Bugs for Cisco IOS Release 15.4(3)S

Open and Resolved Bugs

Bugs describe unexpected behavior in Cisco IOS software releases. Severity 1 bugs are the most serious bugs; severity 2 bugs are less serious. Severity 3 bugs are moderate bugs, and only select severity 3 bugs are included in this section.

In this section, the following information is provided for each bug:

- Symptoms—A description of what is observed when the bug occurs.
- Conditions—The conditions under which the bug has been known to occur.
- Workaround—Solutions, if available, to counteract the bug.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select bugs of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This section consists of the following subsections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Using the Bug Search Tool

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

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.

Note 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.

To use the Cisco Bug Search Tool:

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:
   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. You can mouse over bugs to see more content about a specific bug.
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.

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.

Resolved Bugs—Cisco IOS Release 15.4(3)S9

Table 1 Resolved Bugs—Cisco IOS Release 15.4(3)S9

Caveat ID Number	Description
CSCsv05154	Cisco IOS HTTP server vulnerable to CSRF attacks
CSCui67191	Cisco IOS XE Software Ethernet Virtual Private Network Border Gateway Protocol DOS Vulnerability
CSCun88463	Router reload due to memory corruption with IP SLA
CSCuo87952	Line card FPD upgrade struck, and card FPD status in 'wait' state.
CSCus34406	dmvpn tunnel goes down when removing secondary ip from tunnel source int
CSCus73337	stack stby reloaded by stack-mgr due to active/stdby config out of sync
CSCut45453	icmpv6 reply are blocked
CSCuv80858	byte counters for a port-channel show interface is inaccurate
CSCuw73525	3650 DHCPv6 Guard does not block rogue DHCP server to provide IPv6 addr
CSCux24141	MET mis-programming results in unwanted multicast after switchover
CSCuy14110	CPU Spike seen due to VTEMPLATE BKG OW Process.
CSCuy38144	Protocol Other counted up when executing "show int accounting"
CSCva18762	IGMP packets looping between Active & Standby SP CPU
CSCvb14640	Cisco IOS and Cisco IOS XE Software IPv6 SNMP Message Handling Denial of Service Vulnerability
CSCvc54886	Asr1k(SPA-1XCHSTM1/OC3): Router down after receiving invalid spa ipc-message
CSCvd01613	DSCP value get remarked on the ES+ 10g line cards
CSCvd02153	Router crash due to mpls/ospf config on interface.
CSCvd19860	OSPFv3 AUTH breaks IPv6 traffic intermittently

Caveat ID Number	Description
CSCvd42785	Multicast forwarding when OIF is Null in 7600
CSCve48453	eBGP vrf next-hop setting behaviour is changed by CSCuv07111.
CSCvf12081	Cisco IOS XE Software Verbose Debug Logging Information Disclosure Vulnerability
CSCvf29111	7600 stack low crash
CSCvf74829	CRL download fails due to "failed to create getcacert message"
CSCvf81579	ASR1K: IOSd crash in kmi_initial_check on null map dereference
CSCvg00110	MET table depletion in 7600
CSCvg06443	VPNMAP table depletion in 7600
CSCvg09008	Online Diagnostics detected a Major Error
CSCvg53836	router crashed when MPA with source vlan 1-4094 created
CSCvg84667	Mishandling of udp pkts (that are destined to RP) at 7600 ES+ NP, when BFD is hardware offloaded
CSCvh02536	XE3.16.6B-ES: pmsi_tunnel label value seen as explicit null on downstream PE
CSCvh21686	ES+HD (76-ES+XT-8TG3CXL) LC ports sharing a channel stop forwarding when a port is admin shutdown

Resolved Bugs—Cisco IOS Release 15.4(3)S8

Table 2 Resolved Bugs—Cisco IOS Release 15.4(3)S8

Caveat ID Number	Description
CSCvb61075	ASR920: Dual-rate EEM errors out when hostname has a dot '.' character
CSCvc89965	After reload route policy processing not re-evaluate with route-map using match RPKI
CSCvc58538	BGP crashes when removing advertise-map
CSCuw35828	crash w/BGP show advertised-routes when route-server is on vrf
CSCvd90251	Duplicate BGP prefixes are not dropped
CSCvd09584	eVPN PMSI VNI decoding / encoding as MPLS label
CSCvd16828	High CPU due to periodic route refresh to VPN peers using rtfilter AF
CSCva86436	no export ipv4 unicast map triggered router to crash
CSCva24325	NSF/SSO feature not honouring TCP MSS
CSCvc31517	Router crashes using BGP commands for long cost extended community string
CSCve51657	Slow convergence with scale after a core link flaps
CSCvd43437	Wrong Source IP Selection for eBGP in EVN/VNET environment
CSCve57697	Crash in Bstun SNMP code
CSCvb30567	C7600 ES+ stuck TOD counters for Y.1731 measurements

Caveat ID Number	Description
CSCva34374	ipv6 traffic over bridge-domain carrying on few ports only
CSCve66601	Crash in CISCO-SLB-EXT-MIB code
CSCut87808	Crash While Accessing CallManager XML Config
CSCuz87695	SCCP Phones on CME not forwarding video packets on outbound calls
CSCux18010	Cisco Networking Services Sensitive Information Disclosure Vulnerability
CSCuw77959	1801M - %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCva00899	C841M crashes randomly during execution of the reload EEM script.
CSCvb59372	Double-free of VTY context causes a software-forced crash
CSCux15954	EEM : fatal condition error from operating system
CSCvc98571	EEM applet will not release the Config Session Lock if it ends when CLI is in configuration mode
CSCva42638	Traceback is seen when a EEM script runs
CSCvc44866	3850/3650 - ssh/vty sessions lock up leading to loss of access to device
CSCut77951	Arp entry changes to an encap type of 802.1Q
CSCvc77378	Glare condition exists for mid call DO INVITE when CUBE receives in-dialogue SIP OPTIONS message
CSCva80218	IOS-XE router crashed due to possible memory leak issue due to CCSIP_SPI_CTRL
CSCvb08960	ezvpn client config dissapears from dialer int when pppoe session flaps
CSCve10917	IPSec crash on ASR1k router while processing KMI
CSCvd40880	Modifying crypto ACL leads to a removal of crypto map config
CSCvb94392	Cisco IOS and IOS XE System Software SNMP Subsystem Denial of Service Vulnerability
CSCuz15131	dqueue not empty prior to destruction crashes ipv4fib_les_switch_wrapper
CSCvd97524	Fixed versions for CSCuz15131 crash when traffic with maximum size is on wire
CSCvb25357	NHRP registration requests failed after ipv6 tunnel source change
CSCvb65892	ISDN process crashed unexpectedly
CSCve60376	Crash in ADSL DMT SNMP code
CSCvc15923	L2TP Account accuracy: SSS disconnect ACKs are not received for few sessions
CSCvb41889	NTP leap second inserted every day after leap second occurs
CSCuw97889	Incorrect CLI output after netconf edit-config
CSCuz95908	Memory leak due to path querry with Null outgoing interface
CSCva38391	CVE-2016-1550: NTP security against buffer comparison timing attacks
CSCuz94245	IGP-LDP sync interoperability for OSPF multi area adj
CSCuv69650	OSPF Virtual-link using the lowest cost path
CSCut21950	3560 / RBAC / Unable to exclude enable command.
CSCuv04247	3850 config-sync failure on standby w/ 'no shut' on wlan
CSCuw53025	Cat3850 reports "Error, ECI has run out of event blocks" message

Caveat ID Number	Description
CSCus23013	show cmd under "parser view include-exclude" cause standby router to reload
CSCuz22162	Digital certificates does not sync to standby
CSCva66819	Non-Vlan1 did not get initiated with pnp startup-vlan conf after reload
CSCuw60955	non-vlan1 doesn't seem to initiate in Beni-MR3
CSCux52544	PnP Fails to Initiate with Non-VLAN1 Feature Configured
CSCuw15272	PNP: non-vlan 1 zero-touch upgrade does not work
CSCut25533	PnPA: non-vlan CLI should only apply to newly bootup devices
CSCvc80135	Crash when removing and re-adding bandwidth remaining percent while class-default has fair-queue
CSCvd23034	Multiple Parent Events Per Node lead to a crash
CSCvc56422	XE316:NIM serial interface flaps after soft OIR with traffic
CSCuy08656	SNMP Traps leading a leak in CHUNK functions
CSCve60402	Crash in Voice DNIS SNMP code
CSCve21448	multiple ISR4K VGW's crashed with Segmentation fault(11), Process = DSMP
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.
CSCvc86595	HTTP 304 response causes mc error and bad magic

Open Bugs—Cisco IOS Release 15.4(3)S8

Table 3 Open Bugs—Cisco IOS Release 15.4(3)S8

Caveat ID Number	Description
CSCux26195	"aaa accounting suppress null-username" not working as expected
CSCvd69608	Asr1k crashes at PPP process on pushing 4 or more per-user static ipv6 routes
CSCve54313	Crash in ALPS SNMP code
CSCuw97842	Standby RP crash at be_ancp_get_dsl_line_attrs
CSCva00765	crash after no ipv4 multicast multitopology command
CSCvf10260	7600 - ACL not programmed upon configuration changes - all incoming packets processed by CPU
CSCts36318	7600: Native Vlan not removed from trunk port
CSCvd86374	ES20 module crash after FRR object is freed then accessed
CSCvc68496	Discrepancy in number of ACEs in active and Standby after CoA
CSCun31438	Abnormal Call Disconnection due under load due to DP errors
CSCux41072	EIGRP sending hello messages with interface in passive mode.

Caveat ID Number	Description
CSCvb86484	wrong EIGRP redistribution statement in startup config breaks BGP settings atfer router reload
CSCuv74256	IOS: HMAC key miscalculated with DH Group 21 and IPSec PFS enabled
CSCve13491	Router might crash due watchdog when creating a new swidb at if_index_allocate_index
CSCva55916	CUBE crash in resolve_sig_ip_address_to_bind NULL ccb
CSCuv08835	IPSEC key engine process leaks /w dynamic crypto map in scaled scenario
CSCuv14856	WATCHDOG timeout crash during IPSEC phase 2
CSCuv51788	GM Router failed to register after reload.
CSCup84620	"show crypto isakmp stats" should print dropped IKE messages
CSCup90021	IKEv1 periodic DPDs sent per IPsec SA, not per IKE
CSCvc21452	ASR903:ISIS routes are set with Max Metric due to IGP LDP Sync
CSCvc82325	Crash after the MPLS LDP neighbor flap in the NSR scenario
CSCvf21718	ASR1K crash when running 'show ip nhrp vrf ... detail'
CSCvc65670	NTP leap second addition/deletion for consecutive leap months not working properly
CSCuz62898	Crash in BGP due to regular expressions
CSCvf24928	QFP exmem memory leak in cpp_fm_sce_result_chunk
CSCuv02537	ASR1K ESP200 reload in a B2B CGN NAT scenario with PAP+BPA
CSCux93752	SRST Double Ringback heard on blind transfer to PSTN
CSCuv74171	crash on command "show snmp view"
CSCve46273	%TRANSCEIVER-3-RPC_FAILED: Application error (rc = 3)
CSCux86075	Unexpected crash during SSH operation
CSCvb72458	Router repeatedly crashing with "%UTIL-3-TREE: Data structure error"
CSCuu71299	MPLS LDP flap with %TCP-6-BADAUTH: No MD5 digest
CSCve66658	Crash in TN3270E-RT-MIB code
CSCva08142	IOSd crash on LISP enable router
CSCva00551	Cisco Router may crash on SIP MA Process Due to sstrncpy()
CSCuz72665	DATACORRUPTION-1-DATAINCONSISTENCY error when copying from PAI header

Resolved Bugs—Cisco IOS Release 15.4(3)S7

Table 4 Resolved Bugs—Cisco IOS Release 15.4(3)S7

Caveat ID Number	Description
CSCva47253	AAA crash on multiple username deletions - Part 2
CSCvb64818	ASR1k/ISG : 3.13.6 : Crash due to bad id in id_to_ptr when sending Accounting to non-existing group
CSCvc42499	Function radius_message_authenticator_decode
CSCuy76789	16.2 Throttle: UDP Packets are getting dropped with nat64+ZBFW configs
CSCuw66787	Clear ip nat translation vrf X impacts vrf Y
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
CSCuz93698	PPTP Traffic issue with Carrier Grade NAT on IOS-XE
CSCva86436	no export ipv4 unicast map triggered router to crash
CSCva24325	NSF/SSO feature not honouring TCP MSS
CSCva25965	Router may crash after multiple show ip bgp sum/neighbor
CSCuv69297	Catalyst 3850: SSH/VTY session hangs on show run or other show commands
CSCvc33619	Major error status seen on card WS-X6748-GE-TX
CSCva61877	IPv6 neighbor discovery packet processing behavior
CSCvb69386	Controller SPA-1CHSTM1 OC3V2 goes into wedge state after excess controller flaps
CSCva94139	IPv6 neighbor discovery packet processing behavior with SIP-400
CSCva91655	FIB recursive loop crash
CSCuz81292	IPv6 neighbor discovery packet processing behavior
CSCuh23818	HTTPS Secure server script crashed iosd and reloads with traceback
CSCuv97379	[ST-P] STBY router crashed on disconnecting call on ACTIVE
CSCuy30957	For IPv6:Activate Under GDOI Fail-Close Disappears on Reboot
CSCva62029	Crash observed on GM when rekey message received from Key server
CSCvb94852	IKEV2 Default Proposal Reset After Reload
CSCva61415	Unable to initiate IKE sessions due to mismatch in CAC counters
CSCvb29204	BenignCertain on IOS and IOS-XE
CSCva44179	IKEv1 DPD delete logic causes stale phase 2
CSCuz42299	Crash when configuring CWS
CSCut45177	CWS HTTPs traffic fails to load on ISR configured with NVI
CSCva18067	CPU HOG and Crash by MFIB_rate
CSCuz28618	sup2t: sup crashed after MFIB errors
CSCva43443	DNA/SA,Upon Quad SUP SSO,Mcast decap traffic black holing for ~50 sec
CSCva59927	UCI,On QuadS6T Second SSO,PIM joins are not encapsulating over VRF LISP
CSCva99279	RSP3:Labels not getting assigned in spite of having free label space
CSCva97469	VA stuck in protocol down state after failing to establish IPSec session

Caveat ID Number	Description
CSCux99025	Evaluation of Cisco IOS and IOS-XEl for NTP January 2016
CSCux46898	NTP associations vulnerability
CSCvb19326	NTP leap second failure to insert after leap second occurs
CSCvb00272	OSPFv3 IPSEC socket session is not coming up after reboot
CSCvb66420	PFR Sync Issues between MC and Border router ,active probes are missing on border router randomly
CSCvb96706	Client auth and enroll to subca fails
CSCuy13701	IOS PKI: Crash while editing a VRF aware TP with enrollment profile
CSCuv44053	PKI Rollover: rollover cert is being added as active id cert
CSCvb73018	PKI: Cannot import RSA SubCA signed by ECDSA
CSCva15013	AAA/RADIUS memory leak on IOS-XE
CSCuz87179	Crash observed while bringing up PTA sessions in SSS Manager
CSCva67564	No V-Cookie in accounting stop due to idle timeout or manual clearing
CSCuz57124	Tracebacks *MSG 00001 TRUNCATED* on standby, after PTA Sess brought up
CSCvb24139	H225 Sanity Check Failure
CSCuz82533	Router crashed when the virtual access interface comes up
CSCuo75126	Ucode crash seen with Firewall configs in B2BHA setup
CSCva65990	'sh police int' hidden command causes RP to crash
CSCuz76821	tableid_ha: Memleak @ eobc_pool_getbuffer
CSCva37519	stale flowmgr entry during ipv6 tacacs transaction leads to crash
CSCuy38157	Router crash during handling L2 and L3 subscribers at the same time
CSCuv41355	Unable to telnet -- No wild listener: port 23
CSCuh09324	udp entries not deleted from flowmgr table
CSCuz03079	ISR-4K Processing Error: H323 Setup parameter "mediaWaitForConnect TRUE"
CSCva22751	Router crashing due to a watchdog in the ISDN process
CSCvb24266	ISR 4K Crashes When Running "Debug Voice Translation"
CSCva00015	STBY SBC router crashing multiple times
CSCvc19209	SIP session between VXML GW and the Nuance server remains active after callback (CCB) is scheduled
CSCvb90483	VXML GW hardening changes for ICBC memory corruption issue

