Proxy support with ISG. For detailed information, see the following Cisco document:: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/configuration/xe-16-10/isg-xe-16-10-book/isg-dhcp-radius-proxy.html.
- LISP: Enhance debug LISP filter. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/command/ip-lisp-cr-book/lisp-debug-cmds.html
- BGP: Show ip bgp neighbors command additions. For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios/iproute_bgp/command/reference/irg_book/irg_bgp5.html
- CUBE Media Proxy. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-media-proxy.html

- Exclusive Elliptical Curve Ciphers on CUBE. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-sip-tls.html
- APPNAV-XE APP-ID classification filter. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/routers/access/4400/appnav/isr/isr_appnav.html
- Umbrella on ASR1K platforms. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_umbrbran/configuration/xe-16-10/sec-data-umbrella-branch-xe-16-10-book.html
- UTD (IPS and Url-filtering) migration to IOX Containers on ISR4k, CSR, ISRv. For detailed information, see the following Cisco document: : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16-10/sec-data-utd-xe-16-10-book.html
- Multicast: Extend debug command. For detailed information, see the following Cisco document:: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/debug/command/i1/db-i1-cr-book.html
- BNG: Raise a syslog message when queued packet are reaching in vpdn control-plane. For detailed information, see the following Cisco document: : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/vpdn/configuration/xe-16-10/vpd-xe-16-10-book/vpd-cfg-additional-feat.html
- Programmability—gRPC Dial-in and Dial-out. Expands existing Model Driven Telemetry capabilities with the addition of gRPC protocol support and Dial-Out (configured) telemetry subscriptions (Network Essentials and Network Advantage).

  For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1610/b_1610_programmability_cg/model_driven_telemetry.html.
- Programmability—YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16101. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same GitHub location highlights changes that have been made in the release..

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

Service Policy

Attaching a policy in the same direction on both the main interface and subinterface is not allowed.

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 and FAQ.

Before You Begin

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

Procedure

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

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

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

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

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 and 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 Gibraltar Release 16.10.x

Resolved Caveats—Cisco IOS XE Gibraltar 16.10.2

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

Caveat ID Number	Description
CSCvm76464	ASR1k crash due to QoS in case of 4k subscribers per subinterface
CSCvn00277	ASR 1006-X RP2: Standby RP Crashed after configuring **license boot level adventerprise** command.
CSCvn02171	HOLE is not created when **acl default passthrough** command is configured.
CSCvn30138	Crash with show service-insertion service-context command in AppNav Cluster
CSCvn38590	CTS policies download fails with Missing/Incomplete ACEs error
CSCvn72973	Device is getting crashed on the **cts role-based enforcement**
CSCvo00968	Radius attr 32 NAS-IDENTIFIIER not sending the FQDN.

Caveat ID Number	Description
CSCvo03458	PKI "revocation check crl none" does not fallback if CRL not reachable
CSCvo24170	Crash due to chunk corruption in ISIS code
CSCvo25785	Crash on an LNS router in process ACCT Periodic Proc
CSCvo27553	PKI incorrect fingerprint calulation during CA authentication
CSCvo38985	Crash at the VRF configuration

Open Caveats—Cisco IOS XE Gibraltar 16.10.1a

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

Caveat ID Number	Description
CSCvm25851	qfp-bqs-internal ucode still crashes with fix in CSCvc35307
CSCvm39485	Small clock changes or time drifts can cause GETVPN TBAR drops (GDOI/IPSEC-PI)
CSCvm46362	ASR1k node in HA pair might crash due to punt-keepalive failures
CSCvm51112	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys
CSCvm55018	A control plane 'delete' command to flush the queue is not being drained out of the command queue
CSCvm57021	Crash in CENT-MC-0 process after Doubly-linked list corruption
CSCvm76452	IPSec background crash while sending SNMP trap
CSCvm78937	ASR1K crash when running 'show ip nhrp brief"
CSCvm91323	Router crash with reload reason: LocalSoftADR and core file generated 'cpp-mcplo-ucode'
CSCvm93589	Performance Monitor not working when "collect transport round-trip-time" is configured
CSCvm93794	FlexVPN MPLS - label in CEF not added when shortcut to hub is created (by glitch)
CSCvm99745	Can't configure multiple CFM IP SLA with the same source MEP on ISR1k,ISR4k,ASR1k
CSCvm99778	IOS-PKI: grant auto trustpoint <tp_name> does not work with IOS Sub CA
CSCvn01894	ASR1k IF down/up happen when config "plim ethernet vlan filter disable" with copper SFP
CSCvn09472	cpp_cp_svr memory leak in module: IPHC Svr Info_st
CSCvn12253	Software crash due to watchdog after entered switchport command.
CSCvn14454	iWAN router PDP crash

