Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10S

This chapter provides information about the caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10S.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.10S

This section contains the following topics:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.10S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.10S.

Caveat ID Number	Description
CSCve54313	Crash in ALPS SNMP code
CSCvc42729	Autonomic Networking Infrastructure Adjacency Discovery DoS Vulnerability
CSCve57697	Crash in Bstun SNMP code
CSCvd36388	link-number argument disappears in configured channel-group
CSCve22290	Storm Control Suppress Counting but No log Trap
CSCvc19100	Multicast lose after port-channel flapping on 7600
CSCve66601	Crash in CISCO-SLB-EXT-MIB code

Caveat ID Number	Description
CSCuw77959	1801M - %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCvc12306	Limit ike-init queue to improve performance in scaled scenarios
CSCvb94392	Cisco IOS and IOS XE System Software SNMP Subsystem Denial of Service Vulnerability
CSCvb66239	Willr noL3 tunnel MTU is not signaled properly for locally-originated packets
CSCva17339	LDP session stuck in established with no TCP connection
CSCuz95908	Memory leak due to path query with Null outgoing interface
CSCva38391	CVE-2016-1550: NTP security against buffer comparison timing attacks
CSCve66658	Crash in TN3270E-RT-MIB code

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.9S

This section contains the following topics:

- Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.8S, page 587

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.9S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.9S.

Caveat ID Number	Description
CSCvb29204	BenignCertain on IOS and IOS-XE
CSCuv87976	CLI Knob for handling Leap second Add/delee ignore/ handle
CSCvb19326	NTP leap second failure to insert after leap second occurs
CSCuv71273	ASR 1000 Series Aggregation Services Routers Data-Plane Processing Denial of Service Vulnerability

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.8S

This section contains the following topics:

- Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.8S, page 587

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.8S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.8S.

Caveat ID Number	Description
CSCuy03054	ASR1K IOSd may crash in BGP Accepter process due to segmentation fault

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.8S

This section documents the open issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.8S.

Caveat ID Number	Description
CSCus46259	ASR1k (ISG Radius-Proxy): Memory Leak after excessive client roaming

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.7S

This section contains the following topics:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.7S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.7S.

Identifier	Description
CSCuv52648	ESP memory leak under cpp_cp_svr due to BFD feature
CSCuv61799	ASR1000 power supplies require SW debounce of PWR_OK signal

Identifier	Description
CSCux57066	ASR1K : Lawful Intercept not working as expected for IPv6 traffic
CSCut77070	SPA-1xCHOC12/DS0 not supporting Framed E1 connections.
CSCut03205	SPA modules on ASR1K show "missing" under show platform output
CSCut33723	error counters getting incremented on ports which are down
CSCuv30635	RSP1: standby rsp led not glowing post ISSU
CSCuv09066	Incorrect P-bit for CPU originated packets once EoMPLS VC on
CSCuu75177	BGP crash if community-list name is bigger then 80 characters
CSCuu85298	FIB/LFIB inconcistency after BGP flap
CSCuv07111	IOS and IOS-XE devices changing the next-hop on BGP route with own IP
CSCux24141	MET mis-programming results in unwanted multicast after switchover
CSCuj68109	7600-SIP-400/12.2(33)SRE4 Egress ESF Engine: ME Breakpoint Error
CSCur96372	l2protocol forward feature is missing under SIP400
CSCux86685	Put an altenate fix for CSCuw93863 (SIP400 crash at hqf_priority_remove)
CSCuw93863	SIP-400 crash after hqf_priority_remove
CSCuv80858	byte counters for a port-channel show interface is inaccurate
CSCut42645	input queue wedged on a SSLVPN enabled router
CSCuq36627	WAAS Express:Failed to create SSL session. (no available resources)
CSCus57583	ASR 1K BGP Process Crash Due to EIGRP Route Redistribution
CSCus25205	Traceback@eigrp_process_dying during unconfiguration
CSCup52101	EnergyWise Denial of Service vulnerabilty
CSCuu18405	NTP leap add is failed using XE3.12 on ISR4400 platform
CSCus37452	show QFP memory command rejects some valid addresses
CSCuv17777	4451 cannot configure NFAS backup using card NIM-8CE1T1-PRI
CSCut55223	ISR4331/ASR1k : Crash at mcprp_dpidx_for_swidb
CSCur72779	XE314 : B2B NAT : Stale NAT translations observed on Active rtr
CSCuv93130	Cisco IOS-XE 3S platforms Series Root Shell License Bypass Vulnerability
CSCuq90747	IKEV2 Virtual-Access Interface goes down when using HSRP VIP
CSCuu45094	Crash after SA requests a rekey
CSCus92857	Crypto Stateless redundancy causing "IPSEC install failed" after preempt
CSCuv08835	IPSEC key engine process leaks /w dynamic crypto map in scaled scenario
CSCuv51788	GM Router failed to register after reload.
CSCuu52012	Router crash when we execute show run | format command
CSCuw08236	Partial Denial Of Service Vulnerability in IOS IKEv1 w/ DPD enabled
CSCuv26780	Memory leak when qos pre-classify is configured with Crypto
CSCuw74752	cpu hog and crash in isis_ip_xlfa_pq_ipaddr_usable
CSCuv81298	LFA SPF causes cpuhog and crash in scaled test with 400 nodes
CSCuv29418	Router is continuously switching between active and standby EoMPLS PW

Identifier	Description
CSCut58291	Crash in L4F (tup_lookup_func) with CWS configured on the router
CSCuv57459	ASR1K Kernel crash at pidns_get() - part 2
CSCtz61014	f Linux kernel NTP leap second handling could cause deadlock
CSCuv46139	DHCP relay does not remove Option82 in Offer forwarded to client
CSCuv05123	c3560e/v151_sy_throttle platform doesn't store NTP drift values properly
CSCuw85826	Evaluation of Cisco IOS and IOS-XEl for NTP_October_2015
CSCuv23475	CPUHOG and crash on "no network 0.0.0.0" with vnet configuration on intf
CSCuu55332	OSPF NSR: Standby Crash on no shut of interface with ip address dhcp
CSCus77875	List Headers leak verified cert chain Held CCSIP_TLS_SOCKET & Chunk Mgr
CSCuw79412	%SYS-6-STACKLOW: Stack for process PPP SIP running low, 0/6000
CSCuv36911	ASR1K active CGN ESP200 may crash when the CGN standby realoded
CSCus09942	ASR Crash on ipv4_nat_ha_upd_to
CSCuv02537	ASR1K ESP200 reload in a B2B CGN NAT scenario with PAP+BPA
CSCuv25212	ucode crashes with Fair Queue and FNF export is configured
CSCuv21984	Fair-queue queue-limit force adjust after change queue-limit.
CSCtn75051	%SYS-3-TIMERNEG: Cannot start timer with negative offset
CSCuu82607	Evaluation of all for OpenSSL June 2015
CSCut46130	MARCH 2015 OpenSSL Vulnerabilities
CSCuq25323	DLSW peers fail to connect when other DLSw peer sends FIN instead of RST
CSCuu71299	MPLS LDP flap with %TCP-6-BADAUTH: No MD5 digest
CSCuw26259	SIP SUBSCRIBE msg is responding back with 503 Service Unavailable

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.7S

This section documents the open issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.7S.

Identifier	Description
CSCuu91954	Fix potential crash in cable lawful intercept
CSCux59115	ASR1002-X Crash with dpidb_tableid_params_initialize
CSCuy20481	Crash due to stale pointer after removing vrf command export AF map
CSCun86606	XE 3.10 IOSD crashed when ip cef show cmd and ospf cleared in parallel
CSCuy18665	CSR crashes on installing bb_1K license
CSCuu28199	[Amur-MR3]IOSD crash reported@spi_iosd_ipc_process_inbound_mts_msg
CSCuw99554	ASR crashes on removing the sub-interface on HSRP active router
CSCuo72301	IKEv2 Crash in free_msg_context

Identifier	Description
CSCuv94186	SNMPWALK crash at ipsmIPSec_policyOfTunnel
CSCuv59898	Kernel Watchdog crash at ktime_get
CSCuy08412	ASR1K fman_fp_image crash with ACL changes
CSCuq24971	ASR1k ucode crash with pa_get_state on using aggregate port-channel
CSCuu75584	cpp ucode crash related to Nat config changes
CSCuv74171	crash on command "show snmp view"
CSCtl81133	CUBE crashes if SIP TLS connection is not successful
CSCut97997	ISR 4K Crashes Due to "CCSIP_TLS_SOCKET" Process

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.6S

This section contains the following topics:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.6S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.6S.

Identifier	Description
CSCus32530	ASR1K ESP crash in internal L4R removal feature routine
CSCut68598	ASR1k BFD randomly down at NAT configured interface
CSCuq75633	BFD down sent from ASR5500 is not recognised by 1K, still sending UP
CSCur53837	ASR1k: SIP can't be re-enabled with 'no hw-module slot X shutdown'
CSCus62358	ASR1k: MAC based filter does not work with EPC
CSCuu14809	Byte counters display incorrect value for multicast traffic over sub-int
CSCus51697	BDI not working correctly on ipbase license
CSCur24793	l2protocol forward not work for STP, LLDP, PPTPv2 and E-LMI in EVC
CSCuu85007	split-horizon group communication failure
CSCut21885	fman_fp_image and cpp_cp_svr memory leak - QFP PfR MP Prefix H...
CSCuu12008	rework CSCut21885: chunk_destroy memory leak.
CSCus71003	ASR1002-X - Kernel crash - general protection fault
CSCuu72025	Multiple ESP Core on ASR1006