Open Bugs—Cisco IOS Release 15.4(3)S7

Table 5 Open Bugs—Cisco IOS Release 15.4(3)S7

Caveat ID Number	Description
CSCux26195	"aaa accounting suppress null-username" not working as expected
CSCuu36200	Radius auth fails if ip radius source-interface vrf default in startup
CSCvb05362	RP crashed - UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ANCP HA
CSCuz21435	IOS-XE: 'ACE event' process watchdog crash.
CSCus85112	CGN, QFP: Show cmd display incorrect NAT trans stats for per-host IP add
CSCup57389	Traffic drops while testing VRF Lite coexistance with SP NAT for LNS
CSCuw97842	Standby RP crash at be_ancp_get_dsl_line_attrs
CSCul15273	AN Link local Tunels not deleted after no autonomic is issued
CSCuo97277	iosd crashed at bfd_chkpt_create_and_send_msg
CSCvc12039	ASR903/RSP1B&RSP3C 3sec to 10sec loss on RSP switchover when SSO enabled
CSCut40990	BGP:send-community inheritance when explicit configuration match default
CSCva00765	crash after no ipv4 multicast multitopology command
CSCus04010	dmvpn hub router crashes when clearing bgp peers
CSCus19601	IPV6 RR not changing Next-hop for a IPV6 prefix
CSCuq27095	Memory leak in BGP table if terminate at show bgp af summary auto more
CSCup33405	Prefixes from GR peer not removed from BGP table when peer goes down
CSCvb22903	RP3 fails to clear SA in the large scale IPSec SCM configuration
CSCup01258	sh ipv6 dhcp pool command display wrong output after router reload
CSCva13768	ISR 4K|PPPoE Interface|Not Forwarding all IP fragments
CSCun31438	Abnormal Call Disconnection due under load due to DP errors
CSCux41072	EIGRP sending hello messages with interface in passive mode.
CSCvb86484	wrong EIGRP redistribution statement in startup config breaks BGP settings atfer router reload
CSCur72967	43xx/44xx "show platform software cerm-information" not accounting pkts
CSCuv74256	IOS: HMAC key miscalculated with DH Group 21 and IPSec PFS enabled
CSCtw50974	ASR/ISR4K DTMF 2833 to 2833 Not Working with MTP CoLocated and OOB+2833
CSCut79286	ASR1K QoS feature doesn't work fine with RP2/Rls3.x
CSCup26658	Unexpected Process Restart after "no spanning tree", "default interface"
CSCuw43115	CSR1Kv XE 3.13.3S Crashed on clearing ip ospf process
CSCva55916	CUBE crash in resolve_sig_ip_address_to_bind NULL ccb
CSCuq17104	CUBE disconnecting a call after call transfer due to Hold timer
CSCuu12283	CUBE failed to create DP session on STBY for Webex flow
CSCuw39465	During a transfer CUBE doesnt update the media to the Recording server
CSCuq24354	GETVPN KS rekeys without pol changes may cause IOS XE GMs to re-register
CSCuv08835	IPSEC key engine process leaks /w dynamic crypto map in scaled scenario

Caveat ID Number	Description
CSCux16726	ipv6 OSPFv3 crypto session doesnt come UP after reload
CSCuj53943	Multicast packets are dropped after "clear crypto gdoi ks members"
CSCvc78492	Unable to pass traffic if spoke to spoke fails to build in phase 2
CSCuv51788	GM Router failed to register after reload.
CSCuu41857	Incorrect GDOI registration backoff timer calculation after crash/reload
CSCup84620	"show crypto isakmp stats" should print dropped IKE messages
CSCup90021	IKEv1 periodic DPDs sent per IPsec SA, not per IKE
CSCun72450	IPv6 GETVPN traffic dropped after un-configure then re-configure VRF
CSCvb65892	ISDN process crashed unexpectedly
CSCul24766	Core files are corrupt - crc error
CSCuy03680	V3Lite IGMP packets sent instead of V3 when UDP based feature is present
CSCur10311	MAG does not accept PBA without GRE key during de-registration
CSCvc21452	ASR903:ISIS routes are set with Max Metric due to IGP LDP Sync
CSCuv00547	CRASH SEEN AFTER FLAPPING MPLS INTERFACES
CSCuq95663	CENT: small increase in IPC still exists in longevity
CSCuz22260	ISR G2: unexpected byte lost with PfRV3 and NBAR based QoS integration
CSCvb92697	High CPU due to NHRP when NHRP cache entry for remote spoke's tunnel address is deleted
CSCux80450	%REGISTRY-3-STUB_CHK_OVERWRITE: error seen during boot up
CSCvc65670	NTP leap second inserted every day after leap second occurs
CSCvb48912	SNMP crashes getting ntpAssociationEntry with low/fragmented memory condition
CSCuz62898	Crash in BGP due to regular expressions
CSCuv69650	OSPF Virtual-link using the lowest cost path
CSCum19502	Inconsistent behavior between telnet and ssh in low memory conditions
CSCus23013	show cmd under "parser view include-exclude" cause standby router to reload
CSCva72564	Customer POC- Autoinstall obtained IP overrides USB bootstrap config
CSCuw24373	Called-station-id and NAS-ID via account profile satus query
CSCun96847	IOS-XE : Zone mismatch vulnerability in Zone Based Firewall
CSCux52451	VRF Domain half open counter increments when aggressive aging occurs
CSCuv02537	ASR1K ESP200 reload in a B2B CGN NAT scenario with PAP+BPA
CSCvb77570	ASR1K: Crash after upgrade to 3.16.3 at transmit_pkt_marmot_spa_d
CSCuw95297	ESP200 crash with 550K translations with cablevision config
CSCux68096	ucode crash abort called from ipv4_nat_create_inside_addrport_bind
CSCva95830	HQF not cleaned after invalid policy applied to vlan-manual GEC subintf
CSCtx83808	PPP: Traceback when changing police to shaper on LNS
CSCum03909	mvpnv6 mldp router crash on _be_ipv6_pdb_remove_ipdb_private
CSCux93752	SRST Double Ringback heard on blind transfer to PSTN

Caveat ID Number	Description
CSCup04090	asr920 throws error messages on snmp polling of a couple of MIBs
CSCuv74171	crash on command "show snmp view"
CSCux86075	Unexpected crash during SSH operation
CSCvb72458	Router repeatedly crashing with "%UTIL-3-TREE: Data structure error"
CSCuy74990	BGP not forming neighborship on ASR1k with dual RP
CSCuu71299	MPLS LDP flap with %TCP-6-BADAUTH: No MD5 digest
CSCva08142	IOSd crash on LISP enable router
CSCvc81332	ASR Cube crashed @ AFW_M_Connection_EventPreProcess
CSCvb97638	CCSIP_SPI_CONTROL memory usage leads to crash
CSCva00551	Cisco Router may crash on SIP MA Process Due to sstrncpy()
CSCuz72665	DATACORRUPTION-1-DATAINCONSISTENCY error when copying from PAI header
CSCux16650	SHA-2 support on ISR G2

Resolved Bugs—Cisco IOS Release 15.4(3)S6a

This is a special release in Cisco IOS software that addresses Cisco Product Security Incident Response Team (PSIRT) caveats.

Table 6 Resolved Bugs—Cisco IOS Release 15.4(3)S6a

Caveat ID Number	Description
CSCvb29204	BenignCertain on IOS and IOS-XE
CSCuv87976	CLI Knob for handling Leap second Add/delee ignore/ handle
CSCux46898	NTP associations vulnerability
CSCvb19326	NTP leap second addition is not working during leap second event

Open Bugs—Cisco IOS Release 15.4(3)S6

Table 7 Open Bugs—Cisco IOS Release 15.4(3)S6

Caveat ID Number	Description
CSCva15013	AAA/RADIUS memory leak on IOS-XE
CSCva00765	crash after no ipv4 multicast multitopology command
CSCva82501	FNF crash during multiple config

Caveat ID Number	Description
CSCva55916	CUBE crash in resolve_sig_ip_address_to_bind NULL ccb
CSCuu12283	CUBE failed to create DP session on STBY for Webex flow
CSCva71545	Under load crash seen@CCSIP_UDP_SOCKET process in XE3.16 image
CSCva62029	Crash observed on GM when rekey message received from Key server
CSCuy03680	V3Lite IGMP packets sent instead of V3 when UDP based feature is present
CSCuy13701	IOS PKI: Crash while editing a VRF aware TP with enrollment profile
CSCuo75126	Ucode crash seen with Firewall configs in B2BHA setup
CSCuy74990	BGP not forming neighborship on ASR1k with dual RP
CSCva08142	IOSd crash on LISP enable router
CSCva00551	ISR 4K Crash on SIP MA Process Due to sstrncpy()
CSCva00015	STBY SBC router crashing multiple times

Resolved Bugs—Cisco IOS Release 15.4(3)S6

Table 8 Resolved Bugs—Cisco IOS Release 15.4(3)S6

Caveat ID Number	Description
CSCuz48415	"aaa authentication suppress null-username" not working as expected
CSCuw86386	AAA crash when removing TACACS servers
CSCuy21675	Crash@username_command with service pwd-encryption & common-criteria cfg
CSCux69225	Mac filtering option "None" sends blank password
CSCuy01051	MPLS VPN over mGRE Routing issue after reload
CSCuz82218	TACACS Enable authentication fails with null pre shared key
CSCuy03054	ASR1K IOSd may crash in BGP Accepter process due to segmentation fault
CSCux55351	ASR1K router crashed due to running BGP with AIGP
CSCux70093	BGP RR does not advertise vpnv6 prefixes even all RT filters are learnt
CSCuy20481	Crash due to stale pointer after removing vrf command export AF map
CSCux76332	Deleting a statement in export map, removes other statement
CSCux96029	GR Non-restarting peer does not advertise VPN routes default RT filter
CSCuy03504	Incorrect prefix count upon clearing bgp peering
CSCuz58682	Incorrect VPN withdraw with overlapping RT on multiple RT Filter
CSCuz21061	router crashes after %BGP-6-BIGCHUNK + SNMP query.
CSCux62094	Routes are not exported from vrf to global due to incorrect export limit

Caveat ID Number	Description
CSCuw66752	"SSM connection manager" high CPU if VAIs under scale have QOS applied
CSCuy79944	call-home crash because calling XOS API in interrupt level
CSCuw06084	DTMF not getting recognized on ISR G3 when using TCL Script
CSCux60876	Memory corruption due to DHCP
CSCux49494	'allow connections' or 'telephony-service' config is required on ISR4k
CSCuz56699	ISR 4k Paging over SIP / FXS phones have no audio
CSCuy38707	After RSP switchover, BFD hangs for up to 10 minutes before converging
CSCuw48118	ASR920 - crash in bcopy called from 'addnew' during reassembly
CSCux29974	ISR4k:UnconfiguredIpv4Fia drop seen for pkts transit via PPPoE
CSCuz12967	Crash after show ip protocols vrf with RIP enabled
CSCuy48358	Crash during SIP subscribe notify ACK
CSCuz47777	DTMF issue on ISR G3/ASR during the prompt using TCL Script
CSCuy40672	One way audio in a DODO call after transfer with REFER disabled
CSCuz71250	Router crashes when parsing ack for mid call
CSCuz69975	Under load crash is seen in CVP REFER_PASSTHRU scenario
CSCuw23947	For IPv4: Activate Under GDOI Fail-Close Disappears on Reboot
CSCuy43118	XE316: HubBR might be crashed@tunnel_protection_validate_shared_profile
CSCuu44128	GETVPN on ASR with vasi interface fail to install the Rekey
CSCuz14788	New reg invoke PKI function breaks the GETVPN CRL Checking feature
CSCuv31981	ISR Router Crashes When Trying to Delete a Freed SA
CSCuz99865	IPSec MIB queries results in memory leak and shows wrong SNMP value.
CSCuz25240	ISIS not installing back to RIB neighbors loopback when interface flaps
CSCux29806	ISIS routes are not not installed in the routing table from isisdatabase
CSCuz35203	SSM connection manager crash during VFI pseudowire bind
CSCuq32410	"Seg fault @ mLDP Process"&Crash@nile_mc_handle_prefix_L3_and_not_L2
CSCuy02409	BDI not Passing VRRP Multicast Traffic
CSCuz39721	ASR1K/RP2/SW 15.4(3)S4 crash
CSCux78294	Crash on router when removing L2VPN
CSCus72718	L2TPv3 session pending between 2 devices
CSCux58640	LDP NSR: Label Mapping Messages Not Sent on RP SSO and VCs Re-bind
CSCuw65792	CWS not associating CN with nested groups when "," (comma) is used
CSCuw65059	mfib on the line card stuck in Connecting state
CSCuv02246	With access interface flap, traffic doesnt switch back to data mdt.
CSCuv37022	Extranet MVPN traffic is getting dropped & not switched to data MDT
CSCuy87734	ASR1K RP crashes LCON Main process when heavily loaded
CSCva17339	LDP session stuck in established with no TCP connection
CSCuy71712	FlexVPN: Spoke spawns a virtual access to connect to the hub

Caveat ID Number	Description
CSCuy04757	Crash@ospfv3_router_process_mgd_timers on shut/no shut of sub-intf
CSCuy32709	R-LFA Tunnels not established on setting DS required attribute
CSCux19034	XE3.16 crashes when conf "distribute-list" under router ospf and sh run
CSCuo61229	ASR1002 Crashed after "show pfr master active running"
CSCux20613	Bus error crash at oer_saa_mc_get_probe_stats_cbk
CSCuw57225	PFRv2 not work well for 10% inbound load-balance
CSCuy22067	PfRv2 stream keep remaining in DEFAULT state
CSCuy85870	Wrong TD next-hop for overlapping prefixes
CSCur10056	Memory leak in SSS Manager
CSCuw79412	%SYS-6-STACKLOW: Stack for process PPP SIP running low, 0/6000
CSCuo76385	Router crashes at ic_dp_classify when Serial link flaps
CSCuz99848	Memory exhaustion traceback due to large and complex configuration
CSCva28875	NAT ALG fails on Multipart SIP Header
CSCuw50415	Crash seen @ hwidb_iftype_unlist while doing unconifg of channel-group
CSCuw55717	Memleak @ pak_pool_cache_item_get : Scaled TFEX
CSCuy55849	RTR installs the ISIS(or OSPF) route with Higher Metric in the RIB
CSCuz76295	MPLS-TE FRR packet drops during re optimization.
CSCuy38709	Memory leak with watcher_create_common.
CSCux82377	ASR 1K ISG Router Crashes When Polling "csubSessionEntry" MIB
CSCuy69440	ISG Critical Exception and crashing with SSS-Manager holding memory
CSCuz62915	ISR4451 crash under load due to Segmentation fault(11), Process = DSMP
CSCuy65330	RSVP Reservation Failure Causes Call Drop on Voice to Video Calls
CSCus45019	Media loop detection failure
CSCuj50209	Memory leak @ voip_rtp_recv_fs_input
CSCuy14532	rtp/rtcp media activity timer doesn't trigger when only 1 rtp leg drops
CSCux54794	Configuration under the E&M voice-ports are missing after the reload
CSCuy16501	Static noise introduced on FXO after IOS upgrade
CSCva30483	IOS-XE 4321 Router crash with BRI interface going down
CSCuz52693	ISR 4K Memory Holding in CCSIP_SPI_CONTROL
CSCus03761	Stack overflow crash @ ip_epm_proxy_slow_check.
CSCuy83854	deb voip application vxml with 1 cvp call caused buffer overflow
CSCuz17364	DTMF Type ahead buffer on GW with Nuance not working
CSCuu25704	Memory corruption in the IO pool when a t38 fax gateway receives t37 fax

Open Bugs—Cisco IOS Release 15.4(3)S5

Table 9 Open Bugs—Cisco IOS Release 15.4(3)S5

Identifier	Description
CSCux44606	Name ACL for Multicast Boundary Stops Working Upon Reload
CSCux33568	ESP crash while reconfiguring FR interface to MFR bundle
CSCux07224	ASR1K crash with OTV due to L2BD FIB entry change
CSCux59115	ASR1002-X Crash with dpidb_tableid_params_initialize
CSCux93176	ASR1k:stby RP stuck while bootup
CSCur48133	ATM 3xOC3 SPA failed to program with IFCFG_CMD_TIMEOUT error

Resolved Bugs—Cisco IOS Release 15.4(3)S5

Table 10 Resolved Bugs—Cisco IOS Release 15.4(3)S5

Identifier	Description
CSCuw89522	ASR IOSD crash because of AVC feature
CSCuw13407	PfRV3: transport bytes expected counters overflow and not expected
CSCuv79776	Router with Pfr feature crashed at cpp_free_exmem
CSCuw30599	ISR4331-B: traceback occured when enabling Ethernet Data Plane Loopback
CSCuv84600	Netflow packets are dropped when EPC is enabled
CSCux29703	ASR1000-2T+20X1GE fails to boot on router reload with SPA-3-NULL_BAY_PTR
CSCuu48458	ASR1k/15.4(3)S QinQ frames are dropped under "TCAM Failure Drops"
CSCux55692	TCAM Errors in NL11k TCAM of Fixed Ethernet Linecards
CSCuw98135	ZBFW HA not replicating sessions when matching based upon L4 proto/port
CSCuw21897	Traceback seen with ip cef accounting
CSCux57066	ASR1K : Lawful Intercept not working as expected for IPv6 traffic
CSCux02656	ASR1K: Crash related to collecting NetFlow data for IPv6 flows
CSCuw36887	Crash with with Flexible Netflow enabled
CSCuw78755	IOS-XE need not require appxk9 license to support per-tunnel DMVPN QoS
CSCup91567	ASR1001-X boot-loops with CMCC crash and XGM MAC10 block errors
CSCux01133	interface counter stuck on build-in interfaces in ASR1001X
CSCux43951	Packet drops on built-in 1Gig ports of ASR1001-X
CSCuv26762	ASR1001X HMAN generating error msg when reading /proc/cpuinfo
CSCux42411	ASR1001-X Frame Relay with Fortitude NIM fails due to LMI packet padding
CSCuv93130	Cisco IOS-XE 3S platforms Series Root Shell License Bypass Vulnerability
CSCup70353	IOS-XE router reload due to WebUI log file leak
CSCuw49798	ASR1K: cpp_cp_svr core@cpp_qm_cmn_delete_queue