Caveat ID Number	Description
CSCvn15214	Device registered to CSSM loosing the registration on upgrade from 16.06.04 CCO SL-mode to 16.10.01
CSCvn17037	Anyconnect Profile Download: ASR1001-X crashes when it receives an incoming SSL VPN connection
CSCvn17655	Removing ip flow monitor from an interface caused ESP crash
CSCvn19382	Crash after comparing tunnel FIB entries
CSCvn20629	Hseck9 license not displayed as consumed on CSSM portal after DLC conversion
CSCvm78104	AVC feature not shown in use when configured in CSL mode
CSCvn10596	Device is not registering to the CSSM portal move from 16.6.4s SL to the 16.10.1a SL only image.
CSCvn17114	ASR1K: Unable to retrieve the information error on standby RP with ISSU downgrade.
CSCvn21716	SW Redundancy and Firewall coming in DLC Path in SL Only mode
CSCvn06412	IPSEC License not consumed on ASR1001-X
CSCvn01251	1610_SL_Only: Router hangs when downgrading from 16.10 to 16.6.4 CCO image (SL Registered)

Resolved Caveats—Cisco IOS XE Gibraltar 16.10.1a

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

Caveat ID Number	Description
CSCuv90519	IKEv2 session fails to come up after tunnel source address change
CSCvb03610	Watchdog crash after "% AAA/AUTHEN/CONT: Bad state in aaa_cont_login()."
CSCve14080	Error message "LID: Handle 0x0 is invalid" filling console logs
CSCvg32796	External Interface on the PfR MC stuck in the shutdown state
CSCvg54267	Cisco IOS and IOS XE Software Cisco Discovery Protocol Denial of Service Vulnerability
CSCvg56110	Error and pending objects when mma policy flap with egress monitor for multi-VRF case
CSCvh49364	PFRv3 Incorrect time-stamp in traffic-class router change history
CSCvh49380	PFRv3 Incorrect reported value of TCA threshold in traffic-class router change history
CSCvh57657	NAT MIB not populated when using traditional NAT
CSCvh59431	Byte counters for physical interface and subinterface don't match

Caveat ID Number	Description
CSCvh77310	Wrong initial number of DPD incrementing error counter.
CSCvh97101	NAT-HA on Cisco 2900s breaks if it is asymmetric routing.
CSCvi32156	Router crashes when DMVPN tunnel moves accoss ports
CSCvi50061	Evaluate NTP February 2018 Vulnerabilities.
CSCvi58996	Several OID from CISCO-CLASS-BASED-QOS-MIB stop working when performing upgrade to Denali-16.3.x
CSCvi63840	vif interface counters do not increment with multicast service reflection on IOS-XE
CSCvi79674	CPP 0 failure Stuck Thread resulting in Unexpected Reboot
CSCvi90729	IKEv2 CoA does not work with ISE (coa-push=TRUE instead of true)
CSCvi93967	EEM: event mat mac-address not triggered on router with NIM-ES2-8-P
CSCvi93972	IWAN versions with prefix tracking only allow prefix splitting for internet and not enterprise
CSCvi94425	TBAR issues on KS after running "clear crypto gdoi ks coop role"
CSCvi96874	ASR1001 has crashed with cgm_avlmgr_find_node
CSCvi97054	When configured vlan unlimited with port-channel subinterface, statistics does not increment
CSCvj01098	Evaluation of IOS-XE and IOS for OpenSSL CVE-2018-0739 and CVE-2018-0733
CSCvj02081	CPP crash on L2TP router
CSCvj03263	H225 gatekeeper request dropping under "ALG PARSER" with ZBF
CSCvj06391	Recommit of CSCvg77924 - FRR feature not working in ESP100 & ESP200
CSCvj06493	NAT ALG ASR1K does not translate call id 0 of PPTP client correctlly.
CSCvj06909	Reverse-route configuration is unsupported under gdoi crypto map
CSCvj08248	Packet throughput drops down when enable tunnel visibility with single tcp flow(>1MPPS)
CSCvj11876	Provide Passthrough Reason in IOS-XE for AppNav
CSCvj12370	cpp_cp_svr crash in bqs while running QMRT test tool.
CSCvj13382	IOS-XE FIPS mode is enabled by default in QFP even if it is not enabled in CLI
CSCvj15262	ASR1k with stateful nat conf, mapping ID got locked after vrf delete
CSCvj16489	Enabling IPSec Anti-Replay with SNS in an IPSec profile enables it globally.