Identifier	Description
CSCus86476	ASR1K NAT ALG ucode crash @ipv4_nat_destroy_addrport_bind
CSCut63804	CPP crashed when device in pair became active
CSCur60943	l2bd_bfib_timer_timeout_handler Crash due to problem in IOS internals
CSCut74937	ASR1K PBR VRF Selection not working when source is local router
CSCut16173	"show interface" bits/sec and packets/sec counters stuck to non-zero
CSCus51303	Combi card ASR1000-2T+20X1GE Standby RP doesn't accept configuration
CSCus28745	POS FRR issue with traffic loss around 1 sec instead of 50ms
CSCut34273	ASR1K, "unknown" process leak under cpp_cp_svr
CSCus65095	SSTE: QoS Pre-classify was broken
CSCus86256	uCode crash when MPLS packet received on LAN side of AppNav intercept
CSCut41061	ESP crash with monitor capture and debug platform-trace
CSCur08811	Acoustic Shock Prevention (ASP) statistics not incrementing
CSCur96943	CCSIP_SPI_CONTROL leak in sippmh_parse_record_route
CSCus54955	Crash occurs while handling 3xx w/o user part and "no notify redirect"
CSCut42351	CTS500-32: Video Issues after Hold/Resume
CSCus16065	CUBE - dial-peer bind command disappears
CSCur64006	CUBE crash in local_xcode_rtp_xmit similar to CSCui55556
CSCus73488	CUBE doesn't send H245 CLC for outstanding OLC if TCS is received
CSCur12550	Cube hangs sip sessions when redirect ip2ip is configured
CSCut80576	CUBE LTI transcoder sessions getting stuck.
CSCuq53018	CUBE PhoneProxy: ASR router crash with tftp-server domain name config
CSCuq31542	CUBE sending T38 caps in mid-call INVITE for HOLD
CSCut70261	CUBE SIP media forking using Voice Print server causes unexpected reboot
CSCuu00050	CUBE with SRTP fallback is dropping SRTP RTP/SAVP from the 200 OK SDP
CSCus80096	FP Crashed for SRTP-RTP audio call load tests
CSCut99190	Memory Leak due to CCSIP_SPI_CONTROL due to sipSPIUpdateCallEntry
CSCuu44302	Memory leak under process RECMSPAPP with PC voip_rtp_create_fork_object
CSCur54389	SRTP-RTP Call with HOLD/RESUME disconnected
CSCus13757	TLS socket read and hung DSP issues with Alert followed by FIN
CSCuq37551	white noise on SRTP-RTP call when placed on hold and resumed & DSP leak
CSCur35618	[XE 3.15] FP Crashed for SRTP Video Call + DSP
CSCuu54392	Different Tunnel Protection with shared profile cannot be used
CSCus96078	duplicated ipsec sa does not fully delete isakmp sa
CSCup97873	IPSec datapath should not print debug messages without debugs enabled
CSCur29861	Traceback seen on c2900 platform for ike_keepalives
CSCuq40081	Crash on primary KS with suiteB configs
CSCuq81305	GET COOP-KS: TEK not synced between KSs before rekey

Identifier	Description
CSCuu28193	GETVPN: "GKM KS PROCESS" stuck on Key Server in COOP
CSCus35789	GETVPN: Post Registration Policy Update Issue for Downloadable ACL on GM
CSCut32445	Crash - IPSec/ISAKMP Timer driven crash involvement suspected
CSCtr15891	DPD behaviour change - to send per IKE
CSCus30128	RRI dynamic L2L after client change ip address Ipsec rekey lost routes
CSCuq87353	RRI static route not removed after the peer is removed from CMAP
CSCur27771	FlexVPN tunnel mode gre ipv6 doesn't work
CSCun57148	High CPU in FNF Cache Ager P
CSCus92575	[XE15-ST]: Memory leak seen @ccsip_get_recording_participant_header
CSCut64644	ASR1K goes to crash after TCAM messages appearing
CSCut41684	ASR 1K crash due to CCM_ACK interupt
CSCus85852	CPP DRV: Disable IIC Interrupts (Revert CSCuq05197)
CSCut03813	ASR1K ucode crash seen at mpls_icmp_create
CSCut83522	Ultra CRPG simulation intermittently broken by CSCut03813
CSCut72639	ASR1k CPP crash with IP Options
CSCur90494	sbs_entry allocation failure causes ESP crash
CSCut56117	ASR NAT timeouted out sessions not cleared.
CSCus00801	ASR1002-X cpp crash while processing ICMP Unreachable
CSCus69026	ASR1K B2B CGN NAT ASR1K lost sync in standby IP NAT allocated addresses
CSCus66974	ASR1K QFP reload in a B2B CGN NAT scenario with PAP+BPA
CSCur31425	ASRNAT: PPTP ALG: Incorrect UNNAT of Peer-Call-ID in Outgoing-Call-Reply
CSCur67171	Dial-peer stats poll cause SNMP high CPU if 500+ dial-peers configured
CSCur67691	Continous reload issues seen on ASR1K B2B Redundancy
CSCur21757	Memory leak *Dead* = AFW_application_process and QSIG-rose
CSCue79042	Unexpected Reload: Exception to CPU vector D - AFW_application_process
CSCus66811	Bus error crash on 0D0D0D1D
CSCut18365	Tracebacks found @ moh_multicast_recv_input
CSCus89791	g722-64 codec crash during dial tone with country code
CSCuq88060	"no transport udp" is getting removed from "sip-ua" after reloading ASR
CSCut13290	"P-Associated-URI" handling on CUBE should follow rfc3455
CSCur19344	Cannot start timer on "CCSIP_SPI_CONTROL" process
CSCuq54871	Crash seen when forwarding of SIP MWI as qsig MWI. 15.2M is NOT affected
CSCup83118	KPML dialing fails for CUCM Lineside SIP phones
CSCut88299	MMoH fails in Directed Call Park Call Flow
CSCur31540	MMOH Over SIP CUBE does not work when there is an H323 call on hold
CSCus67448	Router crashing on command "show sip call dtmf-relay sip-info"
CSCum30814	SIP GW sends incorrect SIP INVITE: --uniqueBoundary not closed properly

Identifier	Description
CSCur94272	sip_get_sipspi_message memory leak in CCSIP_SPI_CONTROL
CSCus75537	add the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite support for vxml httpc
CSCut61279	crash with AFW functions during call clearing
CSCus48584	POODLE ptotocol fix:IOS : Voice-XML HTTPS client (Use TLS)
CSCut66144	VXML GW fails to handoff call to VXML Application on second VRU leg
CSCus00058	Invalid ip address is accepted as mta send server

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.6S

This section documents the open issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.6S.

Identifier	Description
CSCut38445	PPP negotiation fails when MRRU is 9217 or bigger
CSCuu56904	ASR1K cannot output messages about stby harddisk/bootflash failure
CSCug63576	Path traversal vulnerability with fpd: filesystem
CSCut66894	evsi session fail to come up using multicast on all the virtual-access
CSCur46422	ASR1k - Uncomment the POST for 3DES, AES
CSCty26186	Enhancement request to capture watchdog reset on asr1k
CSCuu91954	Fix potential crash in cable lawful intercept
CSCus11391	ASR1k/3.10.2 : MLPPP packets incorrectly marked out of order and dropped
CSCur44103	ASR1k: Port leak while using NAT with interface mappings
CSCup57389	Traffic drops while testing VRF Lite coexistance with SP NAT for LNS
CSCut09922	cpp_cp traceback from qos cpp_qm_rm_tree_obj_add
CSCur48133	ATM 3xOC3 SPA failed to program with IFCFG_CMD_TIMEOUT error
CSCut77070	SPA-1xCHOC12/DS0 not supporting Framed E1 connections.
CSCut03205	SPA modules on ASR1002-X show "missing" under show platform output
CSCud67560	Rotate Command for Trace files does not rotate PMAN Logs on FRU
CSCup25858	ASR1K NAT: PAP limit defaulting to incorrect value when BPA set-size set
CSCuo59226	pactrac: incorrect hexdump display with terminating 3-byte boundary
CSCuq24354	GETVPN KS rekeys without pol changes may cause IOS XE GMs to re-register
CSCuf35287	Reverse route injection with gateway option failed
CSCuv14856	WATCHDOG timeout crash during IPSEC phase 2
CSCur88256	GETVPN Dataplane counters show negative values due to counter overflow
CSCur88233	Mismatch in primary and secondary keyserver's GM database
CSCul78096	"no route set interface" lost after reload in the default author policy

Identifier	Description
CSCun20781	Crash at IKEv2 due to an invalid configuration
CSCuo72301	IKEv2 Crash in free_msg_context
CSCur89554	Unable to clear the 'conn-id' because of out of range value.
CSCut99067	ESP crashed desc:CPP Client process failed: cpp_cp
CSCuu14810	LNS Setup Rate takes over one hour for 58K sessions (copy of CSCut20591)
CSCup81323	additoinal support for filter combination(s) on IOS-XE
CSCuq24971	ASR1k ucode crash with pa_get_state on using aggregate port-channel
CSCur84475	XE315, fw/hsl: ipv4 template is used for ipv6 session
CSCuv02537	ASR1K ESP200 reload in a B2B CGN NAT scenario with PAP+BPA
CSCuo40409	B2B NAT : TB @lst_gpm_addr_handler after inside intf flap on Active
CSCuu75584	cpp ucode crash related to Nat config changes
CSCun97477	ASR CUBE-ENT not sending RTP to endpt in ACK w/SDP: DO-DO
CSCtl81133	CUBE crashes if SIP TLS connection is not successful
CSCus57110	CUBE not forwarding the pre connnect announcement
CSCut97997	ISR 4K Crashes Due to "CCSIP_TLS_SOCKET" Process

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.5S

This section contains the following topics:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.5S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.5S.