Identifier	Description
CSCuw94014	cpp_cp crashes with BB profile #6 48k PTA
CSCut49714	GEC:QoS: pkt buff util high after apply/remove flat policy w/ fair-queue
CSCuw81487	Kahuna RP crash when bringing up PTA sessions with QoS
CSCuw73223	Polaris : cpp_cp_svr crash when the interface goes down
CSCux10321	ASR1000 CLI hangs on executing the "show platform hardware qfp xxx"
CSCud50181	SBC srtp ucode crash doing srtp-rtp interworking
CSCuu45832	STUN packets not handled properly by CPP SBC module in ASR CUBE
CSCuw71226	Call stuck in a deactivating state (CUBE-SP)
CSCut78545	delegate registration failed after password change

Open Bugs—Cisco IOS Release 15.4(3)S4

Table 11 Open Bugs—Cisco IOS Release 15.4(3)S4

Identifier	Description
CSCuv07111	IOS and IOS-XE devices changing the next-hop on BGP route with own IP
CSCup33405	Prefixes are not removed from BGP table with BDI interface shut
CSCut79286	ASR1K QoS feature doesn't work fine with RP2/Rls3.x
CSCuw09483	Unexpected reload w/"privilege exec level '0-15' show macdb" configured
CSCuu12283	CUBE failed to create DP session on STBY for Webex flow
CSCuu26224	CUBE with SRTP fallback will crash when call hit on incoming dial-peer 0
CSCuv61208	ASR1k EasyVPN server looses RRI for clients behind PAT
CSCuw02157	DMVPN Hub: IOS crash at crypto_ipsec_show_map_info
CSCuq24354	GETVPN KS rekeys without pol changes may cause IOS XE GMs to re-register
CSCuw09323	GETVPN: ASR GM stops decrypting until old SA expires after KS ACL change
CSCuw08567	Ident SM exists without Dynamic Crypto Map leading to rekey failures
CSCuj55363	lispgetVpn traffic is dropped when getvpn profile is applied in wan intf
CSCuj53943	Multicast packets are dropped after "clear crypto gdoi ks members"
CSCus85701	AQoS peer mismatch with NAT
CSCuv66070	Crash on executing "show nhrp group-map" command
CSCuv86821	Router crashed due to Crypto IKMP
CSCuv21051	XE310:Traceback@crypto_isakmp_profile_free after unconfiguration
CSCuv94186	SNMPWALK crash at ipsmIPSec_policyOfTunnel
CSCuv79429	IPSEC: static reverse-route is removed after retransmissions in IKMP
CSCun72450	IPv6 GETVPN traffic dropped after un-configure then re-configure VRF
CSCuv59898	Kernel Watchdog crash at ktime_get
CSCus62778	Stale Data MDT entry

Identifier	Description
CSCuq95663	CENT: small increase in IPC still exists in longevity
CSCuv74171	crash on command "show snmp view"
CSCup31575	HTTPS : Back to Back POST request fails
CSCus06158	ISR4x/ISR3x: Mask IOS-XE SSLVPN syntax from configuration
CSCuw14345	High CPU due to "IP Connected Rou" process and Low Memory .

Resolved Bugs—Cisco IOS Release 15.4(3)S4

Table 12 Resolved Bugs—Cisco IOS Release 15.4(3)S4

Identifier	Description
CSCus21322	Adding NAS_IPV6_ADDRESS in the Sanet
CSCut27272	CPUHOG and crash due to Auth Manager process
CSCur59242	Crash due to tplus_client_stop_timer
CSCuu59324	router crashes @aaa_memerase
CSCus82903	BGP - %IPV6_ADDRESS-3-NULLIDB: Uninitialized interface pointer
CSCuu85298	FIB/LFIB inconcistency after BGP flap
CSCuv66776	MQC Policy-map counters do not update in T3/E3 SPA
CSCur68351	%COMMON_FIB-4-FIBIDBMISMATCH when configuring sub-int for port-channel
CSCur35098	cmfib line card crash
CSCut42214	High memory & CPU utilization on mfib-const-lc Pr process
CSCuv39005	Supervisor crash after configuring NetFlow on a BGP PIC enabled router
CSCuv15500	TCAM utilization increasing up to 100%
CSCuu50392	aaa attr list leak at dsensor_process_pkt_update_cache
CSCuv39338	ISG: DHCP Server RADIUS Proxy Memory Leak
CSCut10251	Some commands are not in running-config after AUTOINSTALL finishes
CSCus25205	Traceback@eigrp_process_dying during unconfiguration
CSCut12738	[ASR1K HSRP] Physical Link Failure Causes HSRP to Fail
CSCuu68439	Crash after no route-target import command
CSCut28445	CSCur47160 broke load balancing
CSCuu26303	Router crash triggered by service policy and ipv6 traffic
CSCus65125	Router crash with NAT @ ipnat_for_us_feature
CSCut80144	Beni MR1: Debug enabled by default on Mingla
CSCuv19154	After upgrade of IOS-XE software, appnav functionality maybe impacted.
CSCuv83793	AppNav-XE drop packets when traffic from WAAS has wrong ID
CSCuu82763	Evaluation of ciscossl in binos for OpenSSL June 2015 vulnerabilities
CSCur32628	7600 mis-programming causing intermittent packet loss

Identifier	Description
CSCuu80048	interface IP address change cause leaked routes in exported vrfs
CSCuv43978	IPv6 GRE over 6PE does not work properly
CSCuv80943	MCP_DEV:Packet drops@Ipv6NoRoute with ipv6gre configs
CSCut24140	Old active not coming up after first sso also seeing a traceback.
CSCuu28199	[Amur-MR3]IOSD crash reported@spi_iosd_ipc_process_inbound_mts_msg
CSCuu29667	ASR1K crash when snmp setting cipSecTunnelEntry
CSCus92857	Crypto Stateless redundancy causing "IPSEC install failed" after preempt
CSCuu54392	Different Tunnel Protection with shared profile cannot be used
CSCut87217	GETVPN - ASR1K GM deny policy fails when the policy is updated by the KS
CSCur29582	IPSEC-VPN: removal of "crypto-map" kills BFD session forever
CSCus79972	Crash on 'tunnel protection ipsec profile profile-name'
CSCut14502	Address pool leak upon Anyconnect reconnect and subsequent disconnect
CSCuu93699	Crash on IKEv2 cluster hub when anyconnect client tries reconnect
CSCut32445	Crash - IPSec/ISAKMP Timer driven crash.
CSCus30128	RRI dynamic L2L after client change ip address Ipsec rekey lost routes
CSCuv26780	Memory leak when qos pre-classify is configured with Crypto
CSCuj13127	SSTE: DNS IPv6 traffic fails with IKEv2 and ZBFW configured
CSCut88270	Duplicate hsrp vmac entries after OTV AEDs fail over
CSCut30167	ISIS may crash when reaching LSPFULL condition with IPv6 routes
CSCuu77927	OTV stuck in inactive status when failover due to missing isis vlan tlv
CSCup51000	CEMoUDP: PW interface still being unprovisioned, retry later
CSCuv56754	EoMPLS xconnect remains "RECOVERING" after RP SSO on egress
CSCuv29418	Router is continuously switching between active and standby EoMPLS PW
CSCuu50269	RSP2: MSPW sessions down on S-PE after SSO
CSCuu92194	RSP3:HSPW PW-Group Switchover results in traffic blackhole with no scale
CSCuv34896	VPLS autodiscovery PW failed to comeup when BGP recovers from failure
CSCuu36041	VPLS BGP AD resignalling time takes ~20-40s for multi-homing scenario
CSCuq70725	LDAP Address Error at ldap_clear_transaction_all
CSCuu88964	ASR1K Kernel crash at pidns_get()
CSCtz61014	f Linux kernel NTP leap second handling could cause deadlock
CSCuu12600	SR is not working fine in mk2fc2-sup720 device
CSCuu90695	DM/SM boundary (S,G) are not repopulated: Multicast Missing Registration
CSCur70478	Software crash at ldpx_mem_reallocz_grow due to insufficient memory
CSCuv61750	ASR903 MCP_DEV: Mismatch in VC label programming, EoMPLS scenario
CSCuu76169	PfRV3: Collocated hub MC/BR keep on publish site-prefix with enter-pfx
CSCuv83586	PI25: channel flapping with NBAR based QoS Policy for NTT
CSCut85551	Crash with DMVPN NHS using FQDN

Identifier	Description
CSCut77619	APRIL 2015 NTPd Vulnerabilities
CSCuv65370	Avoid any action on Leap SEcond indictor flag for non-leap second months
CSCup81878	Line by Line Sync fails while deleting dynamic NTP peer
CSCus34757	bgp rpki: crash if bgp default received
CSCus68229	Memory leak in OSPFv3R
CSCut63500	dot1q encapsulation causes vam2+ to crash
CSCut96721	Crash on pfr master router at oer_mc_apc_changed_prefix
CSCuu08872	Crash on pfr master router at pfr_exp_send_tc_config_internal
CSCus13902	Failure seen in OER Border router functionality
CSCuv22992	PFR router crashes due to watchdog when displaying config
CSCuu98524	PFR/OER related IOS crash
CSCuu97977	Pfrv2 load-balance not working with passive mode.
CSCuu18348	IOS PKI HA fails to initialize on standby router after reload or upgrade
CSCuu81737	Router crashes when using crypto
CSCut22660	Session in attempting state on standby when method list is default
CSCur88124	default throttling require other defaults in some cases
CSCut67877	IOS crashes when changing tunnel destination on a Tunnel with QoS
CSCuu46604	Router crashes when a failed primary link comes back up
CSCuq75576	Input queue wedged on outside interface of standby nat-ha router
CSCuo93893	RG-Infra: Add a hook for RG Domain for Reloading peer event:
CSCuu82607	Evaluation of all for OpenSSL June 2015
CSCut46130	MARCH 2015 OpenSSL Vulnerabilities
CSCus06143	CSR1k SSLVPN: Mask unsupported virtual-template type VPN from config
CSCut65242	ISG passing traffic while configured default drop should be used
CSCuu75354	ISG: Dedicated session provisioning failure post lite session conversion
CSCut87425	CPU hog in "EEM TCL Proc" after TCL script termination with long runtime
CSCuv51901	ASR1K BGP send UPDATE don't observe the TCP OPTION
CSCul10482	TFEX: Image auto download fails due to "ip tftp source-interface" config
CSCus46844	802.1x 3650 Radius Response not picked up by AAA code

Open Bugs—Cisco IOS Release 15.4(3)S3

Table 13 Open Bugs—Cisco IOS Release 15.4(3)S3

Identifier	Description
CSCut04815	LDAP authentication is not working on 5760 or 3850
CSCuu36031	Kernel crash is related to a GPF related to memory corruption.

Identifier	Description
CSCut12738	[ASR1K HSRP] Physical Link Failure Causes HSRP to Fail
CSCur32628	7600 mis-programming causing intermittent packet loss
CSCuu32159	CUBE issue with webex HA
CSCuu00050	CUBE with SRTP fallback is dropping SRTP RTP/SAVP from the 200 OK SDP
CSCur35618	[XE 3.15] FP Crashed for SRTP Video Call + DSP
CSCuu29667	ASR1K crash when snmp setting cipSecTunnelEntry
CSCut14502	Address pool leak upon Anyconnect reconnect and subsequent disconnect
CSCut30167	ISIS may crash when reaching LSPFULL condition with IPv6 routes
CSCue32350	kron crash after deconfiguring the occurance
CSCus62778	Stale Data MDT entry
CSCur70478	Software crash at ldpx_mem_reallocz_grow due to insufficient memory
CSCuq95663	CENT: small increase in IPC still exists in longevity
CSCut67137	Memory fragmentation on ASR903 due to OSPF
CSCuu24757	ASR1k QFP leak with cpp_sp_svr at module FM CACE
CSCuo51601	ISR4400 - Traffic incorrectly forwarded through class class-default
CSCus06143	CSR1k SSLVPN: Mask unsupported virtual-template type VPN from config
CSCup04062	IOS SSLVPN - Anyconnect Data traffic failure with TLS transport
CSCur10056	Memory leak in SSS Manager
CSCus77343	DSMP crash while doing OIR or module reload when active call exists
CSCut66144	VXML GW fails to handoff call to VXML Application on second VRU leg

Resolved Bugs—Cisco IOS Release 15.4(3)S3

Table 14 Resolved Bugs—Cisco IOS Release 15.4(3)S3

Identifier	Description
CSCut09164	Memory leak in AAA/EAP code in 3.3.5
CSCut31678	Memory leak in AAA/EAP code in 3.3.5
CSCur57035	ASR 1k crash on __be_bfd_fib_nh_change_cb
CSCuq09320	ASR-1002 crashed with LAN BFD and HSRP with ipv4 and ipv6
CSCus20997	ASR1k: BGP Notification of Admin shutdown triggers Graceful-Restart
CSCur66140	Import of Global routes to VRF will fail
CSCun68322	Support BGP GR for VPN AF in platform without MPLS
CSCus26146	VRF LISP routes not exported to global table with valid next hop
CSCus01544	XE3.13 rejects routes from ebgp peer due to malformed ATTR-SET attribute
CSCus54365	Memory leak in tlv_calloc
CSCur87549	ipv6 traffic over bridge-domain not working

Identifier	Description
CSCur88455	7600 IP FRR: MPLStoMPLS traffic Blackhole after VRF Configuration
CSCut31584	c7600 drops Register-Stop messages resulting into punting ASM stream
CSCut27149	POS FRR issue with traffic loss around 1 sec instead of 50ms
CSCus95226	Compact Flash corruption due to call-home directory being created
CSCus38037	crash with "show voice class ctl-file"
CSCut92745	Crash while placing MLPP calls
CSCur70959	Memory leak @ sipContentObjPvtSetBody
CSCus65095	SSTE: QoS Pre-classify was broken
CSCus34949	DHCP defect - crash due to an invalid access to a freed memory structure
CSCur55365	50% ping failure with IPv6 dual stack and dialer configured
CSCus72257	50% ping failure with IPv6 dual stack and dialer configured
CSCus57583	ASR 1K BGP Process Crash Due to EIGRP Route Redistribution
CSCup52101	EnergyWise Denial of Service vulnerabilty
CSCut01967	crashed after executed show ethernet cfm errors
CSCus53146	ASR crashes at hal_get_next_packet
CSCur43251	POODLE protocol-side fix: HTTPS Client
CSCur49548	Upgrade from 3.4.6S to 3.13.0S doesn't work with traceback and error log
CSCus86256	uCode crash when MPLS packet received on LAN side of AppNav intercept
CSCut46126	MARCH 2015 OpenSSL Vulnerabilities
CSCut30579	Dynamic PBR policy inconsistent & never update after path failover
CSCus78750	6RD: Knob to disable security check missing.
CSCur96943	CCSIP_SPI_CONTROL leak in sippmh_parse_record_route
CSCus75907	Router crashes when Fax T38 Protocol Configured
CSCur68999	config change on Tunnel int using shared tunnel protection stops traffic
CSCuq15567	Crash with %SYS-3-OVERRUN with crypto_ipsec_clear_peer_sas
CSCup97873	IPSec datapath should not print debug messages without debugs enabled
CSCuq91734	NHRP Packets are dropped after EzVPN decryption
CSCur29861	Traceback seen on c2900 platform for ike_keepalives
CSCur65486	GETVPN: Fail to delete GMs on sec-KS after 3 scheduled rekeys failure
CSCun57148	High CPU in FNF Cache Ager P
CSCus74192	Link down event does not flush the routes correctly with isis
CSCut24465	Static VFI went down after PTF reset
CSCus89274	Crash with nat/reflective acl and TCP session going through that box
CSCus69732	IOS-XE: Evaluation of glibc GHOST vulnerability - CVE-2015-0235
CSCut57290	Egress LER TTL propagation misbehaviour in per-ce label allocation mode
CSCuo67247	High CPU due to NHRP process on ASR in DMVPN ph3 after upgrading IOS-XE
CSCur28336	Memory leak and possible crash when using a logging discriminator

Identifier	Description
CSCus05038	"revocation-check ocsp none" does not timeout fast for unreachabl server
CSCus77875	List Headers leak verified cert chain Held CCSIP_TLS_SOCKET & Chunk Mgr
CSCus73553	Memory corruption crash in PKI certificate processing
CSCus54238	PKI "revocation check crl none" does not fallback if CRL not available
CSCut17865	ASR1K:13RU IOSd crash @PnP Agent Discovery after router reload
CSCus46259	ASR1k (ISG Radius-Proxy): Memory Leak after excessive client roaming
CSCut26988	Broken bw repartition - traffic is send as w/o configured bw under MQC
CSCut46705	Wrong bandwidth distribution in SIP 200 & 400 causes queue limit of 2
CSCur20444	I/O memory leak due to DHCPv6 packets.
CSCun29420	Crash observed with active IP SLA probes
CSCuq39109	Memory Fragmentation due to IP SLA
CSCus40410	ATM SPA: Incorrect SOM-COM-EOM flag set in packet buffer hdr in Ingress
CSCus88868	IOS openssl leak observed with SSL Anyconnect VPN
CSCuq25323	DLSW peers fail to connect when other DLSw peer sends FIN instead of RST
CSCue88982	MA2b:Supervisor crash seen upon Remote login and the session is idle
CSCut08626	DSMP crash at DSP packet buffer allocation
CSCuu29539	voice statistics CLIs are missing in ISR4k image
CSCut18365	Tracebacks found @ moh_multicast_recv_input
CSCus89791	g722-64 codec crash during dial tone with country code