Caveat ID Number	Description
CSCvj17682	MAC filtering incorrectly set on builtin ports of ISR4300
CSCvj23301	IOS: Crypto Ruleset fails to get deleted
CSCvj25678	Crash after failing to modify xcode
CSCvj29593	debug platform condition start causes keepalive failures with Vasi interface
CSCvj31705	ASR1k unexpected crash when appNav holds a stale pointer.
CSCvj37835	EPA-1X100GE/CPAK-100G-SR4 stays in a down/down state after a reset.
CSCvj41550	default channel operation state changing from I/O to D/O failed when zero-sla enabled
CSCvj47957	Packet trace does not work with re-injected UTD packets
CSCvj51510	Crash after service-policy APPNAV change on WAAS instance
CSCvj53634	The OID - adslAtucCurrOutputPwr returns incorrect output.
CSCvj57502	Memory leak@CENT-BR-0 when change the path label frequently
CSCvj61603	"dtmf-interworking rtp-nte" command breaking software MTP.
CSCvj63450	router crashed with '%SYS-2-NOPROCESS: No such process 158 -Process= "SC CMM Recv Process"'
CSCvj67042	LAN Switches does not learn the right ED upon OTV failover
CSCvj67623	DNS ALG will not work when trying to match specific destination hosts
CSCvj70568	FlexVPN || DHCP entries not flushing for ikev2 timed out reconnect sessions
CSCvj71853	"sdavc_ppdk.pack force" command not accepted during boot up
CSCvj72273	GETVPN Key Servers after split may generate TEK with same SPI but different key material
CSCvj76662	GetVPN TBAR failure does not generate syslogs
CSCvj78083	Path of Last Resort Sending Probes in Standby State
CSCvj78551	ASR1001X @incorrect traffic statistics reported of port-channel sub interface using SNMP.
CSCvj80490	ASR1001-X: Investigate "license request failed , err=0x22" seen at Manufacturing test
CSCvj84104	PLR channel is not muted for some time
CSCvj84155	Policy configuration changed under AppNav Cluster failed to push down
CSCvj84158	PfRv3: BR May Crash due to Channel Creation/Modification and Next-Hop State (Copied from CSCva72274)