Identifier	Description
CSCuq43357	ASR1K - Y1731 Frame Delay Measurement broken
CSCuq49527	ASR1k IOSD crash while configuring IPSLA with Y1731
CSCur07193	ELC-40:Popinac Crash after CSCuq82536 commit when configured Portchannel
CSCun32287	SW: ASR1002-X ifHCInOctets can decrease before wrapping around.
CSCur00762	ASR1k - incorrect traffic classification after HW TCAM is exhausted
CSCuq85115	ASR1K enable "ip cef accounting non-recursive” cause fman_rp crash

Identifier	Description
CSCur09918	ASR1K: RP2 kernel crash
CSCuq88560	ASR CPP crashes due to stuck thread interrupt
CSCur09725	ASR1K crash when loading Nbar pp version 10.0
CSCuq66758	ASR1k - CPP ucode crashes on configuring OTV
CSCur18685	QOS SG: Lev1 shape rate is de-actived after dynamic config on the fly
CSCur35347	ASR1002-X "SBC File Daemon Crash" / High CPU During Harddisk Log Delete
CSCun62047	ASR1k: Cleanup tracebacks seen while testing CEoP SPA-24CHT1-CE-ATM
CSCur46656	3.10.4S-UNIX-EXT-SIGNAL: Segmentation fault(11), Process = IOSD ipc task
CSCuq91599	ASR1k wccp pending-ack in fman-wccp caused standby-fp reload every 1hr
CSCuq15237	GM hangs while applying show crypto gdoi command
CSCuq51959	Observed Memory Leak in L2 REP with Interface FLAP Scenario
CSCuq68961	Update IC2M test harness to support AES KW algorithm validation testing
CSCuq96691	Utah crash during ezconfig installation.
CSCuq63167	XE313 : PAP address allocation issue - retry with mods to gaddr_unlock
CSCuq80765	500 internal server error Occurring while update.
CSCur12414	ASR ANAT Hold-Resume IPv4-IPv6 one way audio
CSCuq76439	Cube adds a=inactive in SDP during resume operation (RTP-SRTP call)
CSCuq05240	CUBE consumes Reinvite when m=audio line has more than 1 codec
CSCur59627	CUBE has stuck/stale TCP socket opened by SIP TLS application
CSCuq42803	Less number of rtp connections obtained then expected
CSCup58405	router crash at __be_sipAppProbeHeaderPresence
CSCuq32792	Unexpected reload of CUBE with AQM+HA involved
CSCuq15567	Crash with %SYS-3-OVERRUN with crypto_ipsec_clear_peer_sas
CSCui58112	Fail/close Traffic pass clear when after GM lost connection to KS
CSCuo95771	IPSec SA are deleted incorrectly by background process
CSCur29582	IPSEC-VPN: removal of "crypto-map" kills BFD session forever
CSCup01088	CPUHOG and crash on 'clear dmvpn session' with large NHRP cache
CSCun13772	NHRP: CPUHOGs seen when many child entries expire simultaneously
CSCur65486	GETVPN: Fail to delete GMs on sec-KS after 3 scheduled rekeys failure
CSCuq17828	ASR: Radius Accounting fails when using EDCSA certs
CSCuh58880	ipsec:route-set=prefix av-pair is not pushed to the anyconnect client
CSCug74947	ISAKMP is still UP after shutdown remote site physical interface
CSCun72450	IPv6 GETVPN traffic dropped after un-configure then re-configure VRF
CSCup09848	[Mang] Traceback seen during call connect
CSCur07571	Processor memory leak with MRCP_Client at cc_api_get_call_active_entry
CSCum45864	MTP signatures failed due to addition on new custom MTP fields
CSCui61103	DMVPN Phase 3 NHRP refresh clears rib/nho flag and RIB not updated

Identifier	Description
CSCui68274	Nodes skipped in multicast replication when NHS recovery is used
CSCuq54655	ASR1K: Ucode@PAR1_CSR32_PAR1_ERR_LEAF_INT__INT_PAR1_STEM_CB_SEL_INV_ERR
CSCuq97925	cpp_cdm: CPP crashed after oir CLC
CSCur46638	XE3.10+ Flapping ATM i/f or VC may cause small memory leak
CSCul79546	GEC pactrac: show fia-traced packet has unexpected unformatted output
CSCuh97072	ASR NAT causes punted traffic to be incorrectly handled
CSCur33915	ASR1000 QFP crash due to stuck thread
CSCur17355	ASR Crashes due to SRTP when Fax T38 Protocol Configured
CSCum61559	SYS-2-INTSCHED 'may_suspend' at level 6 -Process= "Per-minute Jobs"
CSCuq99173	Conditions experienced parsing H225 pkt may cause crash.
CSCuq23360	H323 GW plays ringback after H225 connect for PRI calls
CSCuq43266	VXML gateway Crash @msw_recog_start process
CSCur16675	VXML gateway Crash @ms_handle_stream_timer
CSCuq10236	LMR rtcp Packet are Sent to rtp Port using IOS 15.2.3T4-ED to 15.4.3M-ED
CSCuq47742	CUBE not opening random UDP ports for SIP.

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.5S

This section documents the open issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.5S.

Identifier	Description
CSCus32530	ASR1K ESP crash in internal L4R removal feature routine
CSCuq75633	BFD down message sent from ASR5500 is not recognized by ASR 1000, it continues to send BFD up message.
CSCus13106	Error in generating keys: resources not available
CSCus15668	ASR1k/03.07.06 forwarding delay increased drastically with NAT
CSCup57389	Traffic drops while testing VRF Lite coexistence with SP NAT for LNS
CSCur48133	ATM 3xOC3 SPA failed to program with IFCFG_CMD_TIMEOUT error
CSCur68999	Configuration change on Tunnel int using shared tunnel protection stops traffic
CSCuq24354	GETVPN KS rekeys without pol changes may cause IOS XE GMs to re-register
CSCuo72301	IKEv2 Crash in free_msg_context
CSCuq24971	ASR1k ucode crash with pa_get_state on using aggregate port-channel
CSCun79934	IN/OUT_UNEXP_OCT_EXCEPTION debug message should include cause of error.
CSCus00801	ASR1002-X cpp crash while processing ICMP Unreachable

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.4S

This section contains the following topics:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.4S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.4S.

- CSCtg39038

  Symptom: Memory leak seen in the "makeErrHandleData" h323 function which is called from the generic CCH323_CT main process. This will lead to MALLOCFAILs which indicates low memory and the router may reload.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCtr87413

  Symptoms: Static route that is injected by "reverse-route static" in crypto map disappears when the router receives the delete notify from the remote peer. Static route also gets deleted when DPD failure occurs.

  Conditions: The symptom is observed when you configure "reverse-route static" and then receive a delete notify or DPD failure.

  Workaround: Use clear crypto sa.

- CSCua81347

  Symptom: Call is getting cleared when media inactivity criteria configured as RTP

  Conditions: Test set up: Analog ph--OGW---CUBE---TGW---Analog ph sip-sip calls with ipv4 Configs gateway media-inactivity-criteria rtp timer receive-rtcp 4 timer receive-rtp 180 When rtp based media inactivity is configured, call is cleared due to media inactivity even though 2 way rtp and rtcp present. RTP based media inactivity detection is not supported in CUBE, this will be a negative test.

  Workaround: Configure media-inactivity-criteria as rtplib, rtcp or all Further Problem Description: Symptom: Call is getting cleared when media inactivity criteria configured as rtp

  Conditions: Test set up: Analog ph--OGW---CUBE---TGW---Analog ph sip-sip calls with ipv4 Configs gateway media-inactivity-criteria rtp timer receive-rtcp 4 timer receive-rtp 180 When rtp based media inactivity is configured, call is cleared due to media inactivity even though 2 way rtp and rtcp present. RTP based media inactivity detection is not supported in CUBE, this will be a negative test.

  Workaround: Configure media-inactivity-criteria as rtplib, rtcp or all

- CSCuf44203

Symptom: AFW memory corruption

Conditions: AFW process crashes, when Request URI or other header string is of size greater than 1k

Workaround: There is no workaround.

- CSCuf73889

  Symptom: Copper SFP's always show Half-Duplex in show interface

  Conditions: Basic copper SFP bringup

  Workaround: There is no workaround.

- CSCuh09580

  Symptom: With IOS-XE 3.7.3S on ASR1K and global crypto ikev2 dpd configuration, all crypto sessions have dpd enabled as expected, after performing RP Switch-Over, the crypto ikev2 dpd configuration is missed, all crypto session are re-established with dpd disabled.

  Conditions: DPD and RP Switch Over

  Workaround: There is no workaround.

- CSCuh23178

  Symptom: Call failure when supplementary services (hold/resume, transfer) is attempted on a call traversing a Cisco CUBE Enterprise gateway. Dead air will be heard and the call will timeout. output from "debug ccsip error" shows the following error. SIP/Error/ccsip_api_response_answer: Media Negotiation failure in 200 OK

  Conditions: Calls traversing a CUBE Enterprise gateway configured for SIP-SIP call-flow. IOS versions impacted vary. So far, all IOS between 15.1(1)T3 and 15.3(2)T is impacted. Failure is reproduced when a consult transfer is attempted on a call that's established with codec g729r8 in a CUCM environment but can occur when there is a codec mis-match during a mid-call event (RE-INVITE) where media is renegotiated.

  Workaround: Resolve the codec mismatch. The most common one is when g729r8 is established as the codec. CUCM will, when acting as the UAS, send a 200 OK advertising g729r8 with no annexb= parameter to specify either 'yes' or 'no.' Per RFC 3555, section 4.1.9, this implies that the parameter is set to 'yes' triggering CUBE to determine CUCM is advertising g729br8. If this is not configured on the dial-peers matched or voice-class codec configured, the call will fail to negotiate a codec and fail.

- CSCuh37526

  Symptom: show crypto entropy stat , output, shows Status = Faulted - syslog message "A pseudo-random number was generated twice in succession" was logged two hours after boot

  Conditions: ISM 15.2(4)M Crypto features enabled

  Workaround: There is no workaround.

- CSCuh54693

  Symptom: Crypto Socket remains CLOSED on DmVPN setup.

  Conditions: This symptom is observed when DmVPN with extended CLI mentions IKE profile as the ISAKMP profile.

  Workaround: Remove the IKEv2 profile configuration from the IPSEC profile.

- CSCuh64174

  Symptom: During IKE QM exchange, the IKE SA can be prematurely deleted without sufficient retransmission because the maximum IKE SA error count is reached during a transient network failure that causes the QM exchange to fail.

  Conditions: This condition can occur if there are multiple simultaneous QM negotiations that are happening around the same time, and they are not successful.

  Workaround: There is no workaround.