Resolved Bugs—Cisco IOS Release 15.4(3)S2

Table 15 Resolved Bugs—Cisco IOS Release 15.4(3)S2

Identifier	Description
CSCur51387	NG3K stack: standby gets reloaded due to reason "configuration mismatch"
CSCur13587	ANCP session terminated due to message len check
CSCuq83441	BGP L2VPN uses default static next-hop instead of outging intf-addr
CSCuq99797	BGP Route-Target not advertised when rtfilter address family in use
CSCur66140	Import of Global routes to VRF will fail
CSCup48874	IPv6 neighbor link-local address not learnt after RSP Failover
CSCun68322	Support BGP GR for VPN AF in platform without MPLS
CSCus01544	XE3.13 rejects routes from ebgp peer due to malformed ATTR-SET attribute
CSCue87829	Bridge Domain EVC EFPs not mapped to VLAN post Reload/SSO
CSCun80617	Active SP crashes @ mfib_pltf_entry_extract_source followed by RP crash
CSCur94457	AToM traffic is blackholed after RP switchover
CSCur41785	IXP_MAP-3-QOS_CONFIG: ACL is not programmed after reload or RP SSO
CSCur96372	l2protocol forward feature is missing under SIP400

Identifier	Description
CSCum59931	7200 crash with DHCP suspending WCCP
CSCur10249	ASR1006 crash when IPv6 PPPoE sessions increase to several hundred
CSCup99634	IPV6 dhcp database not working on PI25 and Xe3.13
CSCuq78983	RIPv2 key-chain CLI disappears when doing config replace
CSCur11538	ASR1k lldpMIB walk (1.0.8802.1.1.2.1.3.7.1) , but lldpMIB unsupported
CSCur45606	logging discriminator doesn't work
CSCup99438	MK2:tun_decap_tinfo_control subsys missing in DFC
CSCur78068	Quad+fex mk2 (fc):after issu LV - IPC trace back, sw2(ICS) is crashed
CSCuq17828	ASR: Radius Accounting fails when using EDCSA certs
CSCur23619	IKEv2 reconnect radius accounting stop should mention terminate cause
CSCur85771	ISDN Segmentation Fault on ISR 4451
CSCuq51439	ASR903: ISIS LSP generation delayed after receiving BFD down event
CSCur97045	IS-IS Passive-interface default unavailable
CSCum90471	ASR1k: Ping failure b/w CE1 & CE3 after Switchover.
CSCur78744	LISP mobility with HSRP invalid host detection events
CSCuq85667	Crash@mcast_rw_link_dequeue on config replace in MCAST THS
CSCur36464	mVPN: Inter-AS Option B: Different RDs: proxy vector: local RD is picked
CSCur09682	Router crashes in PIM due to infinite recursion at ip_set_mdb_flag
CSCuo81912	SSTE: Unable to remove performance-monitor once the interface is deleted
CSCup67317	max_chunk_size validation incorrect in funciton chunk_create_inline()
CSCup59760	'sh mpls fwding tabel vrf slot<>' takes longer time & stucks terminal
CSCur92862	TE leaks memory when restarting isis
CSCur07571	Processor memory leak with MRCP_Client at cc_api_get_call_active_entry
CSCur62553	Netconf - Duplicate xml version start tags in hello packet
CSCuq70163	RESTAPI: POST /api/v1/acl/{acl-id}/interfaces does not show in config
CSCus38393	ASR1k:IOSD crash @process_run_degraded_or_crash
CSCur10058	IOS PKI : CRL parsing may fail if HTTP Content-Length is not specified
CSCuq74176	PKI IOS removed valid CA certificate before expiry date
CSCur14783	PnP: ZTD in ISR's blocked due to config wizard
CSCun87941	PPP link interfaces causes SUP to crash
CSCus01735	cbQosTSCfgRate64 is not supported on ASR1k/IOSXE
CSCui23670	Even if show sup-bootdisk is executed, nothing is displayed.
CSCuc68034	IO Memory Leak on FlexWan WS-X6582-2PA exec 'sh cef interface internal'
CSCuo92155	RSVP sync process crash observed with TE NSR configs
CSCup80756	SNMP Engine Crashes in IOS-XE, Segfault When Processing rttMonStats MIB
CSCum87411	software install from tftp get failed fts_client issue
CSCur78381	After a reboot of SPA-4XCT3/DS0, first 4 packet loss in channelized mode

Identifier	Description
CSCuq74492	IOS/IOSd Multiple Vulnerabilities in OpenSSL - August 2014
CSCur44075	AC ICE+ ver <= 4.0 Client unable to connect to XE SSL Headend {CSR1K}
CSCun89616	IOS Does Not Properly Respond to TLS 1.2 Client Hellos
CSCup86552	Issue with qos service installation
CSCuq54260	Session is not syncing to the standby with collect identifier remote-id
CSCuh92882	XE3.11 Seginfo->l2hw_cond_debug is set to "1" when there is no condition
CSCur68259	XE3.13 : Subscribers not pingable after 2nd "clear ip route vrf x *"
CSCur29261	Memory courruption in retrans TCP sanity check causes ISR crash
CSCup41482	TCP snd window stuck with CEF enabled

Resolved Bugs—Cisco IOS Release 15.4(3)S1

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

This search uses the following search criteria and filters:

Field Name	Information
Product	Series/Model Cisco IOS and NX-OS Software => Cisco IOS
Release	15.4(3)S1
Status	Fixed
Severity	2 or higher

Open Bugs—Cisco IOS Release 15.4(3)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.4(3)S. All the bugs listed in this section are open in Cisco IOS Release 15.4(3)S. This section describes only severity 1, severity 2, and select severity 3 bugs.

- CSCuo73442

  Symptom: A Cisco switch may crash after issuing the **no ip dhcp pool** command.

  Conditions: This symptom occurs when DHCP is configured.

  Workaround: There is no workaround.

- CSCup10266

  Symptom: IPv6 default route does not get redistributed into EIGRP without metrics.

  Conditions: This symptom occurs when redistribute static is issued without mentioning metrics.

  Workaround: Mention metrics when issuing the **redistribute static** command under EIGRP.

- CSCup11348

  Symptom: Incremental memory leaks are observed.

  Conditions: This symptom occurs under the following conditions:

– TFTP server should not be reachable which is mentioned in the DHCP database.

– Remove and add the DHCP pool.

Workaround: There is no workaround.

- CSCup13169

  Symptom: The Default static route tag value does not get updated on OSPF.

  Conditions: This symptom occurs under the following conditions:

  1. Add static default route with tag value.
  2. Configure OSPF with redistribue static and default-information originate.

  The tag value does not get updated.

  Workaround: Create a separate route map for updating the tag value. Route map should be tagged with the **default-information originate** command under OSPF.

- CSCup26658

  Symptom: An unexpected process restart occurs after running the following commands in quick succession:

  ```
  no spanning tree mode
  default interface <intf>
  ```

  Conditions: This symptom occurs when service instances are configured on the interface with encapsulation and bridge-domain configuration under the interface. Spanning tree must also be configured before running the commands.

  Workaround: Leave a 10 second gap between entering the above mentioned commands.

- CSCup48742

  Symptom: A Cisco router gets crashed.

  Conditions: This symptom occurs under the following conditions:

  1. Configure the below CLI and make sure that the SCP server IP is unreachable:

  ```
  ip dhcp database scp://tom:cisco@192.168.50.25/dhcp4 write-delay 60 timeout 5
  ```

  2. Wait for 60 seconds or the following message:

  ```
  %DHCPD-3-WRITE_ERROR: DHCP could not write bindings to
  scp://tom:cisco@192.168.50.25/dhcp4
  ```

  3. Make SSH connect from this device to the other device and exit from that connection so as to be back to the original device (optional).
  4. Press “Enter”.
  5. The following message appears:

  ```
  [Resuming connection 1 to UNKNOWN ... ]
  [Connection to UNKNOWN aborted: error status 0]
  ```

  6. The router would hang or crash. If not, run any show command (show ip int br).
  7. If all the above conditions are met, wait for the router to crash. Cisco ISR routers take around 5-10 minutes to crash and Cisco ASR routers crash immediately most of the times.

  Workaround: Use FTP or TFTP with “ip dhcp database”. Do not use SCP with “ip dhcp database”.

- CSCup54679

  Symptom: TE FRR paths are lost after an SSO.

Conditions: This symptom occurs under the following conditions:

1. TE tunnels are configured between PE1 and PE2.
2. TE NSR is configured on PE1 and FRR node protection is configured on PE1.

Before SSO, the FRR database shows the FRR paths and after SSO the FRR paths are lost.

Workaround: There is no workaround.

Resolved Bugs—Cisco IOS Release 15.4(3)S

- CSCee32792

  Symptom: A Cisco router reloads at snmp_free_variable_element while using SNMPv3 commands.

  Conditions: This symptom occurs while using SNMPv3 commands.

  Workaround: There is no workaround.

- CSCte77398

  Symptom: A Cisco ATM router configured with ATM PVC Range commands report the following error when attempting to configure a PVC Range:

  Unable to configure PVC Range. Possibly multiple users configuring IOS simultaneously.

  Conditions: This problem occurs randomly and even if there are no multiple sessions accessing the pvc-range at the same time.

  Workaround: There is no workaround.

- CSCtq21722

  Symptom: A Cisco switch may reload when configured for SNMP.

  Conditions: This symptom is observed when SNMP inform hosts are configured.

  Workaround: Remove the SNMP host configurations for SNMP informs.

  ```
  Example: no snmp-server host x.x.x.x informs version 2c <removed>
  ```

- CSCtx82890

  Symptom: After removing the encapsulation on MFR member interface, tracebacks are observed.

  Conditions: This symptom is observed when serial interface is configured with FR MLP configuration.

  Workaround: There is no workaround.

- CSCty92208

  Symptom: Customer faced crash on 6509 after configuring WCCP.

  Conditions: Customer configured WCCP with hash assignment and enabled port hashing and it will happen during redirection if packet are software switched.

  Workaround: The possible workarounds are:

  1. Disable port-hashing if we are using hash-assignment.
  2. Use mask-assignment method.

- CSCtz45833

  Symptom: A Cisco router crashes with the following message:

  ```
  Router crash: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = MPLS TE LM
  ```

Conditions: This symptom occurs when a router acts as the mid point for MPLS-TE tunnels and performs an ERO expansion. In case the ERO expansion fails (due to IGP race conditions or inter-AS scenario) and backup tunnels are in use (for MPLS-TE FRR feature), the router may crash.

Workaround: Configure the head-ends to perform a full ERO computation to avoid mid points performing any ERO expansion. This can be done using the dynamic path option or by using the explicit path that specifies strict hops for each node along the desired LSP path (using "loose" hops or partial strict hops can lead to this issue).

- CSCuc60868

  Symptom: A router randomly crashes either due to memory corruption at bgp_timer_wheel or memory chunks near bgp_timer_wheel (For example, BFD event chunks if BFD is configured or AtoM Manager chunks if LDP is configured). A crash occurs right after an LDP neighbor is up in the L2VPN setup.

  Conditions: This symptom occurs when **vpls bgp signaling** is unconfigured and then reconfigured. Both L2VPN and BGP are unconfigured and reconfigured after all L2VPN and BGP data structures are fully deleted (about 3 minutes for 5 BGP VPLS prefixes). For the repro on file, OSPF (for IGP) is also unconfigured and reconfigured. Both LDP and BGP signalling are affected by this bug.

  Workaround: Avoid unconfiguring and reconfiguring BGP L2VPN.

- CSCue00996

  Symptom: The Cisco IOS Software implementation of the Network Address Translation (NAT) feature contains two vulnerabilities when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address these vulnerabilities.

  There are no workarounds to mitigate these vulnerabilities.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-nat

  Note: The March 26, 2014, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2014 bundled publication.

  Individual publication links are in Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html

  Conditions: See the published Cisco Security Advisory.

  Workaround: See the published Cisco Security Advisory.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2014-2111 has been assigned to document this issue.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCue84703

  Symptom: When a switchover is triggered before the converge of a unicast (and multicast), the MFIB is not in “running state”, and is held in the initializing state forever.

  Conditions: This symptom occurs when a switchover is triggered before the converge of the unicast.

  Workaround: Switchover after the converge of the unicast.

- CSCuf51357

  Symptom: A vulnerability in the Secure Sockets Layer (SSL) VPN subsystem of Cisco IOS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  The vulnerability is due to a failure to process certain types of HTTP requests. To exploit the vulnerability, an attacker could submit crafted requests designed to consume memory to an affected device. An exploit could allow the attacker to consume and fragment memory on the affected device. This may cause reduced performance, a failure of certain processes, or a restart of the affected device.

  Cisco has released free software updates that address these vulnerabilities.

  There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ios-sslvpn

  Note: The March 26, 2014, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2014 bundled publication.

  Individual publication links are in Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html

  Conditions: See published Cisco Security Advisory.

  Workaround: See published Cisco Security Advisory.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2014-2112 has been assigned to document this issue.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCug17485

  Symptom: A buffer leak is observed on a Cisco router.

  Conditions: This symptom occurs while using SSLVPN.

  Workaround: There is no workaround.

- CSCug45421

  Symptom: The standby RP crashes.

Conditions: Memory corruption occurs in certain cases when the following commands are executed in quick succession. It leads to a crash later when the memory is accessed. The issue is seen only with on-demand PVCs and when the commands are copied and pasted or executed using a script or tool.

```
configure terminal
interface ATM0/0/0.2 multipoint
range pvc 11/41 11/51
create on-demand
/* Prob commands begin */
pvc-in-range 11/45
exit
no pvc-in-range 11/45
/* Prob commands end */
end
```

Workaround: Do not execute the commands in quick succession.

- CSCuh05259

  Symptom: Prompt is provided for configure replace command when **file prompt quiet** is configured.

  Conditions: This symptom is observed when “file prompt quiet” has been configured.

  Workaround: Use “force” along with the **configure replace** command.

- CSCuh09324

  Symptom: UDP based entries are not deleted from the flowmgr table resulting in crash, or poor system response, with CPU hog messages being shown.

  Conditions: Affected Platforms - images

  – ct5760-ipservicesk9.bin

  – cat3k_caa-universalk9.bin

  – cat4500e-universalk9.bin

  Device is configured with UDP services that originate from the device. This includes but not limited to the following features:

  – TFTP

  – Energy Wise

  – DNS

  – Cisco TrustSec

  Workaround: If you suspect that you are affected by this bug, please do the following, for confirmation:

```
Router#config terminal
service internal
end
Router#show flowmgr
```

  The output of this command will show many lines entries holding with the same port numbers. Disabling the feature that is being held in the flows until an upgrade can be performed, is a workaround.

  A reload is required to clear the held flows.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2013-6704 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-6704

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuh49066

  Symptom: VSS standby crashes due to LBL sync on issuing the below parser command:

  ```
  parser view li-view
  ```

  Conditions: This symptom occurs in a VSS with parser view configuration.

  Workaround: Remove the "parser view" configuration.

- CSCui05000

  Symptom: A Cisco router may crash upon importing a prefix into VRF after applying **no ipv4 multicast multitopology** under "vrf definition" for that VRF.

  Conditions: This symptom occurs while initially configuring the VRF. **address-family ipv4/6 multicast vrf** must be configured under "router bgp" mode before import route-targets are configured under "vrf definition" mode.

  Workaround: There is no workaround.

  More Info: If the crash does not occur, it is likely that importing of the prefix will not work.

- CSCui17084

  Symptom: Delay between VPN convergence and BGP-based MDT tunnel creation after router reload may cause multicast traffic loss.

  Conditions: In a BGP MVPN setup utilizing MDT SAFI, problem is seen upon BGP exiting read-only mode. VPN prefixes will be advertised immediately, whereas MDT prefixes are advertised after a BGP scanner run.

  Workaround: There is no workaround.

- CSCui63461

  Symptom: The Cisco router crashes when using CCP 2.6 and 2.7 to provision the device.

  Conditions: This symptom is observed under normal condition.

  Workaround: There is no workaround.

- CSCui64807

  Symptom: An active RP crashes during FIB sync because of memory overrun when the standby sup becomes unavailable.

  Conditions: This symptom occurs when redundant RPs are configured in SSO mode and the standby RP becomes unavailable (for instance because of crash or physical removal). The issue occurs only on Cisco 7600 RSP 720, Cisco 7600 Series Supervisor Engine 720, and Cisco 7600 platforms where the tableid "ISSU FOF LC" support is enabled. As of 03/17/2014, the tableid "ISSI FOF LC" feature is only supported on SY releases. This issue does not impact Cisco ASR 1000 Series platforms.

  Workaround: There is no workaround.

- CSCui79766

  Symptom: Upgrading hardware platform from Cisco 2811 Integrated Services Router to Cisco 2911 Integrated Services Router introduces periodic, intermittent delay in the delivery of STUN packets to OEM (Motorola) equipment.

  Conditions: This symptom occurs while upgrading hardware platform from Cisco 2811 Integrated Services Router to Cisco 2911 Integrated Services Router.

  Workaround: There is no workaround.

- CSCui83823

  Symptom: When CU executes “show tech” or any show commands which gives a long output using putty, the SSH2 putty closes prematurely.

  Conditions: This symptom is observed when “term length 0” is enabled. The putty session closes prematurely while executing “show tech show memory”.