Caveat ID Number	Description
CSCvj86316	Different ISP name smartprobes are received in branch WAN interface, the channel cannot detect
CSCvj88138	VASI NAT: FTP ALG translation is sometimes failed
CSCvj88805	ASR1K - No kernel/coredump generated with watchdog reload event
CSCvj90426	Dash i2c Kernel message outputted during boot up
CSCvj90814	Crash due to Memory corruption in ISR4k
CSCvj91448	PKI:-IP address parsing issue while printing the subject name if classless IP is used in Trustpoint
CSCvj94133	ASR1001-X : netconf interface goes into oper down state afer reboot tests
CSCvj94863	Channel with wrong label may be created on hub border
CSCvj95361	Crashed due to process = IPSec background proc
CSCvj97483	ASR 1009/1013 (ESP200) will drop traffic when a rate limiting packets at 67.104gbps
CSCvj99489	standby router shows warning message as image is missing when image in present in active and standby
CSCvj99599	Traceback Generated While Placing Bulk Conference Call on SM-X-PVDM-3000
CSCvk00895	double exception in ipv4_nat_icmp_lookup_embedded
CSCvk02072	Hoot-n-holler multicast traffic marked with DSCP 0
CSCvk04614	ASR1K not reachable by Unicast on Port-Channel Sub interfaces when EVC + Sub-interface is configured
CSCvk12152	Unable to remove command 'ip nat inside destination'
CSCvk12448	ESP crash due to fatal error
CSCvk15062	Modification to ZBFW access-lists do not reflect in TCAM
CSCvk17777	ASR1001X - when using VRF NAT port used for ftp data is not freed
CSCvk26109	ISAKMP using UDP500 rather peer(translated) port from peer structure while initiating IKE SA for DPD
CSCvk26471	NG: Ping fails after cahanging Copper SFP to Fiber SFP on 1GE built-in interface.
CSCvk27007	MGCP status remains Down after IOS upgrade caused by CSCvh70570
CSCvk29692	DSP detected FXO "supervisory disconnect dualtone mid-call" is treated as CNG tone
CSCvk30939	Memory corruption at PKI Session End
CSCvk34152	Invalid throughput level in the "show version" output

Caveat ID Number	Description
CSCvk47929	IOS XE 16.08.01 - monitor capture missing packets (TCP ACKed unseen sgmts)
CSCvk51560	Fixed ISR: Increase Maximum Configurable VLAN# and STP# from 32 to 63
CSCvk53938	IOS-XE : IPv6 ACL for Tunnel QoS not matched
CSCvk56331	Initial contact in IKEv1 phase 2 rekey (QM1) causes all crypto sessions to drop
CSCvk58746	Unexpected reboot when ipv6 crypto map applied to several tunnel interfaces
CSCvk62278	DSCP value for MGCP signaling traffic cannot be configured
CSCvk62742	On demand PCM captures Fail on some IOS-XE versions
CSCvk63602	WAAS Policy Configuration push may caused AppNav Class-maps programming issue in TCAM
CSCvk63706	Active RP3 hard oir can cause module to go UNKNOWN
CSCvk65072	Crash due ZBF + NAT
CSCvk66712	[UniScale] CSR1v may crash in hal_process_ipc when performing "clear ip nat tr *" with max NAT pools
CSCvk67137	Crash observed on ASR1002-X @ fnf_age_recalculate_record_len with AVC performance monitor config
CSCvk70428	Router crashed when enrollment type changed from http to pem in between certificate request process
CSCvm03696	ISDN PRI calls getting dropped with cause 47 because of bad interaction between CDAPI and TSP layers
CSCvm03744	"%FMFP-3-OBJ_DWNLD_TO_DP_FAILED:fman_fp_image:xxx" appears when configured "ip port-map" on ISR44xx.
CSCvm06270	ICMP unrechables are not sent to the client on C1117 platform
CSCvm16619	CPP-mcplo-ucode crash while encrypting SIP packets with ALG NAT for SIP
CSCvm19399	CRL file is getting overwritten when PKI server turns up after reload
CSCvm20374	Polaris Router - CPUHog - SNMP ENGINE crashed with Watchdog timeout
CSCvm36190	Traceback seen when attempting to recover sw port from bpduguard err-disable state
CSCvm44488	ASR1001-HX 10GE SFP+ ports may operate as 1000Mbps
CSCvm49190	Hairpin call to PSTN fails with primary-net5 switch-type on ISR4k.
CSCvm56670	ACL dropping packets after updating it - %CPPEXMEM-3-NOMEM
CSCvm57644	Small clock changes or time drifts can cause GETVPN TBAR drops (Crypto-DP)

Caveat ID Number	Description
CSCvm57817	ASR1002-X crash due to ccp_cp_svr going into lockdown state.
CSCvm59483	Host crashes the DSP if ipv6 commands are configured under Service-Engine [Purge ipv6 config option]
CSCvm66103	Crash due to communication failure - IPC (Inter-Procedure Call) messages between DSP and RP.
CSCvm96663	An IOS-XE router crashes after umbrella is configured.

Related Documentation

Platform-Specific Documentation

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

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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