- CSCuh89946

  Symptom: You may see the following error messages:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
  %SYS-2-MALLOCFAIL: Memory allocation of 80 bytes failed from0x5CEEBCC, alignment 0
  Pool: Processor  Free: 196745624  Cause: Interrupt level allocation Alternate Pool:
  None  Free: 0  Cause: Interrupt level allocation  -Process= "<interrupt level>", ipl=
  3, pid= 147  %IPMCAST_RPF-3-INTERNAL_ERROR: An internal error has occured while
  obtaining RPF information (No memory available to create pathinfo for RPF lookup)
  ```

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCuh95602

  Symptom: Self bound traffic dropped by firewall

  Conditions: NAT64 is configured and traffic is sent from IPv6 client (in) to IPv4 egress interface of UUT (self)

  Workaround: There is no workaround.

- CSCui55984

  Symptom: Jul 30 08:15:34.099 edt: SDP-3-SDP_PTR_ERROR Received invalid SDP pointer from application. Unable to process. -Traceback= 63BE4438z 61BB36ECz 61B3DF48z 61A025F4z 61A2131Cz 61A24344z

  Conditions: SIP Options received with no SDP and sdp content pass thru enabled

  Workaround: disable SDP content passthru.

- CSCui80379

  Symptom: Can not update audio file using the "audio-prompt load" command.

  Conditions: Using the B-ACD TCL scripts and loading the audio files from the local flash.

  Workaround: Reload router.

- CSCui99153

  Symptom: On bringing up flexvpn session between peers by executing "crypto ikev2 client flexvpn connect" on peer1 memory leak is seen on peer2

  Conditions: Memory leak is observed with responder-only configuration on one of the peer

  Workaround: There is no workaround.

- CSCuj10443

  Symptom: Switch crashes when being added to stack after switchoer

  Conditions: This occurs in switchover scenarios

  Workaround: Reload the complete stack and boot again.

- CSCuj53943

  Symptom: Multicast traffic gets dropped a few seconds after issuing "clear crypto gdoi ks members" on the primary KS.

  Conditions: This symptom is observed under the following conditions:

  1. GMs are registered to the KS with a policy that includes multicast and unicast traffic. Traffic goes fine.

  2. Change the KS policy to "permit ip any any" and configure GM local ACL.

  3. Issue "clear crypto gdoi ks members" on the primary KS.

  4. The GMs correctly reduce TEK lifetime and continue sending traffic. However, some 70 seconds before TEK expiry, multicast traffic starts getting dropped. Unicast traffic is still going fine.

  Workaround: There is no workaround.

- CSCuj70952

  Symptom: Router with 2 IPSec sessions sends DPD to UP-IDLE session even though there is UP-ACTIVE one available.

  Conditions: Router with 2 IPSec sessions sends DPD to UP-IDLE session even though there is UP-ACTIVE one available.

  Workaround: There is no workaround.

- CSCuj79520

  Symptom: Increased use of global addresess over time while running PAP

  Conditions: NAT PAP enabled along with vrf on outside interfaces

  Workaround: If global address pool becomes deleted, it may become necessary to clear ip nat translations or reload the CPP.

- CSCuj94346

  Symptom: Mid-call UPDATE with SDP is rejected with "500 Internal Server Error".

  Conditions: This issue is seen only for EO-EO/EO-DO call-flows.

  Workaround: There is no workaround.

- CSCuj99605

  Symptom: When a long very long Refer-To header is received, router crashes

  Conditions: During call transfer, In REFER message long Refer-To header results in crash.

  Workaround: There is no workaround.

- CSCul06522

  Symptom: IOS routers can sometimes create duplicate IPSec SA pairs. This decreases platform scalability. Traffic flow is not affected.

  Conditions: This was observed in IOS 15.2(4)M4, 15.2(4)M5, 15.3(3)M1. Other versions can be affected as well.

  Workaround: None, apart from clearing both normal and duplicate SAs with "clear crypto ipsec sa" or "clear crypto session".

- CSCul32304

  Symptom: DSP invoked for non-xcode call

  Conditions: For Signalling forked call,DSP resources are used for no transcoded call.

  Workaround: There is no workaround.

- CSCul46066

  Symptom: Hung Calls with SIP SPI with Refer Consume Load

  Conditions: This symptom is observed under following conditions:

  1. Configure max connection with 3 Refer to Dial-peer & outbound dial-peer towards CVP.

  2. Run Load with 1000 calls for few hours. CPS: 10 CHT: 100 secs Total Number of active calls : 750 Issue observed with max-conn with multiple dial-peers

  Workaround: Use dial-peers without max-conn.

- CSCul84718

  Symptom: The recursive behaviour causes the (physical) box to crash.

  Conditions: With incorrect config on the Client/LAC routers, ASR1K is receiving a bad encapsulation due to which it tries to route to the Multilink bundle through the bundle itself.

  Workaround: There is no workaround.

- CSCum00643

  Symptom: Router experience several crashes during the day.