  Workaround: Redirect the output to a file.

- CSCuj14595

  Symptom: A Cisco 3945 voice gateway running Cisco IOS Release 15.2(4)M3 or Cisco IOS Release 15.2(4)M4 may have a processor pool memory leak in the CCSIP_TCP_SOCKET process.

  Conditions: This symptom is seen on slow TCP connections, where the response is slow and frequent transmission errors are observed.

  Workaround: There is no workaround.

- CSCuj17827

  Symptom: CCD unable to unpublish hosted DN patterns on forwarders running service-routing code. This can result in stale or duplicate routes in remote cluster’s Learned Pattern table.

  Conditions: This symptom is observed during disabling the advertising service, resetting the CCD sip trunk, rebooting a cluster, or a cluster losing connection to all SAF forwarders may trigger this defect.

  Workaround: No workaround for preventing duplicate or stale routes, these routes can be purged from a remote cluster by resetting that cluster’s requesting service or configuring a temporary Blocked Learn Pattern that matches the affected patterns.

- CSCuj23293

  Symptom: A memory leak is seen in the MALLOCLITE process:

  ```
  show processes memory ------------------ Processor Pool Total: 282793968 Used:
  280754252 Free: 2039716 I/O Pool Total: 41943040 Used: 18560544 Free: 23382496
  PID TTY Allocated Freed Holding Getbufs Retbufs Process 0 0 268189264 170950536
  88785564 1354 634324 *Init* 0 0 0 0 141933756 0 0 *MallocLite* 409 0 451333208
  202702788 40928844 83639 83639 CCSIP_UDP_SOCKET 299003084 Total The memory continues
  to increase there.
  ```

  Conditions: This symptom is observed while parsing to header, Gateway gets errors as below:

  ```
  Feb 26 12:07:28 EST: Parse Error: url_parseSipUrl: Received Bad Port Feb 26 12:07:28
  EST: //2765/000000000000/SIP/Error/sippmh_cmp_tags: Parse Error in request header
  ```

  The correct response for the above should have been to send 400 Bad Request The request cannot be fulfilled due to bad syntax

  The memory associated with the above is not getting released is the side effect of the above.

  Workaround: There is no workaround.

Further Problem Description: This issue was not seen on versions earlier than 15.3X

- CSCuj31290

  Packet of Disconnect (POD) functionality does not work after upgrading router from Cisco IOS Release 15.1 to 15.2 code. POD fails with following error:

  ```
  *Sep 10 16:51:48.063: RADIUS: Dynamic-Author-Error[101] 6 Missing Attribute [402]
  Symptom: Packet of Disconnect (POD) functionality does not work after upgrading router
  from Cisco IOS Release 15.1 to 15.2 code.
  POD fails with following error:
  *Sep 10 16:51:48.063: RADIUS: Dynamic-Author-Error[101] 6 Missing Attribute [402]
  ```

  Conditions: This symptom is observed under the following conditions:

  1. When PoD with just username is sent
  2. IOS device is configured for packet of disconnect
  3. IOS device is running Cisco IOS Release 15.2 Mainline code

  Workaround: Downgrade router back to Cisco IOS Release 15.1 release of code.

- CSCuj40804

  Symptom:

  1. IPDT gets enabled on all bundle ports including RSL port due to which FEX does not come up after a reload, link flap, or SSO. FEX RSL channel members will be in ?u? state, that is unsuitable for a part of the etherchannel.
  2. IPDT also gets enabled on the Service module (FWSM) internal port-channel and there is no way to recover them other than removing NMSP (as internal port-channels are non-configurable and non-accessible).

  Conditions: This symptom occurs after a reload with “NMSP” protocol.

  Workaround: Apply “attachment-suppress” on the port first and bundle the port later. There is no workaround in the case of FWSM internal port-channel.

- CSCuj44818

  Symptom: A warning message is displayed.

  Conditions: This issue occurs while unconfiguring video monitoring.

  Workaround: There is no workaround.

- CSCuj55540

  Symptom: Exception is seen on 3945E with whitelisted scansafe traffic.

  Conditions: This symptom is observed when there is a lot of whitelisted traffic going through the ISR box.

  Workaround: Disable whitelisting.

- CSCuj66067

  Symptom: Router running out of memory after an upgrade to Cisco IOS Releases 15.3(1)S, 15.3(3)S, and 15.4(1)S.

  Conditions: This symptom is observed when huge number of route server (approximately more than 700) contexts configures in the router.

  Workaround: Perform the following workaround:

  1. Reduce the number of Route server contexts.
  2. Downgrade the IOS version to 15.2(4)S or lower release.

- CSCuj68289

  Symptom: Static SGACL permissions are not updated for authentication server assigned SGT.

  Conditions: This symptom is seen with an authentication server assigned SGT.

  Workaround: Use manual SGT or dynamic SGACL.

- CSCuj89036

  Symptom: IOSd crashes following an OIR of an eToken.

  Conditions: This symptom occurs during OIR activity on either USB port of a single eToken.

  Workaround: Do not OIR an eToken.

  More Info: When an eToken is inserted, files on the eToken need to be recursively scanned to build up the master file directory structure. This recursive scanning and building the database can take a very long time depending on the eToken contents. When dual IOSd redundancy mode is enabled, this process appears to take almost twice as long and can easily go over 10 seconds to trip off the IOSd watchdog timeout. Fix is to allow other processes to take over CPU so watchdog timeout will not happen.

- CSCuj89374

  Symptom: CFT was reporting two flows for incoming packets on a dialer interface.

  Conditions: PPPoE on underlying physical interface with ip nat outside configured on the dialer interface.

  Workaround: There is no workaround.

- CSCuj96546

  Symptom: After SSO, egress WCCP stops working in hardware, as netflow does not get installed.

  Conditions: When GRE redirection and hash assignment used for egress redirection and if the tunnel created takes the source address as the WCCP egress interface's IP address.

  Workaround: Create loopback interface and assign highest IP address to it, so that the tunnel created takes this IP address as tunnel source address.

- CSCul10573

  Symptom: On receiving a BGP update from a neighbor, the router will send an illegal network notification and flap the session.

  Conditions: This symptom occurs when the prefix received is a Leaf A-D route (RFC 6514) with an S-PMSI route serving as the Route Key.

  Workaround: There is no workaround.

- CSCul18552

  Symptom: After a switchover, QoS policy map in standby is not synced as in the case of active.

  Conditions: This symptom occurs after a switchover.

  Workaround: There is no workaround.

- CSCul24025

  Symptom: A Cisco ASR 1000 Series router crashes at __be_slaComponentProcessEvent when **ip sla udp-jitter** is unconfigured.

  Conditions:This symptom occurs when 1000+ IP SLA udp-jitter is configured and then all unconfigured immediately.

  Workaround: There is no workaround.

- CSCul27924

  Symptom: Customer experienced crash on ASR-1001 during normal operation.

  Conditions: This symptom is not observed under any specific condition.

  Workaround: There is no workaround.

- CSCul39964

  Symptom: Sessions do not get cleared. They get stuck in WT_ST state.

  Conditions: This symptom occurs when sessions are closed in bulk mode by shutting any trunk link or during a clear all session from DUT.

  Workaround: There is no workaround.

  More Info: The memory leak issue and WT_ST are related. Along with memory leak, sessions are not cleared on active RP They get stuck in WT_ST state.

```
asr1k-1#sh clock
07:18:07.045 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#
asr1k-1#
asr1k-1#sh clock
07:20:08.295 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#
asr1k-1#sh clock
07:46:34.113 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#s
6557 sessions in FORWARDED (FWDED) State
7908 sessions in WAITING_FOR_STATS (WT_ST) State
14465 sessions totalUniq ID PPPoE RemMAC Port VT
```

```
VA State
SID LocMAC VA-st Type
5978 5978 0000.6ca3.0116 Gi0/0/0.2940148 1 Vi2.3091 WT_ST
b414.8901.8e00 VLAN: 294/148 UP
5979 5979 0000.6ca3.0117 Gi0/0/0.2940149 1 Vi2.3092 WT_ST
b414.8901.8e00 VLAN: 294/149 UP
6460 6514 0000.6ca3.0134 Gi0/0/0.2940178 1 Vi2.3354 WT_ST
b414.8901.8e00 VLAN: 294/178 UP
6454 6508 0000.6ca3.0135 Gi0/0/0.2940179 1 Vi2.3350 WT_ST
b414.8901.8e00 VLAN: 294/179 UP
6453 6507 0000.6ca3.0136 Gi0/0/0.2940180 1 Vi2.3349 WT_ST
b414.8901.8e00 VLAN: 294/180 UP
6518 6572 0000.6ca3.0137 Gi0/0/0.2940181 1 Vi2.3395 WT_ST
b414.8901.8e00 VLAN: 294/181 UP
6514 6568 0000.6ca3.0138 Gi0/0/0.2940182 1 Vi2.3393 WT_ST
b414.8901.8e00 VLAN: 294/182 UP
6516 6570 0000.6ca3.0139 Gi0/0/0.2940183 1 Vi2.3394 WT_ST
b414.8901.8e00 VLAN: 294/183 UP
6560 6614 0000.6ca3.013a Gi0/0/0.2940184 1 Vi2.3413 WT_ST
```

- CSCul40478

  Symptom: A crash was seen in the periodic accounting process due to the stale reference of the attribute list with AAA accounting DB (this specific attribute list is used by the periodic accounting process for sending the interim accounting records).

  Conditions: This symptom occurs with Policy Component allocate AAA attribute list handle. This handle reference is shared among multiple components for processing. A component can free the attribute list using this handle. AAA does not validate the handle before usage. The policy will not share the same attribute handle reference with other components. The policy will share a copy of the attribute list to other components so that the component does not refer the same handle.

  Workaround: There is no workaround.

- CSCul43968

  Symptom: Mroute states never expire on egress PE without any active downstream receivers.

  Conditions: This symptom occurs in an IPv6 multicast running in a VRF scenario and during unconfiguration of such a loopback interface that has MLD joins on it.

  Workaround: There is no workaround.

- CSCul46792

  Symptom: VCs remain down on ISSU from previous Cisco XE3.12 to Cisco XE3.12 Release.

  Conditions: This symptom is observed under the following conditions:

  1. VPLS BGP Signalling is configured
  2. VC’s are established in the Active RP

  Workaround: There is no workaround.

- CSCul49375

  ```
  Symptom: The Cisco ASR 1000 router displays the following messages in the logs:
  %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0) -Traceback=
  1#cb40dca901558e45a65b881a8695af4f :400000+8653B3 :400000+893696 :400000+DF330C
  :400000+DED89B :400000+DF8643 :400000+1F57F36 :400000+1F4BBFB :400000+1F33BA7
  :400000+1F336C1 :400000+1F34FF9 :400000+1F27763 :400000+1F29B16 :400000+2546FF3
  :400000+2546EDD :400000+1F2930B
  ```

  No new PPPoE sessions can be established anymore.

Conditions: The conditions to this symptom are unknown.

Workaround: Reload the device.

- CSCul49852

  Symptom: A router might see PPPoE-sessions in the WAITING_FOR_STATS (or WT_ST) status.

  Conditions: This symptom was observed by specific users or because of using a specific profile or service like ShellMaps and Radius. The system is configured as BRAS aggregating PPPoEoA or -oE-sessions.

  Workaround: There is no workaround.

- CSCul54254

  Symptom: Invalid LSAs are not flushed by the router which has their Advertising Router ID. Specifically, Router LSAs which do not have LSID of 0 will not be flushed if the router does not re-originate them, and any LSA with a type that the router does not recognize.

  Lingering LSAs could lead to incorrect routing in some very obscure instances. For example, stale Router LSA fragments from two neighboring routers would need to remain in the network. There would not be a routing problem if only one router's stale Router LSA fragment was allowed to linger.

  Conditions: There are several possible scenarios that could lead to this symptom. One example is that a router is configured with many interfaces attached to an OSPFv3 instance such that it originates more than one Router LSA fragment. Then the router is reloaded before the configuration is saved, and after the reload it does not reoriginate some of the Router LSA fragments.

  Workaround: There is no workaround.

- CSCul55900

  Symptom: A FlexVPN Scale rate degradation occurs due to more CPU consumed by static processes.

  Conditions: This symptom occurs under the following conditions:

  1. Configure UUT to be the flexvpn server which can scale upto 10K sessions.
  2. Configure IKEv2 Authorization policy.
  3. Try to bring up the flexvpn 10K sessions and monitor the CPU usage.

  Workaround: Remove IKEv2 authorization policy. In such a case, IKEv2 routing and mode configuration cannot be verified.

- CSCul72121

  Symptom: Continuous trace backs on the PTF console is observed and PTF crashes during a soak.

  Conditions: This symptom occurs under the following conditions:

  1. Create an MDS profile as attached.
  2. Leave the setup for soak for 12 hours.

  Workaround: Reload ACT and SBY PTF.

- CSCul75876

  Symptom: A router may crash in an OSPF process during reconfiguration.

  Conditions: This symptom occurs under the following conditions:

  1. Configure the router with "ipfrr" in area 0.
  2. Connect router to area 0 through two links. For some route one interface is the primary path, and the second is the repair path.

3. Configure router as ABR, that is, have a non-zero area with a neighbor. Do not configure “ipfrr” in the non-zero area. Quickly remove the IP address from both the interfaces in area 0 and router the may crash.

Workaround: Changes to the reconfiguration procedure will avoid the crash.

- Shutdown the interface before removing the IP
- Remove the IP from one interface in area 0, wait for a few seconds and remove the IP address from the second interface in area 0.

- CSCul86211

  Symptom: When LNS switches off while the sessions keep on establishing at LAC, LAC finds the l2tp db memory exhausted after sometime. Due to this, it fails to update the session in the database and during this period a crash is observed.

  Conditions: This symptom occurs when LAC tries to add l2tp session in the database and fails to do so. In order to handle this error condition, LAC frees the l2tp and l2x session twice. This double free is the reason for crash.

  Workaround: There is no workaround.

- CSCul87037

  Symptom: An “sg subrte conte” chunk leak occurs while roaming.

  Conditions: This symptom occurs after an account-logoff and if service permit is configured in control policy. In case of a service permit, the subscriber remains unauth and is redirected to the portal once again. Post successful second account logon and the subscriber session is cleared by timeout or cli, the leak is seen and the same client will not be able to create the session once again. The leak is seen after simulating for the second time account-logon. And if service permit is configured.

  In case of service disconnect configured under account-logoff, account-logon is not a practical scenario as the portal is not reachable for the client.

  Workaround: Use **service disconnect** for **event account-logoff**.

  ```
  class type control always event account-logoff 1 service disconnect delay 10 !
  ```

- CSCul88004

  Symptom: DPSS packet injects fails to work.

  Conditions: This has been observed to occur when the onePK application name contains space characters, for example, white space and tab.

  Workaround: Rename the application with no white-spaces.

- CSCul90553

  Symptom: Cisco IOS-XE RP2-based platforms are unable to reach 4000 IPSec tunnels with DMVPN EIGRP.

  Conditions: This symptom occurs when DMVPN with EIGRP is used on Cisco IOS-XE RP2 platforms.

  Workaround: Use previous Cisco IOS XE images (such as Cisco IOS XE Release 3.11).

- CSCul90667

  Symptom: Error messages and tracebacks are printed to the console.

  Conditions: This symptom occurs when IGP times out while Standby RP becomes NSR Active.

  Workaround: Enable NSR under IGP to ensure no timeout occurs.

- CSCul92497

  Symptom: The Cisco 7600 router providing layer2 EoMPLS services may stop forwarding ingress and egress traffic for an xconnect for which a backup peer config has been applied.

  Conditions: This symptom occurs in Cisco 7600 routers running Cisco IOS Release 15.2(4)S4a with ES+ cards (access or core facing) and xconnect configured under a service instance.

  Workaround: Clear the xconnect on the Cisco 7600 router side. Clearing on the remote size does not have an effect.

- CSCul96778

  Symptom: A router may crash and reload with BGP related traceback in an extremely rare timing condition while running “show ip bgp vpnv4 vrf XXXX nei A.A.A.A”.

  Conditions: While making BGP related changes such as moving the same neighbor with quick operation of “no neighbor x.x.x.x” and then “neighbor x.x.x.x” across VRFs. Imediately after this if we type a “show ip bgp vpnv4 vrf XXXX nei A.A.A.A” - on a Cisco router running IOS and BGP, then in extremely rare timing condition the router may crash. The possibility of this to happen increases if the configuration and unconfiguration is done from one console and the show operation done from other console.

  Workaround: When doing configuration and un-configuration and then show, its better to serialize the operation rather than aggressively use multiple consoles to do all actions at the same time.

- CSCul99015

  Symptom: In VPLS using BGP signaling with Inter AS, when a PE on another AS is reachable through multiple ASBRs, the PW destination and the next hop PE address of some or all of the PWs in the standby RP remains as the non-preferred ASBR address instead of the preferred ASBR address.

  Conditions: This symptom occurs under the following conditions:

  1. BGP L2VPN NLRIs received first from an ASBR becomes a less preferred ASBR on receiving NLRIs for the same VE-IDs from a more preferred ASBR.
  2. NLRI received from the more preferred ASBR has the same values (VEID, VBO, VBS, Label Base, MTU and CW) as the ones received previously from the other ASBR.