  ```
  UTC: %SIP-3-INTERNAL:  Corrupted scb  000160: Dec  7 16:30:31.931 UTC:
  %SYS-2-INTSCHED: 'suspend' at level 0 , all interrupts disabled -Process=
  "CCSIP_SPI_CONTROL", ipl= 0, pid= 426
  ```

  Crash was observed while trying to free the memory allocated for handling the authentication. showing it as 0X0D0D0D. So crashing while trying to free this memory.

  Conditions: Crash was observed while trying to free the memory allocated for handling the authentication. showing it as 0X0D0D0D. So crashing while trying to free this memory.

  Workaround: There is no workaround.

- CSCum04325

  Symptom: Duplicate entry seen in "sh lldp neighbor"

  Conditions: if the physical link is a member of a etherchannel bundle. lldp packets are processed on the bundle UIDB.

  Workaround: There is no workaround.

- CSCum20746

  Symptom: Key Server (KS) fails to send rekey & Group Member (GM) fails to process rekey when "clear crypto gdoi ks members" is executed on the KS after changing the IPsec ACL with Suite-B configured on the KS. Secondary KSs don't show any TEKs after changing crypto ACL.

  Conditions: Key Server (KS) has Suite-B configured with a certain IPsec ACL. Change the IPsec ACL on the KS so that the new ACL has no overlapping entries as the old ACL and issue "clear crypto gdoi ks members" on the Primary KS.

  Workaround: Issue "clear crypto gdoi" on the GMs to force their re-registration. Further Problem Description:

- 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:

  a) 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

  b) Temporarily increase CAC to accommodate new SA requests: crypto call admission limit ike in-negotiation-sa 60

- CSCum86411

  Symptom: BGP performance will be slower on RP2 on 15.4(02)S release or newer images.

  Conditions: Large scale BGP routes

  Workaround: Use Image 15.4(01)S or older.

- CSCun05121

  Symptom: Memory leak at SRTP Keys in Dolby Feature.

  Conditions: Memory leak seen in SRTP Call

  Workaround: There is no workaround.

- CSCun20588

  Symptom: When REFER is received on CUBE and CUBE send to ITSP where ITSP did not respond to the REFER and CUBE try to Resume the call Memory Leak seen .

  Conditions: When REFER is received on CUBE and CUBE send to ITSP where ITSP did not respond to the REFER and CUBE try to Resume the call Memory Leak seen .

  Workaround: There is no workaround.

- CSCun30311

  Symptom: 'show platform software status control-processor brief' on ASR1K inserted with ASR1000-6TGE & ASR1000-2T 20X1GE will show the card status as unknown

  Conditions: 'show platform software status control-processor brief' on ASR1K inserted with ASR1000-6TGE & ASR1000-2T 20X1GE will show the card status as unknown

  Workaround: There is no workaround.

- CSCun39803

  Symptom: Intermittent connectivity loss between hosts at different OTV sites. Pinging from one host to the other more than 8 times restores connectivity for about 8-10 minutes. Packet captures show ARP request broadcasts from a host at one site not being received by the host at the other site for about 7-8s, and then suddenly starting to work. This problem has a tendency to get worse over time, with more and more hosts being affected over the course of a week or two until connectivity between sites is essentially gone.

  Conditions: ASR1K running 15.4 or 15.3 code, possibly earlier code, with OTV configured.

  Workaround: There is no workaround.

- CSCun60555

  Symptom: An ESP crash may occur after removing an MFR interface soon after it was created.

  Conditions: This behavior may be seen on IOS-XE platforms running software versions that support MFR. It may be dependent on the timing of the configuration and removal of the interface. The crash only affects the ESP card.

  Workaround: There is no workaround.

- CSCun62181

  Symptom: A Cisco ASR 1002 router running Cisco IOS XE Release 3.4S crashes when recalculating PMTU.

  Conditions: The symptom occurs when the outgoing tunnel interface flaps.

  Workaround: There is no workaround.

- CSCun73233

  Symptom: No way audio (silence) issue is noticed on transcoded SIP-SIP calls on CUBE when supplementary services like Hold/Resume or Call Transfer is invoked. Issue is observed with both SCCP based transcoding and LTI (Local Transcoding Interface) based transcoding. When using SCCP Based Transcoding, "show sccp connection" output looks as below during no-way audio issue (Mode - Inactive, rport - Empty, ripaddr - Empty, conn_id_tx - Empty) CUBE-2#show sccp connections sess_id conn_id stype mode codec sport rport ripaddr conn_id_tx 65545 36 xcode inactive g729 16414 0 :: 65545 40 xcode inactive g711a 16412 0 :: When using LTI based transcoding, "show dspfarm dsp active" shows no entry of the call during no-way audio CUBE-2#show dspfarm dsp active SLOT DSP VERSION STATUS CHNL USE TYPE RSC_ID BRIDGE_ID PKTS_TXED PKTS_RXED Total number of DSPFARM DSP channel(s) 0

  Conditions: IOS Release 15.3(3)M Issue happens only under following condition. 1. When "midcall-signaling passthru media-change" is configured on CUBE 2. There is change in codec in one of the call leg after invoking supplementary services like Hold/Resume or Transfer

  Workaround:

  1. Disable "midcall-signaling passthru media-change" Voice service voip Sip no midcall-signaling passthru media-change

2. Use same codec through-out the call (Avoid change in codec behavior by controlling supported codec list)

- CSCun76377

  Symptom: On CUBE if MTP invoked for the call Forking packets showing 0:

  Conditions: On CUBE if MTP invoked for the call Forking packets showing 0:

  Workaround: There is no workaround.

- CSCun78257

  Symptom: command is

  Conditions: Configured "mgcp echo-cancel mode off" and reloaded the voice-gateway observed in 15.2(2)T4 and 15.3(3)M2

  Workaround: re-enter command

- CSCun84368

  Symptom: Netflow cache entry is not created for IPV6 flows and entries for IPv4 entries is not accurate. For IPv4 entries the BGP next hop is not updated and set to 0.0.0.0

  Conditions: Upon Execution of RP switchover.

  Workaround: After RP switch-over, remove BGP configuration from Core router ("P") , and configure it back. updaon BGP update on PE router, the BGP - NH will appear in FNF records.

- CSCun91923

  Symptom: CUBE reloads intermittently while handling SIP call forking scenario.

  Conditions: In SIP Call forking scenario, an INVITE sent from CUBE is routed to multiple SIP endpoints and multiple SIP provisional responses such as 183 Session Progress with different To tags are received.

  Workaround: There is no workaround.

- CSCun92244

  Symptom: Due to errors in the code, when PAP is configured, NAT can create binds in which a particular global address and port can be assigned to multiple local addresses.

  Conditions: NAT with PAP must be configured in order for this problem to manifest.

  Workaround: There is no workaround.

- CSCun92245

  Symptom: A Cisco router or switch may experiences a memory leak due to "Crypto IKMP" process. This may occur if multiple DHCP servers are configured under crypto config. Eg: crypto isakmp client configuration group NAME dHCP X.X.X.X X.X.X.X dhcp X.X.X.X X.X.X.X

  Conditions: Multiple Dhcp servers configured under crypto.

  Workaround: Only use a single Dhcp server. Due to an error in code, only the memory structures associated with data from the last Dhcp server in the list are properly freed after a lookup takes place. Data from other servers in the list is retained indefinitely with each lookup.

- CSCun93593

  Symptom: Caller id is not received intermittently on FXO ports. we have dangling dsm_handle associated with this port and it is preventing from sending further dsp messages to start caller id. Mar 24 16:18:22.054: [0/1/1] htsp_start_caller_id_rx:BELLCORE Mar 24 16:18:22.054: htsp_start_caller_id_rx htsp->dsm_handle 2AC5E96C

  Conditions: The symptom has been observed on IOS 150-1.M7, with PVDM3.

Workaround: Router reload fixes the issue.

- CSCun96598

  Symptom: SNMP query on DS3-MIB objects like dsx3LineLength, dsx3LineStatusLastChange, dsx3LoopbackStatus and dsx3Channelization are showing value 'zero' for SPA-2XT3/E3 card

  Conditions: Testing DS3-MIB objects on 2XT3/E3

  Workaround: There is no workaround. none

- CSCun99798

  Symptom: SNMP query on dot3Stats counters are not updating on ASR1000-6TGE card and ASR1000-2T 20X1GE.

  Conditions: While testing EtherLike MIB

  Workaround: There is no workaround.

- CSCuo00479

  Symptom: Slow memory leak in small/middle I/O buffers. This can be identified by looking at the output of "show buffer" and "show buffer usage" commands You'll see the number of small and middle buffers incrementing to very high values VG224-1#sh buffer | inc peak Small buffers, 104 bytes (total 1116, permanent 50, peak 1242 @ 00:00:17): Middle buffers, 600 bytes (total 1937, permanent 25, peak 2217 @ 00:00:16): The output of 'show buffer usage' will show the SCCP Application as a Resource User of the buffers and increasing until memory is exhausted. Caller pc : 0x6238D4C8 count: 4454 Resource User: SCCP Appli count: 4455 Once memory is exhausted, telnet sessions will fail to establish. Console access may still be available.

  Conditions: VG224 registered to CUCM and defined as a SCCP controlled gateway. This is seen when the CUCM rejects the registration attempts of the VG224 FXS ports due to it reaching the " Maximum Number of Registered Devices" value as defined in the CUCM Service Parameters. This can occur when devices fail-over from the primary to secondary CUCM and the proper device sizing has not been followed as per the CUCM SRND. Too many devices attempt to register and CUCM starts to reject their attempts.

  Workaround: Ensure that in fail-over scenarios, the number of devices that attempt to register to CUCM don't exceed the number set in "Maximum Number of Registered Devices" service parameter.

- CSCuo02270

  Symptom: Issues with source VLAN numbers while using with ERSPAN.

  Conditions: VLAN greater than 1005 were not displayed in the running config. There is no service impact.

  Workaround: There is no workaround.

- CSCuo05164

  Symptom: Sequence number reuse is disabled with anti-replay disabled

  Conditions: Sequence number will not be reused

  Workaround: There is no workaround.

- CSCuo09341

  Symptom: ESP100 crash while running IPoE subscriber traffic class feautres.

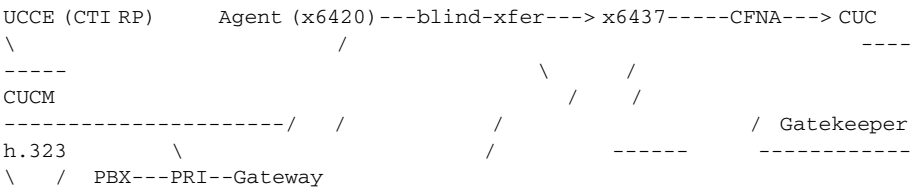
  Conditions: IPoE subscriber traffic class features are configured on ASR1K platform with ESP100 board.

  Workaround: There is no workaround.

- CSCuo12138

  Symptom: One way audio when Agent blind-transfers a call from PSTN (h.323 gateway) to a second DN, which then CFNA's to Unity

  Conditions: The issue seems to be a race condition. The call flow/scenario that seems to cause the race condition is as follows:



  Workaround: Use consultive transfer

- CSCuo18931

  Symptom: DSCP values are set for the VoIP signalling and media packets using the "ip qos dscp" command under the dial-peer. The default value, in the absence of explicit configuration, should be "af31" for signalling and "ef" for media. When setting dscp values for signaling/audio/video under the dial-peer the media packets are marked with AF11 instead of AF33 with the following configuration ip qos dscp af11 media ip qos dscp af21 signaling ip qos dscp af33 video rsvp-none

  Conditions: This occurs when configuration is applied on dial-peer with the following call flow and IOS CALL FLOW CTS endpoint - SIP - CUCM -SIP - CUBE -SIP- SME -SIP- ISDN Video Gateway CUBE Platform/IOS c2900-universalk9-mz.SPA.153-3.M1.bin

  Workaround: Apply the qos configuration on the interface using class map and policy map.

- CSCuo26733

  Symptom: CAC compound scope src-adj,dst-adj cannot be configured

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCuo28583

  Symptom: Ring off/on period is not changed even we configure ring cadence as followings.

  - cptone KR
  - ring cadence pattern01 or
  - cptone KR
  - ring cadence define 20 40
  - cptone KR
  - ring cadence define 20 40 20 40

  ========== Apr 10 14:13:51.525: [2/0] htsp_set_caller_id_tx calling num=2701 display_info= called num=1068 Apr 10 14:13:51.525: [2/0] Caller ID String 80 13 01 08 30 34 31 30 31 34 31 33 02 04 32 37 30 31 08 01 4F AE Apr 10 14:13:51.525: [2/0] voice port htsp_set_caller_id_tx_time: ring cadence not suitable for caller id. on_time_first=1000 off_time_first=2000 on_time_second=0 off_time_second=0 <<<<< Apr 10 14:13:51.529: [2/0] c2400_get_ring_cadence: cadence: 2000, 4000, 0, 0, 0, 0 <<<<<

  Conditions: VG224-MP 15.1(4)M5 cptone KR

  Workaround: There is no workaround.

- CSCuo29084

  Symptom: Call Flow: PSTN -H.323-GW - 3rd Party IVR System. When using payload type 97 & 96 for RTP-NTE with H.323 , gateway is found to set Marker bit as false, which caused 3rd party IVR not to recognize DTMF inputs provided by Caller.

  Conditions: Call Flow: PSTN -H.323-GW - 3rd Party IVR System.

  Workaround: There is no workaround.

- CSCuo31506

  Symptom: Packet drop is observed on GM.

  Conditions: Traffic is dropped after ipsec flap

  Workaround: There is no workaround.

- CSCuo31517

  Symptom: Autoneg status on copper SFP is always displayed as completed. It should be incomplete when there is a mismatch in autoneg configuration/negotiation.

  Conditions: ASR1k-BUILTIN-2x10GE-20x1GE ports with copper SFP (SFP-GE-T) inserted on 1GE port.

  Workaround: There is no workaround.

- CSCuo34250

  Symptom: Inbound and outbound calls through FXO ports are disconnecting always if "supervisory disconnect anytone" command is present in the FXO Voice-port. If we remove the command, calls would work without any issues. However, in 151-3.T1 calls would work fine with "supervisory disconnect anytone" command present in the voice-port. CSCum09273 fixed the issue with inbound calls through FXO port. Outbound calls are still not working.

  Conditions: When "supervisory disconnect anytone" command is configured under voice-port

  Workaround: Remove "supervisory disconnect anytone"

- CSCuo37411

  Symptom: Under heavy load, CPP cpu utilization can become excessive, finally leading to stuck thread interrupt

  Conditions: The issue was seen while running CGN and PAP with BPA although in theory, the error could occur whenever there is a lot of churn on NAT translations and the number of PAT blocks associated with a pool becomes very large (on the order of 8-10 thousand)

  Workaround: There is no known workaround.

- CSCuo42772

  Symptom: Cannot configure erspan session destination port

  Conditions: Cannot configure the erspan destination port when the port index exceed the 9215

  Workaround: reload system

- CSCuo46913

  Symptom: A crash is seen causing a system reload. The crash occurs in the crypto IKMP process: Exception to IOS Thread: Frame pointer 0x3CEFFB58, PC = 0x164CC518 UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Crypto IKMP

  Conditions: This symptom occurs after the following debug: debug cry condition peer subnet XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX The exact conditions are still being investigated.

  Workaround: There is no workaround.

- CSCuo49765

  Symptom: There's a mismatch between the power threshold values in the "show hw-module subslot x/y transceiver z idprom detail"outputs and the power threshold values in the SNMP polling results.

  Conditions: The router is using CWDM SFP.

  Workaround: There is no workaround.

- CSCuo50995

  Symptom: The IP Identification field of packets sent from a ASR1000 acting as an IAP to a Mediation Device/MD always have the value set to zero

  Conditions: This behaviour has been observed on multiple IOS-XE release, including the current latest 3.12S release

  Workaround: Configure the MTU of the IAP, MD and interconnecting devices to avoid fragmentation

- CSCuo51043

  Symptom: The dynamic L2L peer will successfully bring up, both phase-1 and phase-2 although the isakmp profile does not cater to this new peer.

  Conditions: IOS L2L end-point catering to dynamic peers, with a dynamic crypto map, under which we have: a) an isakmp profile that does not match the isakmp identity of this new peer b) no crypto ACL [i.e. no 'match address' statement] Note: a crypto ACL can be configured under the dynamic map, that is either an exact or a super-set mirror image of the peer's crypto ACL, although this is not mandatory.

  Workaround: There is no workaround.

- CSCuo52113

  Symptom: Redundant Gatekeeper setup and high CPU is experienced from time to time during the GUP un-registeration operation.

  Conditions: Traceback= 0x9434BECz 0x942BEC0z 0x942BFE8z 0x942C03Cz 0x9457E08z 0x93FE7CCz 0x94022F0z 0x4DD7EACz 0x4DBDD18z

  Workaround: There is no workaround.

- CSCuo52384

  Symptom: ROMMON get_mac_addr and IOSXE IDPROM access fail on booting standby RP2.

  Conditions: External USB thumb drive used on RP2.

  Workaround: Remove external USB thumb drive on RP2.

- CSCuo53594

  Symptom: CUBE use early dialog Record-Route on ACK message.

  Conditions: CUBE receive another Record-Route on 180 and 200

  Workaround: There is no workaround.

- CSCuo54224

  Symptom: Path-confirmation check failed on CUBE in SRTP-RTP call

  Conditions: Configure CUBE for SRTP-RTP call

  Workaround: There is no workaround.

- CSCuo55412

  Symptom: Configured Asymmetric carrier delay value does not reelect show interface output.

  Conditions: Configured Asymmetric carrier delay for int and confirm the "show interface"

  Workaround: Confirm "show run" only.

- CSCuo55610

  Symptom: Incomplete kernel core file with filename ending in .TEMP_IN_PROGRESS.

  Conditions: Active RP kernel core dump in dual RP2 systems.

  Workaround: There is no workaround.

- CSCuo59922

  Symptom: CUBE use different route header value order

  Conditions: CUBE receive Record Route header with multiple value

  Workaround: There is no workaround.

- CSCuo61455

  Symptom: Router crash with NAT ALG enabled on the router

  Conditions: NAT ALG feature enabled on the router.

  Workaround: Disable NAT ALG using: "no ip nat service all-alg"

- CSCuo68525

  Symptom: Incorrect RTP connections seen for calls from SCCP-Jabber Video Phone

  Conditions: There are no known conditions

  Workaround: There is no workaround,

- CSCuo80152

  Symptom: May 7 16:34:32.486 CET-DST: PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT IOS thread disabled interrupt for 20 msec -Traceback= 1#44e17d688b5204366de10e7ade81ac0c :400000 13D4E91 :400000 4357A45 :400000 43581FA :400000 3C547C3 :400000 76D4576 :400000 71C865D :400000 71C6E07 :400000 76D0230 :400000 76D011D

  Conditions: Seen on asr1001

  Workaround: There is no workaround.

- CSCuo82943

  Symptom: SADB Peer Chunk leak seen

  Conditions: DmVPN Hub with 2000 simulated spokes in stress/scale scenario

  Workaround: There is no workaround. Symptom: SADB Peer Chunk seen

  Conditions: DmVPN Hub with 2000 simulated spokes in stress/scale scenario

  Workaround: There is no workaround.

- CSCuo84925

  Symptom: Rx/tx packets are not getting increased .

  Conditions: Rx/tx packets should get increased ,so that Path confirmation will be successful

  Workaround: There is no workaround.

- CSCuo85191

  Symptom: Crash is observed on ASR1000.

  Conditions: This symptom is observed when memory allocation fails.

  Workaround: There is no workaround.

- CSCuo85982

  Symptom: High RP and ESP utilization and generation of many large (~ 1 MB) logging files with names of the form "cpp_cp_F*".

  Conditions: IPv4 multicast packets received on interfaces configured for IP-interface subscriber sessions.

  Workaround: There is no workaround.

- CSCuo89222

  Symptom: Ping across NAT router fails after multiple switchovers

  Conditions: Multiple switchover

  Workaround: There is no workaround.

- CSCuo97597

  Symptom: ISSU Minimal Disruptive Restart(MDR) upgrade does not work for Gigabit Ethernet SPAs, POS SPAs and Ethernet Line cards from 15.4(03)S to 15.5(01)S

  Conditions: Seen only with ISSU/MDR. The issue is seen ONLY with MDR (mdr keywords in ISSU command line). There is NO issue with regular ISSU (without MDR)

  Workaround: There is no workaround.

- CSCuo99185

  Symptom: When PE receives a packet with the destination of CE's interface's address, PE router crashes.

  Conditions: topo: CE(1.1.1.1)------PE1------(mpls)--------PE2 there is a static ip route on PE1: ip route vrf xxx 1.1.1.1 255.255.255.255 3.3.3.3. and 3.3.3.3 is the PE1's VRRP address. Then PE2 sends traffic with dst address 1.1.1.1 to PE1 and PE1 crashes.

  Workaround: remove above static ip route.

- CSCup03259

  Symptom: Memory leak in Normal Buffers In the output of the command show buffers old, PC point to pak_copy_network_start_particlized Open a TAC case to validate this

  Conditions: This behavior is seen in 15.4(2)T and in 15.3(3)M3 Found similar case where this behave was seen since the upgrade from Version 15.2(3)T4 to Version 15.4(2)T

  Workaround: Remove the command "qos pre-classify" in a crypto map. Reload the device to release memory Use the memory-size iomem command to assign more memory to the I/O pool to prolong use.

- CSCup07972

  Symptom: MMOH stops working after upgrading the IOS to 15.2.4M6 or 15.2.4M6a and 15.3(3)M3

  Conditions: IOS 15.2.4M6 or 15.2.4M6a or 15.3(3)M3 should be installed in the Router. It affects the following call flows: CUCM (MMOH Source) -> CUBE -> Unicast - > SIP ITSP Router (MMOH Source from Flash:) - > PRI => Multicast MOH Spoofing

  Workaround: Use Unicast MOH instead. Downgrade the IOS to 15.2.4M5

- CSCup11175

  Symptom: A memory corruption crash on ASR.The crash is related to SIP Gateway.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCup12306

  Symptom: CUBE makes video port o during video escalation

  Conditions: This issue is observed when 2nd preferred video codec is selected in answer SDP. this occurs only during video escalation.

  Workaround: during video escalation if the most preferred video codec is selected in asnwer SDP then this issue is not seen

- CSCup18062

  Symptom: A memory leak is observed.

  Conditions: This symptom occurs on a device running Cisco IOS XE Release 3.7.5S. The leak does not occur with all crypto map-related configuration. It occurs with RSA authentication and with specific configuration as shown below: crypto dynamic-map itcard_dynamic 600 set transform-set <name> set pfs group5 set identity IDENTITY600>*** match address IDENTITY600

  Workaround: There is no workaround.

- CSCup18295

  Symptom: A router will crash with a segmentation fault in IOSD: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = CCSIP_SPI_CONTROL

  Conditions: There are no known conditions

  Workaround: There is no workaround.

- CSCup22018

  Symptom: Termination Tone for SIP Outbound Dialer not detecting properly. Symptoms include cut off prompt left in voicemail boxes for customers of outbound campaigns, where a voicemail is left by the dialer.

  Conditions: SIP outbound dialer being used with an IOS GW to detect voice/voicemail/fax/etc.

  Workaround: There is no workaround.

- CSCup23429

  Symptom: Error response for ReINVITE is not getting passed across by CUBE and the call is getting disconnected.

  Conditions: CUBE adds a wrong header through sip-profile while sending ReINVITE.

  Workaround: There is no workaround.

- CSCup29570

  Symptom: packets of 64,850, and 1200 byte packet sizes are being dropped on Port-Channel interface with WCCP enabled under the interface

  Conditions: ASR1k upgrade from 2.4.4 to 3.10.0

  Workaround: remove WCCP from interface.

- CSCup34371

  Symptom: GETVPN GM stops decrytping traffic after TEK rekey (1-2/day for 7200s TEK lifetime)