  Workaround: Bring up the BGP session with the more preferred ASBR first. This would cause no updates to existing NLRIs even if received from other less preferred ASBRs.

- CSCum00056

  Symptom: ASR IOSd crash occurs with the following error:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ISG CMD HANDLER
  ```

  Conditions: This symptom occurs when changes are made through RADIUS.

  Workaround: There is no workaround.

- CSCum04512

  Symptom: When an RP switchover is done (which is head end for 500 TE tunnel and tail end for 500 TE tunnels), the RSVP label is assigned to the TE tunnel change and this in turn causes a traffic loss of 45 seconds on the pseudowire which is directed through these tunnels.

  Conditions: This symptom occurs under the following conditions:

  – TE RID under the IGP is configured as a loopback other than the first one.
  – SSO is performed.

  Workaround: Configure the TE router ID under the IGP to be the first loopback interface.

- CSCum07119

  Symptom: Router generates tracebacks or crashes depending on platforms when **show application ip route** command is used concurrently with application route deletion.

  Conditions: This symptom is observed when the **show application ip route** command is issued when JAVA onePK SDK is handling route replace operations.

  Workaround:

  1. Use **show ip route** command to display the application routes and not **show application ip route** command.
  2. Use onePK GET ROUTE API to get the status of application added route.
  3. Use **show application ip route** only when there is no route delete is in progress.

- CSCum11118

  Symptom: A Cisco ISR router crashes due to stack overflow in the “ADJ background” process. The following syslog may be seen just before the crash:

  ```
  000105: Dec 9 04:08:44.447 UTC: SYS-6-STACKLOW Stack for process ADJ background
  running low, 20/6000.
  ```

  Can also cause crash due to memory corruption, would show messages like

  current memory block, bp = 0x3B727044, memorypool type is Processor data check, ptr = 0x3B727074

  ```
  next memory block, bp = 0x3B729A60, memorypool type is Processor data check, ptr =
  0x3B729A90
  previous memory block, bp = 0x3B725DCC, memorypool type is Processor data check, ptr =
  0x3B725DFC
  ```

  Conditions: The conditions to this symptom are unknown.

  Workaround: There is no workaround.

- CSCum14830

  Symptom: Leaking IPv6 routes is observed from a VRF table into the global table using BGP. These routes consist of the following:

  1. BGP routes learned from the VRF IPv6 BGP peer.
  2. Redistributed static and connected routes.

  The BGP routes leak fine, but the redistributed static and connected routes have an issue. After the redistributed routes leak, the exit interface shows “null0”. Sometimes instead of showing the exit interface as “null0”, it shows a random interface which is a part of VRF and has IPv6 enabled on it.

  Conditions: This symptom occurs with IPv6 redistributed connected and static routes into BGP VRF (could also be redistributed from other protocols as well but have not been tested).

  Workaround: There is no workaround.

- CSCum15232

  Symptom: A Cisco IOS router may crash using LDAP while performing TLS operations.

  Conditions: This symptom was observed in Cisco IOS Release 15.3(3)M1.4. Other versions can be affected as well.

  Workaround: There is no workaround.

  More Info: LDAP is used in IOS SSLVPN deployment to authenticate users.

- CSCum17958

  Symptom: An IOSd crash is observed during a configuration replace.

  Conditions: This symptom occurs on configuration with a port-channel interface.

  Workaround: There is no workaround.

- CSCum22612

  Symptom: Since the ASR fails to send MM6 [being a responder] in the absence of a valid certificate, IKE SAs start leaking and hence get stuck in MM_KEY_EXCH state. Multiple MM_KEY_EXCH exist for a single Peer on the ASR, however the Peer does not retain any SAs for ASR in this case. Along with CAC for in-negotiation IKE SAs, these stuck SAs block any new SAs or IKE rekeys even after renewing the certificates on the ASR.

  Conditions: This symptom is observed under the following conditions:

  – ASR acting as IKEv1 termination point [sVTI for example] and is a responder.
  – IKE authentication mode is RSA-SIG [Certificates].
  – On the ASR, the ID-Certificate is either Expired or Not-present for a given sVTI tunnel
  – The ASR also has a IKE in-negotiation CAC of a certain value.

  ```
  Example: crypto call admission limit ike in-negotiation-sa 30
  ```

  Workaround: Perform the following workarounds:

  1. Manually delete stuck SAs by using: **clear crypto isakmp 12345**, where 12345 is conn_id of a stuck SA. Repeat this for each stuck SA
  2. Temporarily increase CAC to accommodate new SA requests: crypto call admission limit ike in-negotiation-sa 60

  More Info: Found and Tested in Cisco Release XE 3.7.4 or Cisco IOS Release 15.2(4)S4.

- CSCum29064

  Symptom: Syncing dual-stack iWAG session to STANDBY does not occur.

  Conditions: This symptom occurs when IPv4 and IPv6 FSOL is received from same client at ISG together (or very less time gap) for a dual-stack session. In this case, the session does not sync to STANDBY for the previous IPv6 FSOL and ISG gets a new IPv4 FSOL.

  Workaround: There is no workaround.

- CSCum34830

  Symptom: A router crash is observed.

  Conditions: This symptom occurs while performing VRRP and VRRS-related configuration changes.

  Workaround: Unconfigure the **ip pim redundancy <>** command before deleting the subinterface or disabling PIM on an interface.

- CSCum36825

  Symptom: No IPv6 global unicast address is assigned to PPP Virtual access interfaces and to IPv6 over IP/GRE tunnel interfaces.

  Conditions: Virtual access interface is configured using the command “ipv6 address autoconfig”.

  Workaround: There are no workarounds.

- CSCum45122

  Symptom: An IPv6 MFIB entry is not removed after the mroute expires.

Conditions: This symptom occurs only with the partitioned MDT profile for mLDP. The PE router could get into a trouble state if it receives traffic first and then almost immediately after that receives an MLD join on the same interface for the same group.

Workaround: Remove VRF context and then reconfigure it.

- CSCum46850

  Symptom: Using LISP set tags on routes imported to the RIB when exporting LISP routes from the RIB to BGP fails.

  Conditions: This symptom occurs when redistribute list route-map is used under bgp with a route-map that contains match tag.

  Workaround: There is no workaround.

- CSCum48221

  Symptom: 3560CG box memory is showing as low as 3.15MB.

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCum52216

  Symptom: After a reload, **ip pim sparse-mode** is gone on interface lisp 0.x (x denoted the LSIP interface number).

  Conditions: This symptom occurs after a reload.

  Workaround: There is no workaround.

- CSCum61595

  Symptom: Alignment errors are observed after upgrading to Cisco IOS Release 15.2(4)M5.

  ```
  Jan 9 19:42:59.623 GMT: %ALIGN-3-CORRECT: Alignment correction made at 0x6477F81Cz
  reading 0x6BE87495 Jan 9 19:42:59.623 GMT: %ALIGN-3-TRACE: -Traceback= 0x6477F81Cz
  0x647805D0z 0x6478FE70z 0x64751088z 0x64B99F4Cz 0x64B99FD4z 0x64752 284z 0x647525ACz
  ```

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

- CSCum62783

  Symptom: The following alignment errors are seen after a PPPoE session establishment for the first time after a reboot:

  ```
  *Jan 14 07:24:40.591: %ALIGN-3-CORRECT: Alignment correction made at 0x32B2DFF4z
  reading 0xE7790ED *Jan 14 07:24:40.591: %ALIGN-3-TRACE: -Traceback= 0x32B2DFF4z
  0x32B1E274z 0x32B1EECCz 0x32B1EF90z 0x332E550Cz 0x332E54F0z 0xFFFF1A00z 0xFFFF1A00z
  ```

  Conditions: This symptom occurs when **pppoe-client ppp-max-payload** is configured under the Ethernet interface.

  Workaround: There is no workaround.

- CSCum63121

  Symptom: Localhost not reflected in “show call history voice last 2”.

  Conditions: This symptom is observed when UUTs are loaded with c2900-universalk9-mz.SPA.153-3.M1.9.

  Workaround: There is no workaround.

- CSCum64565

  Symptom: Router crashes while getting NTP status.

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCum65451

  Symptom: A crash occurs due to multicast stack overflow memory corruption.

  Conditions: This symptom may occur when PIM is enabled on a LISP interface and Auto-RP is also enabled.

  Workaround: Configure **no ip pim autorp** before any other PIM or LISP configuration.

- CSCum67166

  Symptom: The router hangs after loading an image.

  Conditions: This symptom occurs with the latest whales-universal-mz mcp_dev image.

  Workaround: There is no workaround.

- CSCum71701

  Symptom: This bug can stop traffic from being forwarded by an upstream router when the **ip pim join-prune-interval** command is configured on the downstream router's upstream LISP interface.

  Conditions: This symptom occurs when the **ip pim join-prune-interval** command is configured with a value greater than the default on a LISP interface.

  Workaround: There is no workaround.

- CSCum78363

  Symptom: Local circuit keeps DOWN state.

  Conditions: This symptom is observed when L2TPv3 session is configured.

  Workaround: There is no workaround.

- CSCum85493

  Symptom: Ping fails with tunnel protection applied.

  Conditions: Tunnel protection applied on GRE tunnel interface, using IKEv1 to negotiate IPsec SAs and remote node (IKEv1 responder) behind NAT.

  Workaround: The users can switch to IKEv2.

- CSCum85813

  Symptom: Shut primary static router and secondary static is not installed automatically.

  Conditions: This symptom is seen on the sites where the BFD state of the backup static route is marked as "U" in the output of "show ip static route bfd".

  Workaround: Reinstall the default backup static route.

- CSCum85923

  Symptom: Router-solicitation (RS) messages are dropped on the switch port that have IPv6 RA guard enabled. On removing RA guard, RS messages go through.

  Releases tested:

  Affected releases: 151-2.SG2 and 152-1.E.bin

  Unaffected releases: 150-2.SG.bin

Conditions: This symptom occurs when “ipv6 nd raguard” is enabled.

Workaround: There is no workaround.

- CSCum86841

  Symptom: When upgrading from Cisco IOS XE Release 3.2S to Cisco IOS XE Release 3.9S, the DHCP server NACKs the client while sending renew. This worked in Cisco IOS XE Release 3.2S and not in Cisco IOS XE Release 3.9S.

  Conditions: This symptom occurs when the DHCP server is provisioned to give out an IP address using a host pool (where the MAC address is tied to IP address). After the client gets the IP address, it downloads the configurations from the TFTP server and update the new MAC address after which when the client sends a renew, the DHCP server NACKs the client till the binding is present.

  Workaround: There is no workaround. Downgrade to Cisco IOS XE Release 3.2S.

- CSCum88382

  Symptom: BFD session not established upon RP Switchover and back.

  Conditions: This symptom is observed during RP switchover and switchback.

  Workaround: There is no workaround.

- CSCum89148

  Symptom: Map-requests are forwarded to sites whose locators do not match the configured allowed-locator policy.

  Conditions: This symptom is observed when the {ipv4 | ipv6} map-resolver allowed-locator registered is configured, and allowed-locator configuration is present under “site”.

  Workaround: There is no workaround.

- CSCum93027

  Symptom: A Cisco router reloads unexpectedly.

  Conditions: This symptom occurs when the following conditions are reproduced:

  1. Configure a subinterface with IPv6.
  2. Configure OSPFv3 on the subinterface.
  3. Configure IPSec authentication for OSPFv3 on the subinterface.
  4. Shutdown the subinterface.
  5. Remove the subinterface.

  Workaround: Unconfigure the OSPFv3 IPSec authentication configuration before removing the subinterface.

- CSCum93078

  Symptom: Image installation fails for K10.

  Conditions: This symptom occurs after trying to install a tar image on K10. Installation of a bin image fails.

  Workaround: Reboot the switch.

- CSCum94228

  Symptom: Local CAC displaying all information about each flows. This may impact show output for customer in a set up where we could possibly have large number of flows.

  Conditions: This symptom is observed in a scaled configuration.

Workaround: There is no workaround.

- CSCum95330

  Symptom: Removing an Ethernet service instance which is a member of a bridge domain may cause the router to reload.

  Conditions: This symptom is observed when the last service instance is removed from the bridge domain and there are still members of the bridge domain which are not service instances (such as VFIs).

  Workaround: Completely unconfigure the bridge domain and reconfigure it.

- CSCun00488

  Symptom: Duplicate records are exported from MMA.

  Conditions: This symptom occurs in the following topology:

  ```
  SRC --- UUT --DST | collector
  ```

  Set the configuration at the UUT to export all the records to the collector. At the exporter, duplicate records are noticed.

  Workaround: There is no workaround.

- CSCun04467

  Symptom: Prior to receiving a label via the Label Distribution Protocol (LDP), the output of **show mpls l2transport vc detailed** and **show l2vpn atom vc detailed** fail to properly indicate the lack of a remote binding.

  Conditions: This symptom has been observed in Cisco IOS Release 15.4(02)S.

  Workaround: There is no workaround.

- CSCun07772

  Symptom: A Cisco router crashes.

  Conditions: This symptom occurs on deleting a subcriber's session in attempting state by a COA script as shown below:

  ```
  #!/bin/sh CISCO=$1 # bras SessionID=$2 CoaSecret='secret' #clear ISG session on BRAS
  /bin/echo
  "User-Name="undef",Acct-Session-Id="$SessionID",cisco-avpair="subscriber:command=accou
  nt-logoff"" | /usr/bin/radclient -x $CISCO:1700 coa $CoaSecret
  ```

  Workaround: Do not use the COA script for deleting the subscriber's session.

- CSCun11782

  Symptom: Rtfilter prefixes are sent with incorrect next-hop equal to next-hop of the default static route in GRT instead of BGP router-id.

  Conditions: This symptom occurs with a default static route present in GRT pointing, for example, to the next-hop known behind the connected interface.

  Workaround: Replace the default static route with a more specific static route or remove static and clear BGP.

- CSCun11927

  Symptom: Link-OAM breaks after link flap between the Cisco Catalyst 4500-X Series Switch and the Cisco ASR 9000 Series Router. With an interface with LACP + Link-OAM configuration when the connection between the Catalyst 4500-X Series Switch(IOS XE) and Cisco ASR 9000 Series

Router(IOS XR) flaps, the link does not restore due to the following deadlock : LACP PDU does not start unless OAM starts on the Cisco ASR 9000 Series Router side and Link-OAM PDU does not start unless LACP starts on the Catalyst 4500-X Series Switch side.

With the above scenario after a link flap the link gets stuck in (suspended) LACP state on the Catalyst 4500-X Series Switch and non-connected state on Cisco ASR 9000 Series Router. The link has to be restored with manual reconfiguration in a particular sequence to avoid the above dead lock.

Conditions: This symptom occurs due to a combination of Link-OAM and LACP between a Catalyst 4500-X Series Switch and a Cisco ASR 9000 Series Router.

Workaround: Manually restart the link-OAM session and toggle LACP. To restore the link, change the configuration sequence on the Catalyst 4500-X Series Switch side in such a way that the LACP packet goes ahead first and then the Link-OAM PDU.

```
interface x/x
shut
no ethernet oam
no channel-group <x> active
no shut
channel-group <x> active
ethernet oam
```

or

Disable EFD on the Cisco ASR 9000 Series Router side.

or

Toggle OAM on the Cisco ASR 9000 Series Router side.

- CSCun13399

  Symptom: Flow-ids are not synced on the standby for some of the IMA VCs on an HA setup.

  Conditions: This symptom occurs when an HA router is reloaded with IMA VCs enabled on it.

  Workaround: There is no workaround.

- CSCun13688

  Symptom: The Cisco Catalyst 6500 Supervisor Engine 2T with CLNS routing configured crashes after **show clnbs route**.

  Conditions: This symptom occurs when CLNS routing is configured.

  Workaround: There is no workaround.

- CSCun19455

  Symptom: When an access-list is applied to an interface using onePK, the “ip access-group” configuration will appear in the running configuration. When the app terminates, this configuration is removed. Additionally, any manually configured access-group for that interface is removed.

  Conditions: This occurs when using onePK 1.1.0. The ACL lifetime need not be set to persistent.

  Workaround: There is no workaround.

- CSCun25912

  Symptom: Configurations dynamically applied to the virtual-access interface might be lost over the reconnection while using the autoreconnect feature on Cisco Anyconnect on the ASR platform.

  For example, the interface after initial connection establishment would have a QOS service policy applied:

  ```
  ROUTER#sh derived-config int virtual-access 1
  !
  ```

```
interface Virtual-Access1
ip unnumbered GigabitEthernet0/0/1
tunnel source 10.1.1.1
tunnel mode ipsec ipv4
tunnel destination 10.10.1.100
tunnel protection ipsec profile ipsec-profile
no tunnel protection ipsec initiate
service-policy input INPUT-POLICY
end
```

After reconnection the INPUT-POLICY is missing:

```
ROUTER#sh derived-config int virtual-access 1
!
interface Virtual-Access1
ip unnumbered GigabitEthernet0/0/1
tunnel source 10.1.1.1
tunnel mode ipsec ipv4
tunnel destination 10.10.1.100
tunnel protection ipsec profile ipsec-profile
no tunnel protection ipsec initiate
end
```

Conditions: This symptom is observed with configurations being applied from the user AAA profile over radius authentication. Affected parameters observed are QOS service policies and access-group.

Workaround:

1. Do not use the reconnect feature.

or

2. Apply the configurations directly to the virtual-template (if this is an option).

- CSCun28171

  Symptom: An ISG will stop processing CoAs for a subscriber session when CoAs are received in rapid succession. The received CoAs are queued but never processed.

  Conditions: This symptom occurs when multiple CoAs for a single subscriber session are received in short time (milliseconds).

  Workaround: The subscriber session needs to be reset to recover. There is no workaround known yet to avoid the situation from happening.

- CSCun31021

  Symptom: A vulnerability in IKE module of Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to affect already established Security Associations (SA)..

  The vulnerability is due to a wrong handling of rogue IKE Main Mode packets. An attacker could exploit this vulnerability by sending a crafted Main Mode packet to an affected device. An exploit could allow the attacker to cause dropping of valid, established IKE Security Associations on an affected device.

  Conditions: Device configured to process IKE request that already has a number of established security associations.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C CVE ID

  CVE-2014-2143 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at:
http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2143

Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCun31450

  Symptom: CPU hog followed by crash.

  Platforms

  – ct5760-ipservices.bin

  – cat3k_caa-universalk9.bin

  – cat4500e-universalk9.bin

  Conditions: This issue occurs while running udp IP SLA applications.

  Workaround: There is no workaround.

- CSCun36655

  Symptom: If the terminal adjacency of a lisp interface is removed and then re-added, the lisp interface MTU may remain at the invalid value of 65535. This can be seen in the **show cef interface** <*intf*> **internal** command output.

  IPsec will obtain the MTU value from CEF and LISP, and the incorrect MTU will cause drops of large packets.

  IPSEC MTU incorrectly computed - causing packet drops on large packets traversing from "inside" to "outside" are dropped.

  Conditions: This symptom is observed in the following Cisco C800 Series: Cisco IOS Software, C890 Software (C890-UNIVERSALK9-M), Version 15.3(3)XB12, RELEASE SOFTWARE (fc2)

  Workaround: A workaround is to toggle the IP MTU config on the lisp interface. Use "show run lisp0.1" to determine the MTU. Then use "ip mtu <mtu>" to first set it to a lower value, and then to set it back to the original value.