  Conditions: Several conditions need to be satisfied for this issue to be seen. The crypto map must shared (example several interfaces with same crypto map sourced from the same interface), the old and new SPI during rekey have a hash collision on the higher 4 bits and in addition the interface of the incoming packet has an address that is higher than the one stored in the SA since the crypto map is shared.

  Workaround: There is no workaround.

- CSCup34928

  Symptom: RP switchover while filling event-buffer with wccp events

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCup37676

  Symptom: ASR1K crashes when pinging end-to-end over OTV with a frame size greater than (MTU-42) bytes.

  Conditions: This has been seen on two ASR1002-X's running IOS-XE 03.10.01.S. Crash was seen when passing large packets across an OTV topology.

  Workaround: Limit oversize packets across overlay topology.

- CSCup39448

  Symptom: show interface counter doesn't increase on partial Serial line with ASR1001-8XCHT1E1.

  Conditions: The stats update is skipped rest of the VC's in that port if one interface is down in that port. All of channelized T1/E1 modules running IOS-XE 3.7.2S (or after) potentially exists this problem.

  Workaround: explicitly shutdown the interface which is in down.

- CSCup46760

  Symptom: Memory leaks are observed for Media Forking B2B HA Call flows on the STANDBY router in a B2B setup.

  Conditions: Basic call with audio forking

  Workaround: There is no workaround.

- CSCup51813

  Symptom: During ipsec rekey, packet drops are seen for some time due to NO SA FOUND.

  Conditions: This is caused by commit of DDTS CSCul06522.

  Workaround: There is no workaround.

- CSCup53658

  Symptom: q-in-q subinterfaces on a Cisco ASR 1000 Series router do not show correct traffic statistics via SNMP ifTable/ifXTable or CLI (show vlans dot1q).

  Conditions: This symptom occurs when the subinterface is configured under a port channel. The issue is not seen when the subinterface is a part of the physical interface.

  Workaround: Traffic statistics via CLI can be obtained directly from the SPA by using the following command for each member interface of the port channel: Using Gi1/3/0 as an example: request platform software console attach 1/3 (Note: On Cisco ASR 1000 releases prior to XE 3.2 this

command may fail. If so, use the hidden command: ipc-con <slot> <bay>) show hw-module subslot 0 tcam all_entries vlan brief Note the VLANs (denoted by V1 and V2) for which statistics are required.

Example:

Slot-0-0>show hw-module subslot 0 tcam all_entries vlan brief ADDR PO V1 V2 C1 C2 ETYPE QVASN IPF IT IACL IRID EPF ET EACL ERID VVID PV PS DA SCTH FE RGN 2076 00 2005 1507 00 00 0000 18 2212 00 0004 0000 0002 00 0004 0000 0000 C0 00 00 0000 00 6

Use the following command to get VLAN TCAM statistics for the TCAM with address 2076 (that handles q-in-q for VLAN 2005 and 1507 as per V1 and V2 columns)

Output will be like the following:

show hw-module subslot 0 tcam counters vlan 2076 VLAN Rx Hit : Pkt: 1066 VLAN Rx Unicast Send : Pkt: 1065 Byte: 126102 VLAN Rx Mcast Send : Pkt: 0 Byte: 0 VLAN Rx Bcast Send : Pkt: 1 Byte: 64 VLAN Rx Osub Drop : Pkt: 0 Byte: 0 VLAN Tx Hit : Pkt: 1066 VLAN Tx Ucast Send : Pkt: 1064 Byte: 126038 VLAN Tx Mcast Send : Pkt: 0 Byte: 0 VLAN Tx Bcast Send : Pkt: 2 Byte: 128

Alternatively to avoid the need to look up the TCAM address beforehand, you can use the following syntax:

show hw-module subslot 0 tcam entry vlan 0 first-vlan-tag second-vlan-tag 0 8 8 | i Pkt

The Hit counters represent overall TX/RX packet counters. The RX/TX send represent packet and byte counts for Unicast, Multicast and Broadcast Respectively Note: The only way to clear the counters is to remove and readd the member interface from the port channel.

- CSCup54337

  Symptom: HA related issues.

  Conditions: When ipsec HA is configured

  Workaround: There is no workaround.

- CSCup57814

  Symptom: Users on the analog phone behind a VG224 cannot hear the zip-zip (double beep) tone while hitting a Route Pattern with FAC required.

  Conditions: 15.1(4)M train release on VG224 Non-US cptone configured on voice port Skinny protocol for registration of VG224.

  Workaround: Configure US cptone. Downgrade to 15.0(1)M release of IOS.

- CSCup69201

  Symptom: ISAKMP NAT Keepalives are not send correctly while fVRF is used

  Conditions: fVRF and ISAKMP NAT Keepalives are used

  Workaround: Use DPDs instead.

- CSCup72039

  Symptom: DMVPN: Phase 2 fails with PROPOSAL_NOT_CHOSEN when two phases 1 In "debug crypto ipsec" following message is seen: *Jul 3 13:20:54.567: Cannot find crypto swsb for idb Ethernet0/0: in ipsec_process_proposal (), 1206 *Jul 3 13:20:54.567: IPSEC(ipsec_process_proposal): TP not configured or sadb not init for idb Ethernet0/0 *Jul 3 13:20:54.567: Cannot find crypto swsb : in ipsec_process_proposal (), 1590

  Conditions: multipoint GRE used (DMVPN) Phase 2 or Phase 3 OR It might be also seen for regular GRE over IPSEC or regular VTI

Workaround: - disable periodic DPDs the hub - use IKEv2

- CSCup76000

  Symptom: IPsec Tunnel may flap under certain network conditions.

  Conditions: IPsec Quick Mode Message 3 is lost during transit over the network. The old SA gets deleted 7 seconds after the QM3 message is sent. On the responder the tunnel is marked as being down until Quick Mode retransmits.

  Workaround: There is no workaround.

- CSCup80547

  Symptom: When a GETVPN GM receives an ESP packet with an invalid SPI, it generates an erroneous syslog with the following format : "CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip) vrf/dest_addr= /x.y.z.w, src_addr= a.b.c.d, prot= 50"

  Conditions: When a GETVPN GM receive an ESP packet with invalid SPI

  Workaround: There is no workaround.

- CSCup80803

  Symptom: No Way audio when dialing out through CUBE using Early Offer. After hold/resume on IP phone, two way audio is heard. After call is connected, "show voip rtp conn" will look like this:

  Show voip rtp conn: 3 2217464 2217466 21352 26732 10.10.10.10 10.0.149.79 <---- looks good (inside leg) 4 2217466 2217464 21356 0 10.20.20.20 0.0.0.0 <----- Oh no (outside leg)

  Conditions: - sdp passthrough configured - Two provisional (18x) messages. First 18x has TO tag

  1. Second 18x message and 200OK has TO tag

  2. - Early offer through CUBE

  Workaround: Use delayed offer Remove SDP passthrough under voice service voip.

- CSCup81326

  Symptom: 2 ASR1000 running in inter-chassis redundancy SBC and both the routers encountered ESP reloads:

  Conditions: SBC inter-chassis redundancy

  Workaround: There is no workaround.

- CSCup98776

  Symptom: Outbound SA creation failure in the ESP under certain conditions, and all further requests are also not processed.

  Conditions: ESP is not available/online when the outbound SA creation request is issued from IPSec PI in a GETVPN setup where ASR1K is GM

  Workaround: Reload the ASR1K.

- CSCuq00749

  Symptom: When IPSEC PI encounter errors in installing IPSEC SAs to HW-crypto, it will trigger GDOI to re-register. If the SAs installation error happen very rapidly, it will in turn request GDOI to perform rapid re-registration. This operation will consume a lot of CPU and make the GM-routers not operating.

  Conditions: This problem only happen if HW crypto-engine has gone into an error state and many IPSEC SA installation fail

  Workaround: There is no workaround.

- CSCuq00944

  Symptom: Incoming calls to SIP GW / CUBE are rejected with 'Malformed/Missing TO: field' or 'Malformed/Missing FROM: field'".

  Conditions: To and FROM Fields contain commas.

  Workaround: Upgrade the ios to 15.4.2T and use inbound SIP-Profiles.

- CSCuq02069

  Symptom: CUBE-SP calls start failing and high CPU is reported when a crypto pki command is entered on the stand-by ASR.

  Conditions: CUBE-SP is configured for HA

  Workaround: There is no workaround.

- CSCuq05276

  Symptom: ASR1K crashes due to chunk already released in ipv4_nat_esp_remove_conn

  Conditions: This crash was witnessed once only in a simulated live network that included Encapsulating Security Protocol (ESP) packets.

  Workaround: This is a very rare condition - the problem should not be seen but if crash does occur - reloading will resolve the issue.

- CSCuq20216

  Symptom: Reduce the GDOI rate-limit window size for IPSec triggered registration

  Conditions: More than one IPsec triggered registration within the GDOI rate-limit window size

  Workaround: Make all the KS ACL changes in one go and force a rekey, instead of multiple changes and rekeys.

- CSCuq21258

  Symptom: Logs seen before/during the crash: 089450: Jul 15 18:26:56.996 UTC: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.248.9.228 (Tunnel1) is up: new adjacency 089451: Jul 15 18:28:23.281 UTC: %MCP_SYS-0-ASSERTION_FAILED: F0: fman_fp_image: Assertion failed: Assertion failed: fman/fp/./src/fman_ipsec_pal.c:1223: "0 != p_reply_base->m_magic" -Traceback= 1#56d8d6d8160084eaf58349be59d88d14 errmsg:C584000 2230 binos:A027000 D2A0 binos:A027000 744C :10000000 3C20AC :10000000 3C5AE8 ipsec_pal_config:B62C000 31170 fman_fp:F835000 244C74 fman_fp:F835000 244E64 :10000000 22F480 :10000000 3B4800 evlib:9FEF000 E16C evlib:9FEF000 10554 :10000000 3F6528 c:7825000 1E938 c:7825000 1EAE0 089452: Jul 15 18:28:24.019 UTC: %IOSXE_OIR-6-OFFLINECARD: Card (fp) offline in slot F0 089453: Jul 15 18:28:46.230 UTC: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.248.9.178 (Tunnel1) is down: holding time expired 089454: Jul 15 18:29:17.117 UTC: %CPPHA-3-FAULT: F0: cpp_ha: CPP:0.0 desc:CPP Client process failed: FMAN-FP det:HA class:CLIENT_SW sev:FATAL id:1 cppstate:RUNNING res:UNKNOWN flags:0x0 cdmflags:0x0

  Conditions: First observed on 15.3(3)S1 ASR1002

  Workaround: There is no workaround.

- CSCuq68196

  Symptom: ASR1k RP crash UNIX-EXT-SIGNAL: Segmentation fault(11), Process = AFW_application_process

  Conditions: There are no known conditions

  Workaround: There is no workaround.

- CSCuq70263

  Symptom: A Cisco ASR1002-X router might reboot unexpectedly.

  Conditions: Cisco ASR is running the Cisco Unified Border Element (CUBE) feature in the Enterprise mode for SIP to SIP calls and is using the IOS-XE version asr1002x-universalk9.03.10.03.S.153-3.S3-ext.SPA.bin

  Workaround: Change the transport mechanism from UDP to TCP for the SIP traffic.

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.4S

This section documents the open issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.4S.

- CSCui36340

  Symptom: Need IOS CLI to track ASR1002-X, ESP-100 and ESP-200 crypto engine healthy status

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCui43325

  Symptom: Traffic blackhole for v6 SSM groups after flapping bgp loopback interface on the egress PE

  Conditions: BGP loopback interface flap

  Workaround: Unconfigure-reconfigure the mdt default command under the v6 address-family for the vrf

- CSCui67325

  Symptom: The ESP may crash in cpp_mcplo %CPPHA-3-FAULT: F0: cpp_ha: CPP:0.0 desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL id:2121 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x8

  Conditions: NAT is enabled

  Workaround: There is no workaround.

- CSCul29434

  Symptom: ELC MDR: %CWAN_HA-4-IFEVENT_BULKSYNCFAIL: receive failed ifevent: 10 err

  Conditions: During Consolidated MDR upgrade.

  Workaround: There is no workaround.

- CSCul37241

  Symptom: Memory leak seen on standy (new active) after SSO and Hold/Resume with SDP passthru

  Conditions: This condition is observed during SDP passthru

  Workaround: There is no workaround.

- CSCul78096

  Symptom: With the command "no route set interface" configured under the default ikev2 authorization policy, the command will be changed to "route set interface" after a reload.

Conditions: This behavior only affects the default ikev2 authorization policy, and not an user-configured policy.