  ```
  Example:
  sh run interface lisp0.1
  interface LISP0.1 ip mtu 1398 crypto map CM end
  conf t
  interface lisp0.1
  ip mtu 1200
  ip mtu 1398

  More Info: Originally [Cisco IOS Release 15.3(1)T] the MTU was accurately computed as:
  RTR13-xTR#sh cry ipse sa vrf DeptA | in mtu path mtu 1456, ip mtu 1456, ip mtu idb
  LISP0.1 path mtu 1456, ip mtu 1456, ip mtu idb LISP0.1 path mtu 1456, ipv6 mtu 1456,
  ipv6 mtu idb LISP0.1 path mtu 1456, ipv6 mtu 1456, ipv6 mtu idb LISP0.1 RTR13-xTR#
  ```
  In 153-3.XB12, the MTU is as follows:

  ```
  !
  RTR#show crypto ipsec sa
  | inc mtu ! plaintext mtu 65458, path mtu 65535, ip mtu 65535, ip mtu idb LISP0
  ```

- CSCun38333

  Symptom: Locator ID Separation Protocol (LISP) local EID database locator configured through the "database-mapping <eid-prefix> ipv6-interface <interface> priority <priority> weight <weight>" command uses deprecated IPv6 address on specified interface.

  Conditions: Multiple IPv6 addresses available on an interface with the lexicographically first address being deprecated.

Workaround: There is no workaround.

- CSCun40868

  Symptom: The following messages are seen continuously on t_base_4 image:

  ```
  *Feb 28 00:18:00.359: %CFT_API-3-CFT_ERRMSG_NO_MEMORY: CFT could not allocate memory
  for the flow cft_private_insert_pre_flow_tuple, parent_fid: 0
  ```

  Conditions: The issue is seen after configuring the router with Medianet.

  Workaround: There is no workaround.

- CSCun41292

  Symptom: On a Cisco ASR 1001 router running Cisco IOS Release 15.3(1)S, a crash occurs when the “show ip ei vrf X topo X.X.X.X/X” command is executed. The X.X.X.X/X must be in “FD is infinity” status in EIGRP as CSCtz01338.

  asr1001_bew_03# show ip ei vrf

  ```
  * to all | i Infinity P 174.162.XX.XX/24, 0 successors, FD is Infinity, U, serno 37,
  refcount 1 snip P 174.180.XX.XX/29, 0 successors, FD is Infinity, U, serno 46,
  refcount 1
  asr1001_bew_03#show ip ei vrf 1 to 174.162.XX.XX/24

  Exception to IOS Thread: Frame pointer 0x7F63DF6602D0, PC = 0x1956C8D
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Exec -Traceback=
  1#980611ad3b9665cd80fe5178bcd6036a :400000+1556C8D :400000+1556B09 :400000+15569D1
  :400000+157DE39 :400000+15197A2 :400000+1518659 :400000+156BA5E :400000+15591D1
  :400000+1189768 :400000+1188E6D :400000+1186E15 :400000+484F270 :400000+11A1CA0
  Fastpath Thread backtrace: -Traceback= 1#980611ad3b9665cd80fe5178bcd6036a
  c:7F64154A4000+BE002
  Auxiliary Thread backtrace: -Traceback= 1#980611ad3b9665cd80fe5178bcd6036a
  pthread:7F640ED43000+A7C9
  ```

  Conditions: This symptom occurs when X.X.X.X/X is in “FD is infinity” status in EIGRP.

  Workaround: There is no workaround.

- CSCun45272

  Symptom:

  1. Standby RP will have out-of-sync entries. With MPLS-TE NSR enabled, the standby RP will have out-of-sync entries which will result in flapping of the path-protected LSP of the tunnel after an SSO.
  2. Leaking an LSP. A third LSP will be signaled and leaked (there is no management of the LSP). There are supposed to be two LSPs at steady state (primary and path protected), but with this defect, there will be primary, path protected, and leaked LSP.

  Conditions: This symptom occurs with a reoptimization of a tunnel that has failed with path protection enabled.

  Workaround: There is no workaround.

- CSCun46486

  Symptom: A Cisco device crashes every 2-3 days when the SNMPSET operation is used to create guest users.

  Conditions: This symptom occurs when guest users are created through SNMPSET operations at a very high rate.

  Workaround: There is no workaround.

- CSCun48344

  Symptom: A config-sync failure occurs due to the **address-family ipv6 unicast vrf** command during the immediate unconfiguration and reconfiguration of VRF definition.

  Conditions: This symptom occurs with attached running configurations.

  Workaround: There is no workaround.

- CSCun52430

  Symptom: Removing explicitly configured queue-limit configuration via “no queue-limit” on a user-defined class may not actually remove the preconfigured queue-limit parameter from PD.

  Conditions: This symptom is observed when an explicitly created queue-limit is removed.

  Workaround: Reconfigure queue-limit with a desired (or default) value.

- CSCun65000

  Symptom: Traffic loss of about 200-500 ms is observed.

  Conditions: This symptom is observed on an RLFA cutover.

  Workaround: There is no workaround.

- CSCun67364

  Symptom: Convergence on Local link failure with rLFA is higher than one second.

  Conditions: Configure rLFA and perform local link failure. The problem is likely seen when configuring a small spf-interval value.

  Workaround: Do not configure too small spf-interval.

- CSCun68542

  Symptom: CSR1000V router running XE3.11 (15.4(1)S) working as Route Reflector.

  The route-reflector is advertising prefixes with incorrect subnet masks to ibgp peers and route-reflector clients. The incorrect prefixes are not present in the bgp table of the route-reflector itself, however they do get installed in the bgp table of the router receiving the update.

  Conditions: This symptom is observed when BGP route reflector uses the additional paths feature.

  Workaround: Disable additional path feature either globally under address-family or per neighbor.

- CSCun71301

  Symptom: A higher layer app such as LISP ends up using a deprecated IPv6 address as returned by the IPv6 service even if a valid address exists for an interface.

  Conditions: This symptom occurs when multiple IPv6 addresses are available on an interface with the lexicographically first address being deprecated.

  Workaround: There is no workaround.

- CSCun72459

  Symptom: High traffic loss is observed with setups having BGP and microloop avoidance combination.

  Conditions: This symptom occurs with the following combination:

  1. IP FRR is turned on.
  2. Cisco IOS XE Release 3.11 code (or newer) that enables microloop avoidance by default.
  3. BGP configurations.

Workaround: Disable the microloop avoidance feature. For example, in ISIS, execute the following commands:

```
router isis <process name>
microloop avoidance disable
!
```

However, there will be some traffic loss due to the lack of microloop avoidance.

- CSCun72939

  Symptom: QoS Egress Marking does not work for GRE Tunnels.

  Conditions: This symptom is observed under the following conditions:

  – The issue happens for fragmented packet.

  – The issue is found on Cisco IOS Release 15.3(3)M2.

  Workaround: There is no workaround.

- CSCun73515

  Symptom: A router crashes due to RMON.

  Conditions: This symptom occurs on activation of an RMON event.

  Workaround: There is no workaround.

- CSCun73782

  Symptom:

  A vulnerability in LISP control messages processing on Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to cause a vulnerable device to disable CEF forwarding and eventually drop traffic passing through.

  The vulnerability is due to insufficient checking of certain parameters in LISP control messages on ITR. An attacker could exploit this vulnerability by sending malformed LISP control messages to ITR. An exploit could allow the attacker to cause a vulnerable device to disable CEF forwarding and eventually drop traffic passing through.

  Conditions: Malformed messages can only be generated by a device that is already registered to a LISP system: a valid ETR or ALT.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

  CVE ID CVE-2014-3262 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at:
  http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3262

  Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCun75719

  Symptom: After a switchover, standby device crashes with traceback.

  Conditions: At present, this is observed only on advipservices images in mtrose branches.

  Workaround: There is no workaround.

- CSCun76733

  Symptom: BFD goes down and remains in Admindown state.

  Conditions: This symptom occurs after applying ACL chaining and flapping of the interface.

  Workaround: There is no workaround.

  More Info: An IPv4 BFD neighbor remains in admindown state on the PE. The ACE configured in ACL for BFD is matched and the receive counters on BFD neighbors are incremented but the BFD is still down.

  This issue occurs only after ACL chaining is applied.

- CSCun77010

  Symptom: A router may crash after or during the execution of the **show ipv6 ospf rib** command.

  Conditions: This symptom occurs when many routes or route paths are present in the OSPFv3 rib. The OSPFv3 rib is significantly recomputed during execution of commands.

  Workaround: Limit the use of the **show ipv6 ospf rib** command.

- CSCun78309

  Symptom: An Mroute entry on FHR is stuck in a registering state in MVPNv4. show ip mroute vrf <vpn-name> -->> shows the mroute entry in registering state

  Conditions: This symptom occurs when the source address of the encapsulation tunnel for PIM registers on the FHR is one of the interfaces that is not in the same VRF as the register tunnel itself.

  Workaround: There is no workaround.

  More Info: Output:

  ```
  PE2#show ip mroute vrf vpn1
  (215.12.1.2, 229.40.1.1), 00:00:29/00:02:30, flags: FT Incoming interface:
  GigabitEthernet3/3.1, RPF nbr 0.0.0.0, Registering Outgoing interface list: Tunnel764,
  Forward/Sparse, 00:00:29/00:03:00
  ```

- CSCun81749

  Symptom: MVPN traffic is unexpectedly terminated since the last-hop PIM router does not send an “SG Join” message on the MDT tunnel.

  Conditions: This symptom occurs when the same IP address is used for the MDT tunnel IP address on the last-hop PIM router and the source IP address of multicast traffic.

  Workaround: There is no workaround.

- CSCun86606

  Symptom: An IOSD crash occurs due to “Process = Virtual Exec”.

  Conditions: This symptom occurs when the **show ip cef internal** command and routing table is cleared in parallel.

  Workaround: When clearing the routing table (for example, clear ip ospf process) avoid running ip cef-related show commands in parallel.

- CSCun87557

  Symptom: A Cisco router crashes.

  Conditions: Set the VTY Service Set maximum response to a small number, for example, 10, and then send multiple commands separated by newline using the same write, for example, “show ver\nshow ver\n”.

  Workaround: Set Maximum response to a bigger number.

- CSCun88267

  Symptom: A Cisco router stops forwarding traffic when an SSLVPN session is established and stops responding.

  Conditions: This symptom occurs with SSLVPN and DTLS enabled. Cisco ISR-G2 platforms may experience a Queue Wedge.

  Workaround: Disable DTLS by configuring **no svc dtls** under policy group.

- CSCun92081

  Symptom: A traceback is seen while removing IPv6 unicast-routing configuration.

  Conditions: This symptom occurs when ISIS IPv4 is not enabled and ISIS is runs on IPv6 multitopology mode.

  Workaround: There is no workaround.

  More Info: The traceback is generated due a warning message that the adjacency database is not empty when ISIS is switching out of the IP mode.

- CSCun92095

  Symptom: IOS-XE running router may reload when unconfiguring BGP along with other removal operations in a scaled setup.

  Conditions: BGP is configured with 1Million+ nets and 4000 VRFs. Then the bgp instance is removed using “no router bgp <>”

  Workaround: Shut down the bgp neighbor sending big scale nets to remove the nets first from BGP and RIB. Then remove the BGP using “no router bgp <>”.

- CSCun99811

  Symptom: If a Cisco IOS box does not support Ethernet Y.1731 delay DMM version 1 (DMMv1), but supports DMM version 0 (DMM), it will not respond to a box trying to run a DMMv1 session.

  Conditions: This symptom occurs with an initiator box running DMMv1 to a Cisco IOS box that supports DMM but does not support DMMv1. Rather than responding as though it were receiving DMMs version 0, as is the required behavior, the session will be rejected.

  Workaround: All boxes that support DMMv1 will also support DMM version 0, so this can be used between two boxes instead. The normal DMM version 0 restrictions apply in this case.

- CSCuo09249

  Symptom: An xTR changes its RLOC, map-request packets from that new RLOC are dropped on the MS/MR due to policy violation, for example:

  ```
  *Apr 2 15:29:15 JST: LISP-0: AF IID 100 IPv4, Map resolver filtered incoming map
  request from 2400:A:A:9999:C267:AFFF:FE52:287 because it does not conform to the
  configured allowed-locator policy.
  ```

  Conditions: This symptom is observed when {ipv4|ipv6} map-resolver map-request validate source registered is configured on the MS/MR and the xTR RLOC is updated, for example, by DHCP when the {ipv4|ipv6}-interface configuration is used in the database-mapping configuration. Both the new and the old RLOC must have been valid.

  Workaround: Remove and re-add database-mapping configuration on xTR, possibly using EEM script on address change Remove “{ipv4|ipv6} map-resolver map-request validate source registered” configuration on MS/MR clear lisp site <name> on the MS.

- CSCuo11238

  Symptom: Router crashes when removing address-family from VRF definition, or when removing the VRF definition.

  Conditions: This symptom is observed when PIM is configured for the LISP interface associated with the VRF.

  Workaround: Unconfigure LISP for the VRF, or remove PIM configuration from the LISP interface associated with the VRF, before removing VRF configuration.

- CSCuo12245

  ```
  Symptom: The following error message is observed with traceback :
  OCE_PUNT_PROCESS-3-LABEL_CACHE_INVALID: inlabel pointer was NULL
  ```

  Conditions: Multicast traffic is label switched in the mpls P2MP tree and replicated at branch bud nodes along the P2MP tree. The error condition is observed at a bud node, where the replicated traffic is dropped with the error.

  Workaround: There is no workaround.

- CSCuo15799

  Symptom: Memory leaks are observed on the node.

  Conditions: This symptom occurs with flaps in the REP segment generating TCNs that are being sent into a different REP segment.

  Workaround: There is no workaround.

- CSCuo21431

  Symptom: NTLM may not work properly.

  Conditions: This symptom occurs when the LDAP server goes down and comes up.

  Workaround: Add a new server as a part of the AAA group server ldap adgroup.

- CSCuo26634

  Symptom: Crash is observed.

  Conditions: This symptom is observed with command “sh frr-manager client client-name <name> det” when the client with the specified name does not exist.

  Workaround: There is no workaround.

- CSCuo34395

  Symptom: BFD OSPF client does not react at interface events on a remote endpoint.

  Conditions: This symptom occurs under the following conditions:

  – BFD is enabled - OSPF is enabled

  – One of the devices where BFD is enabled is running Cisco IOS Release 15.3(3)M2

  Workaround: There is no workaround.

- CSCuo35867

  Symptom:

  1. CPOS-based PPP serial interface is UP/DOWN; but HDLC is UP/UP; loopback local for PPP is also UP/DOWN.
  2. From debug, the following output is seen:

  ```
  *Apr 16 20:46:50.330: AAA/ID(00100066): PPP allocated ....
  ```

```
*Apr 16 20:46:50.831: CCM: Failed to create session, session already exists
<<<<<<<<<<<<
*Apr 16 20:46:50.831: AAA/ID(NA): PPP allocating
*Apr 16 20:46:50.831: CCM GROUP:ERROR group not found with shdb 0
*Apr 16 20:46:50.831: AAA/ID(NA): propagate hw:Se1/0/0.1/1/6/1:0,0x42352E64
sw:Se1/0/0.1/1/6/1:0,0x42353C48 other:nil base:nil unit:0/1 slot:1 shelf:0 tty:nil
*Apr 16 20:46:50.831: aaa_uid_propogate grabbed_id = 1048678
*Apr 16 20:46:50.831: AAA/ID(00100066): PPP allocated
*Apr 16 20:46:52.847: Se1/0/0.1/1/6/1:0 PPP: Missed a Link-Up transition, starting PPP
<<<<<<<<<<<<
```

Conditions: This symptom occurs with PPP serial interface flapping.

Workaround: Chassis reload can temporarily make PPP interface UP/UP, but the problem will reoccur after a few days.

- CSCuo37123

  Symptom: High CPU is seen due to a PIM process after an SSO to standby RP. Huge PIM hello bursts can be seen from the router facing the issue. The severity and duration of high CPU can increase with the uptime of the active route processor.

  Conditions: This symptom occurs due to an SSO.

  Workaround: Disable PIM auto-rp “no ip pim auto-rp” if the CLI is available.

- CSCuo44562

  Symptom: The Cisco ASR 1000 Series Router crashes.

  Conditions: This symptom occurs with duty cycle testing with a lot of negative events.

  Workaround: There is no workaround.

- CSCuo47685

  Symptom: While evaluating the Cisco IOS Release 15.3(3)S3 early release image, the following error message was observed when using the CoPP configuration given below which matches based on precedence only as shown:

  ```
  class-map match-any coppclass-protocol match precedence 6 7

  "Match precedence in IPv4/IPv6 packets is not supported for this interface error:
  failed to install policy map CoPP"
  ```

  Upon occurrence, the entire CoPP policy map is not loaded. There is a concern that some field devices on the current release (Cisco IOS Release 15.0(1)S6) may have the above configuration and as such is prone to this error (CoPP installation failure during upgrade).

  Conditions: This symptom occurs while evaluating the Cisco IOS Release 15.3(3)S3 early release image.

  Workaround: There is no workaround.

- CSCuo48507

  Symptom: While testing ISSU from XE310<->XE311 with ikev2_dvti and GRE features, packet drops is observed after a switchover.

  Conditions: This symptom is observed during upgrade to Cisco IOS Release 3.11 and downgrade to Cisco IOS Release XE 3.10.

  Workaround: There is no workaround.

- CSCuo49923

  Symptom: Performing an ISSU upgrade with the CEF table consistency checkers enabled may result in a crash on “issu runversion”.

  Conditions: This symptom occurs with a Cisco Catalyst 6500 Series Switch running Cisco IOS Release 15.1(02)SY.

  Workaround: Turn off the CEF table consistency checkers before performing an ISSU upgrade.

- CSCuo51246

  Symptom: Traffic flow is not as expected when IPv6 policing is enabled on UUT.

  Conditions: This symptom is observed on loading the Cisco IOS Release 15.4(2.10)T image.

  Workaround: There is no workaround.

- CSCuo53561

  Symptom: BGP fails to apply an inbound route map on prefixes after a switch over.

  Conditions: This symptom occurs when NSR is enabled and RP switchover is performed twice.

  Workaround: Enable the knob “bgp sso route-refresh-enable” or manually do a soft refresh to get the routes back from NSR peers on the new active RP.

- CSCuo55180

  Symptom: A vulnerability in PPPoE processing code of Cisco IOS XE could allow an unauthenticated, adjacent attacker to cause a reload of the affected device and eventually a denial of service (DoS) condition.

  The vulnerability is due to improper processing of certain malformed PPPoE packets. An attacker could exploit this vulnerability by sending a malformed PPPoE packet to an IOS XE ASR1000 device, configured with PPPoE termination. An exploit could allow the attacker to cause a reload of the affected device and eventually a denial of service (DoS) condition.

  Conditions: Cisco ASR 1000 with IOS XE, configured for PPPoE termination.

  Workaround: There is no workaround.

  Further Problem Description: A device crashing, may print the following messages on the console:

```
%SYS-3-OVERRUN: Block overrun at 7F7FAE750B58 (red zone 44534C5F00000000)
%SYS-6-MTRACE: mallocfree: addr, pc ? %SYS-6-BLKINFO: Corrupted redzone blk
7F7FAE750B58, words 404, alloc 6374D1B, InUse, dealloc 10001, rfcnt 1 ?
%Software-forced reload
Exception to IOS Thread: Frame pointer 0x7F7FA0AB5AD8, PC = 0x7F80A8469565
UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps -Traceback=
1#c3a5522ccb47820b036322d6b7226e1c c:7F80A8438000+31565
Fastpath Thread backtrace: -Traceback= 1#c3a5522ccb47820b036322d6b7226e1c
c:7F80A8438000+BDDD2
Auxiliary Thread backtrace: -Traceback= 1#c3a5522ccb47820b036322d6b7226e1c
pthread:7F80A3697000+A7C9
```

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2014-3284 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at:
  http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3284

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuo56173

  Symptom: When PW's remote peer is ALU, it takes 5 to 10 minutes for the PWs to come up.

  Conditions: This symptom occurs when Provision PW is done first on the ALU and then on the Cisco router.

  Workaround: Provision PW on the Cisco router first.

- CSCuo56871

  Symptom: A Cisco ASR 1001 router running Cisco IOS Release 15.2(4)S4 acting as a route server crashes when **clear bgp ipv4 unicast *** is executed.

  Conditions: This symptom occurs when a router is configured as as route server and a command executed in an IPv4 table is reset via **clear bgp ipv4 unicast ***.

  Workaround: Do not execute command **clear bgp ipv4 unicast ***. Instead, one could use the **clear ip bgp *** to hard reset all the BGP tables.

- CSCuo60344

  Symptom: With loss of traffic on primary flow in MoFRR, the secondary flow may not be treated as primary since it is random and the new flow may become the primary.

  Conditions: This symptom occurs in ECMP or TI flow based MoFRR and when there is a loss of primary flow.

  Workaround: There is no workaround.

- CSCuo66491

  Symptom: While using PfR, traffic classes oscillate from controlled to default to uncontrolled when probe creation fails for alternate external interfaces (due to lack of parent route).

  Conditions: This symptom does not occur under specific conditions.

  Workaround: Configure monitor mode active or monitor mode both instead of monitor mode fast.

- CSCuo72301

  Symptom: Crash occurs when IKEv2 attempts to clean up its contexts when it times-out waiting for received Certificate to be Validated by PKI component.

  Conditions: Authentication with certificates and PKI component's response to certificate validation is delayed.

  Workaround: There is no workaround.

- CSCuo72961

  Symptom: An error message is logged in during QoS configuration during an FPM test.

  Conditions: This symptom occurs due to a policy with FPM class.

  Workaround: There is no workaround.

- CSCuo75681

  Symptom: The RP crashes due to "%SYS-2-CHUNKBADMAGIC" in checkheaps.

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

- CSCuo83510

  Symptoms: A stack overflow and boot loop can occur when configuring OSPFv3 for IPv6 using a non-broadcast network type on IOS XE

  Conditions: SVI or Layer-3 Interface using the ospf non-broadcast network type.

  Workaround: Remove the non-broadcast network configuration.

  Further Problem Description: This issue was found during a security audit of the product.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuo83554

  Symptom: A vulnerability in the Autonomic Network Discovery Packets of Cisco IOS XE could allow an unauthenticated, adjacent attacker to receive arbitrary data from other traffic passing through the device

  The vulnerability is due to uninitialized memory used in packet creation. An attacker could exploit this vulnerability by capturing packets on the segment.

  Conditions: Device configured with default configuration.

  Workaround: Not applicable or available.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.3/3:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:U/RC:C

  No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuo84660

  Symptom: The following error message is seen:

  ```
  *May 15 20:22:43.699: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC=
  :10000000+D90018 -Traceback= 1#10ebf8a777fd9b28d42b106d039edefc :10000000+78F240
  :10000000+78F5F0 :10000000+7B9268 :10000000+7548448 :10000000+D90018 :10000000+D8A6D0
  :10000000+D9B2C4 :10000000+DA3BEC :10000000+6A6DC4 :10000000+6ADDB0 :10000000+49DBB2C
  :10000000+6BF11C
  ```

  Conditions: This symptom occurs while updating the running configuration using any type of remote file transfer (via SNMP or copy command). When the source IP resolves to a DNS hostname longer than 63 bytes, an error message will be seen. There is no impact to the system. The running configuration will update as expected.

  Workaround: Copy the file to a local storage first and then copy it from the local storage to the running configuration.

- CSCuo86953

  Symptom: A Cisco router or switch may crash while issuing the **show logging** command.

Conditions: This symptom occurs while issuing the **show logging** command. Let the output of the **show logging** command remain at the more prompt in the trap logging session. While changing the **logging host** command in a different session, resume the output of the **show logging** command. There is a chance that both actions at the same time will make the device crash.

Workaround: Do not make changes to the **logging host** command while the output of the **show logging** command is still outstanding.

- CSCuo88282

  Symptom: A Cisco ASR router crashes.

  Conditions: This symptom occurs under the following conditions:

  Configure a DHCP database as follows: ip dhcp database tftp://192.168.50.100/dhcp write-delay 60 timeout 30 The router is unable to write the database as TFTP is not installed on 192.168.50.100 or TFTP IPis not reachable (both scenarios leading to crash). After a few seconds the router gets crashed.

  Workaround: There is no workaround.

- CSCuo91745

  Symptom: The black hole should not drop TC when TC is learnt at the beginning.

  Conditions: This symptom occurs when the black hole is added in the class as follows: class http sequence 10 match application http policy custom priority 1 one-way-delay threshold 100 path-preference SP1 fallback blackhole

  The HTTP traffic is added. When the TC is learning, it is uncontrolled and hence during this time traffic will be dropped. The dropping will start at the TC learnt and end at the TC controlled. The duration will be a minimum of 30s.

  Workaround: There is no workaround.

- CSCuo93299

  Symptom: ZTB does not work.

  Conditions: This symptom occurs when the image is loaded and left without aborting the setup dialogue box.

  Workaround: This issue has been fixed.

- CSCuo93711

  Symptom: RSVP HA Services leaks memory on the standby RP. Standby RP eventually hits the “out of memory” condition and will reload. There is no traffic impact as the active RP is not affected.

  Conditions: This symptom occurs when the **mpls traffic-eng nsr** command is configured.

  Workaround: There is no workaround.

  More Info: The leak is specific to MPLS-TE tunnel tails. A small memory block is leaked whenever a tunnel tail is setup or torn.

- CSCuo95313

  Symptom: Duplicate cookies are observed in every access request.

  Conditions: This symptom occurs when multilogon or logoff is performed on the same session.

  Workaround: Tear down the session during the logoff event. Do not configure any delay on the account logoff event.

- CSCuo96504

  Symptom: A FlexVPN client router may report alignment errors and experience high cpu utilization in IKEv2 FlexVPN process.

  Conditions: The tunnel interface in use with the FlexVPN client configuration must flap while the client is processing an IKEv2 redirect. The high cpu utilization is seen only if the client is configured to auto connect.

  Workaround: Remove and reconfigure the IKEv2 client configuration block.

- CSCuo97889

  Symptom: IPv4 and IPv6 traffic will be dropped after performing an SSO.

  Conditions: This symptom occurs when you perform an SSO with ISIS as NSR configured, and MPLS-TE as GR configured.

  Workaround: Change ISIS to non-NSR.

- CSCuo98907

  Symptom: Platform-specific images do not build.

  Conditions: This symptom occurs when any platform-specific image is built.

  Workaround: This issue is fixed.

- CSCup00882

  Symptom: A router running Cisco IOS experiences an unexpected reload after removing OSPF IPFRR or OSPF Remote LFA from the configuration.

  Conditions: This symptom occurs when the router was configured for OSPF IPFRR and, possibly, OSPF Remote LFA and IPFRR and (or) rLFA configuration commands are being removed at the same time when IPFRR SPF is running on the router.

  Workaround: There is no workaround.

  More Info: This symptom occurs if IPFRR SPF is running at the time the configuration is being removed.

- CSCup01885

  Symptom: A crash is observed due to a corrupted stack in AAA. This issue was observed on a Cisco ASR 1000 router when an authentication request was sent from IKE (crypto) with a password expiry feature configured.

  Conditions: The symptom is seen with the password expiry feature. The configuration needed is:

  ```
  aaa authentication login <method> passwd-expiry group <radius/tacacs>
  ```

  Workaround: Remove the configuration.

  More Info: With “aaa authentication login userauthen passwd-expiry group radius” configured, over a period of time, there is AAA stack corruption because of a value read from a wrong offset in the memory. It is not specific to any platform.

- CSCup08772

  Symptom: A Cisco device hangs.

  Conditions: This symptom occurs after a save and reload with intent configured.

  Workaround: There is no workaround.

  More Info:

  1. Configure registrar.

2. Configure intent.
3. Save and reload the device.

- CSCup09007

  Symptom: When a CEM interface is configured, the router crashes when it is unconfigured without logging out of the CEM configuration mode.

  Conditions: This symptom occurs when a CEM interface is configured and unconfigured.

  Workaround: Exit from the submode before performing **no xconnect**.

- CSCup10447

  Symptom: When an Any Transport over MPLS (AToM) xconnect is configured on a dual-RP system, memory leaks may be observed on the standby RP.

```
router-stby#sh memory debug leaks chunks Adding blocks for GD...
kernel memory
Address Size Alloc_pc PID Alloc-Proc Name
Chunk Elements:
AllocPC Address Size Parent Name
lsmpi_io memory
Address Size Alloc_pc PID Alloc-Proc Name
Chunk Elements:
AllocPC Address Size Parent Name
Processor memory
Address Size Alloc_pc PID Alloc-Proc Name
Chunk Elements:
AllocPC Address Size Parent Name NA 3DDDFCB4 180 3DDD06C0 (AToM VC binding) NA
3DDDFE24 180 3DDD06C0 (AToM VC binding) NA 3DDDFF94 180 3DDD06C0 (AToM VC binding) NA
3DDE0104 180 3DDD06C0 (AToM VC binding) NA 3DDE0274 180 3DDD06C0 (AToM VC binding) NA
3DDE03E4 180 3DDD06C0 (AToM VC binding) NA 3DDE0554 180 3DDD06C0 (AToM VC binding)
```

  Conditions: This symptom is observed when a label advertisement is received from the peer and checkpointed to the standby RP.

  Workaround: There is no workaround.

- CSCup21524

  Symptom: A crash is observed with the following error messages:

```
Exception to Fastpath Thread: Frame pointer 0x7FEA1735D570, PC = 0x7FEB1F732559
-Traceback= 1#bb8f9a461a7850b52eefb2d5dc713d87 c:7FEB1F701000+31559
c:7FEB1F701000+32A09 :400000+442C515 :400000+4430C38 iosd_unix:7FEB1FED3000+1B0B6
:400000+6D46665 :400000+7AD419 :400000+2534AFB :400000+4422F8B :400000+70D1E1F
:400000+7117396 :400000+71154E6 :400000+6D6801F :400000+6D6787F :400000+4417B48
:400000+441AE07
IOS Thread backtrace: UNIX-EXT-SIGNAL: User defined signal 2(12), Process = SSM
connection manager -Traceback= 1#bb8f9a461a7850b52eefb2d5dc713d87
pthread:7FEB1D279000+83BF
Auxiliary Thread backtrace: -Traceback= 1#bb8f9a461a7850b52eefb2d5dc713d87
pthread:7FEB1D279000+A7C9
```

  Conditions: This symptom occurs after a switchover from the active RP to the standby RP and the device has 1000 PPPoA sessions. Call Admission Control (CAC) is also configured.

  Workaround: Remove CAC configurations. For example:

  call admission new-model call admission limit 1000 call admission cpu-limit 80

- CSCup23792

  Symptom: A loss of service-group configuration under a subinterface is observed.

Conditions: This symptom occurs only when the router is reloaded. It is not seen with a particular LC reload where the interface exists.

Workaround: There is no workaround.

- CSCup33759

  Symptom: ISIS IPv6 distribute-list filters of the form:

  router isis address-family ipv6 distribute-list prefix-list {name} in {interface}

  should be removed from the configuration when the specified interface is deleted or is no longer enabled for IPv6. In some cases this is not happening, which can cause errors when a saved configuration is used during a subsequent reboot.

  On systems with a redundant RP, configuration sync will fail because the distribute-list command will be rejected by the standby RP.

  Conditions: This symptom is observed when using ISIS to route IPv6 traffic.

  Workaround: Ensure that IPv6 is enabled on any interfaces referenced by ISIS IPv6 distribute-list commands. This can be accomplished either by configuring one or more IPv6 addresses on the interface, or by using the command “ipv6 enable”.

- CSCup39674

  Symptom: A traceback is observed consistently during a cleanup.

  Conditions: This symptom occurs when MPLS-TP tunnels are configured and unconfigured.

  Workaround: There is no workaround.

- CSCup47507

  Symptom: In Cisco IOS Release 15.4(3)S or Cisco IOS XE Release 3.13S, the ISIS **summary-address** and **summary-prefix** commands are not synchronized to the standby RP.

  Conditions: The symptom is seen on a router with redundant RPs.

  Workaround: There is no workaround.

- CSCup49636

  Symptom: Estimated Channel Egress Bandwidth gets accounted incorrectly with fast-monitor enabled per DSCP.

  ```
  For example, with monitor-interval as 1s, all TCs on SP1, Total TC BW: 18Mbps, then
  Estimated Channel BW: 540Mbps;
  ```

  Conditions: This symptom occurs when fast-monitor gets enabled for a specific DSCP channel.

  Workaround: There is no workaround.