Workaround: If "route set interface" needs to be disabled, then use an user-configured ikev2 authorization policy instead of the default policy.

- CSCun41391

  Symptom: FP crash after the IOS-XE upgrade to 3.11.0S

  Conditions: ASR1k router running 3.11.0S Crypto map is configured on one of the interfaces. NBAR is configured via ip nbar protocol discovery on one or more interfaces.

  Workaround: There is no workaround.

- CSCun61454

  Symptom: entPhysicalFirwareRev and entPhysicalHardwareRev is not correct for ASR1000-6TGE/ASR1000-2T 20X1GE

  Conditions: When ENTITY-MIB is queried through SNMP

  Workaround: There is no workaround.

- CSCuo11149

  Symptom: SPA FPD recovery fails for SPA-4XT-Serial on 1RU and 2KP if it is done second time. FIrst time the recovery works fine, but ig the SPA is corrupted again then it is not recovered.

  Conditions: OIR/removal of SPA during FPD upgrade send the SPA into out-of-service state. You can recover it once. But if it again it went to out-of-service state then recovery doesn't works.

  Workaround: Either reload the router or recover the SPA on nightster router.

- CSCup01088

  Symptom: On an ASR 1000 Series Aggregation Services Router configured with DMVPN, CPUHOG messages may be observed after 'clear dmvpn session' is invoked. In certain cases, this may lead to a watchdog timeout and an unexpected reboot of the router.

  Conditions: This issue is observed when a router has a very large NHRP table (10-20k entries or more) with a large number (thousands) of child entries per parent entry.

  Workaround: Reduce the size of the NHRP database through supernetting or similar.

- CSCup57389

  Symptom: traffic through the PPP sessions drops

  Conditions: While testing VRF Lite coexistance with ServiceProvider NAT for LNS

  Workaround: There is no workaround.

- CSCup67354

  Symptom: PLIM error messages are displayed in the log at bootup. Messages appears as: *Jul 1 13:34:18.561 EDT: %CMCC-3-PLIM_STATUS: SIP0: cmcc: A PLIM driver informational error Ysn-LsioTxBc1 - uflwTxafifo2, block 2d count 8c These messages have no impact on function of the unit.

  Conditions: Occurs during reinit of IOSd or basically at reload completion of IOS

  Workaround: There is no workaround.

- CSCup79565

  Symptom: 1NG_NATIVE_ERR:set_autoneg on optics failed:13 error showing up on console of built-in SPA of ASR1001-X's. This error has no effect on working of SFP-GE-T.

Conditions: SFP-GE-T should be inserted in one of the built-in SPA's ports.

Workaround: There is no workaround.

- CSCuq04743

  Symptom: The topology is very simple, where ASR1002-x is connected to 6509-E platform via two 2X1G port channels. One of the port channel is configured as 'ip nat inside' and the other one is 'ip nat outside'. Under normal conditions, traffic enters NAT Inbound port-channel, gets NATed, and exits out the NAT Outbound port-channel. Now when one of the member links of NAT Inbound port channel goes up or down, there is an increase in Misses counter in command output 'show ip nat statistics'. On repeatedly flapping the link, the NAT pool utilization ultimately increases by 1 IP address.

  Conditions: NAT Inbound Port-Channel interface (Member Link Up/ Down Event) causes slight increase in NAT pool utilization and ultimately NAT pool exhaustion.

  Workaround: Stop the traffic for 60 seconds (configured as ip nat timeout), which brings down the NAT pool utilization to 0%.

- CSCuq15567

  Symptom: A router will crash when clearing a crypto peer via "clear crypto sa peer x.x.x.x'. The crash will show that there was an overrun in a block residing within processor memory because the redzone was overwritten by two words %SYS-6-BLKINFO: Corrupted redzone blk 42A629AC, words 1038, alloc 15F9E9D4, InUse, dealloc 8141BF1B, rfcnt 1

  Conditions: This crash was triggered by removal of the crypto peer.

  Workaround: There is no workaround.

- CSCuq17828

  Symptom: When reporting Radius accounting for VPN connections terminated on the ASR using ECDSA certs, we see all zero counters even though we see the real stats on the tunnel.

  Conditions: Only seen when using ECDSA certs

  Workaround: There is no workaround.

- CSCuq43222

  Symptom: media bypass isn't working correctly on IMS call flows.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCuq43357

  Symptom: Although supported, when acting as a responder, ASR1K failed to fill in the RxTimestampf field, when configured in vlan mode.

  Conditions: ASR1K device acting as a responder for Y1731/SLA probes.

  Workaround: There is no workaround.

- CSCuq44810

  Symptom: ASR1002 and SIP10 time-stamp cannot be synced when oir IF G0/0/2 of SIP10. But after 1min SIP10 become synced to ASR1002.

  Conditions: oir cable on IF G0/0/2 of SIP10

  Workaround: There is no workaround.

- CSCuq64148

  Symptom: Ping fails ASR1001-X Builtin ports are connected to ISR 3900/3925/3945 Builtin ports.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCuq85115

  Symptom: ASR1K may reload unexpectedly due to fman_rp crash

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCuq88060

  Symptom: If we configure any listening ports under 'voice service voip', sip as below voice service voip sip no listen-port non-secure 5561 Now if we disable transport of udp from sip-ua as below sip-ua no transport udp then 'show sip-ua register status' show udp as disable, however once we reboot the device(ASR1K), command 'no transport udp' gets enabled and under 'show sip-ua register status' show udp gets enabled.

  Conditions: As soon the router is reloaded the command is getting removed

  Workaround: There is no workaround.

- CSCuq88560

  Symptom: The ASR may experience a CPP crash due to a stuck thread interrupt.

  Conditions: This occurs during normal packet processing.

  Workaround: There is no workaround..

- CSCuq91599

  Symptom: standby-fp reload every 1 hr. and there's pending_aces in show platform wccp f0 and pending-ack in aom. there's also error log and traceback in cpp_cp log file. 09/11 16:53:48.245 [(null)]: (ERR): cpp_wccp_translate_fobj_to_cce_result:failed to get cache-idx from cache-id 1 09/11 16:53:48.249 [errmsg]: (ERR): %CPPOSLIB-3-ERROR_NOTIFY: cpp_cp encountered an error -Traceback= 1#527f976a00f210ebb7bf54f5a71e161d errmsg:7FB760EF9000 121D cpp_common_os:7FB763F16000 DA35 cpp_common_os:7FB763F16000 D934 cpp_common_os:7FB763F16000 19C0E cpp_wccp_svr_lib:7FB7760B5000 D096 cpp_wccp_svr_lib:7FB7760B5000 CCCE cpp_wccp_svr_lib:7FB7760B5000 DED5 cpp_wccp_svr_lib:7FB7760B5000 DBAC cpp_wccp_svr_lib:7FB7760B5000 DA81 cpp_wccp_svr_lib:7FB7760B5000 B996 cpp_wccp_svr_lib:7FB7760B5000 721F cpp_common_os:7FB763F16000 11FCE cpp_comm

  Conditions: first entry of redirect ACL is a deny entry

  Workaround: add a permit entry in the beginning of redirect ACL

- CSCur00220

  Symptom: Can't configure encapsulation with vlan ID 1, while there is no such encapsulation on this interface on an ASR1k with Cisco IOS XE Software, Version 03.10.02.S Similar behavior is also seen in XE-3.13. However, the issue is not seen on 03.08.02.S

  Conditions: Encapsulation dot1q 1 is configured on the service instance

  Workaround: There is no workaround.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.3S

This section contains the following topics:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.3S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.3S.

- CSCto07376

  Symptom: The device reloads when we grant certificates. crypto pki server <> grant all

  Conditions: Configured for crypto

  Workaround: There is no workaround.

- CSCty05208

  Symptom: A Cisco router may crash with the following errors: %ALIGN-1-FATAL: Corrupted program counter 16:43:07 KSA Tue Nov 12 2013 pc=0xXXXXXXXXXz , ra=0xYYYYYYYz , sp=0xZZZZZZZZ 16:43:07 KSA Tue Nov 12 2013: Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0xXXXXXXXXX

  Conditions: The router should have voice calls going through it and VTSP debugs need to be enabled.

  Workaround: Do not enable VTSP related debugs while calls are active through the router.

- CSCtz97771

  Symptom: During regular operations, a router running Cisco IOS release 12.4(24)T and possibly other releases experiences a crash. The crash info reports the following: %SYS-2-FREEFREE: Attempted to free unassigned memory at 4A001C2C, alloc 4180794C, dealloc 417616B0, %SYS-6-BLKINFO: Attempt to free a block that is in use blk 4A001BFC, words 134, alloc 4180794C, Free, dealloc 417616B0, rfcnt 0,

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

  Workaround: There is no workaround.

- CSCua71664

  Symptom: %IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME message is seen during ASR boot.

  Conditions: Normal condition at router reboot.

  Workaround: This is just a cosmetic message. There is no functionality impact.

- CSCua73834

  Symptom: IOS CA issues incorrect rollover identity certificates to its clients; the rollover certificates issued will have an expiry date corresponding to the end-date of the currently active (and soon to expire) CA certificate. Thus, the rollover identity certificate will not be valid after the CA rollover takes place.

  Conditions: The issue is seen only if the clients have sent the rollover certificate request via an IOS RA certificate server.

  Workaround: There is no workaround..

- CSCud94511

  Symptom: Multiple Tracebacks seen.

  Conditions: The tracebacks are seen if a scaled config is present on any atm/gig SPA with POS SPA present in the system. Triggers can also vary from router reload to SIP reload or shut/no shut of large number of tunnels. Triggers increase the load on router processing which interferes with the working of POS SPA and hence tracebacks are seen.

  Workaround: There is no workaround.

- CSCue27980

  Symptom: ASR1k suffers a CPP crash triggered by NBAR.

  Conditions: When NBAR and NAT are both enabled on the same interface there could be some rare conditions which could lead to the crash of the ASR.

  Workaround: There is no workaround.

- CSCue99781

  Symptom: VCD id is assigned to ATM pvc interface once it is created, so after you remove the pvc and re-create it, the previous VCD id as the handle is lost, and you cannot delete the corresponding condition except by removing all the conditions at once.

  Conditions: Delete the interface before you undo the condition debug configuration.

  Workaround: Undo the condition debug configuration.

- CSCuf21181

  Symptom: Failure while deleting the configurations.

  Conditions: The trust point configuration exist after you undo the configurations.

  Workaround: There is no workaround.

- CSCuf47613

  Symptom: Call waiting tone is not played by the DSP if cptone gb is configured when the second SIP call arrives to the FXS port's number.

  Conditions: Issue was found with 15.2(4)M1 and dsapp.

  Workaround: Disable cptone GB.

- CSCuf55934

  Symptom: Router crashes while running NBAR from two sessions.

  Conditions: When NBAR is run from 2 sessions. From first session run "show ip nbar protocol-attribute" and from second session configure "ip nbar custom abcd tcp 4000"

  Workaround: There is no workaround.

- CSCug63959

  Symptom: DSPs are getting hung when receiving an incoming Video call

  Conditions: When making the incoming video call on the AS5400XM gateway, the DSP's channels are not freed up after the call is disconnected. Because of this issue, if there is any incoming call (normal audio call), the calls fail with resource unavailable. We need to reboot the router to clear the DSPs.

  Workaround: Reloading the Router temporarily fixes it.

- CSCug87860

  Symptom: The SIP-5-DIALPEER_STATUS syslog message displays the incorrect dial-peer ID when the status changes. It appears to display the dial-peer interface index instead of the dial-peer tag. There is no way to correlate the dial-peer tag with this number which makes it nearly impossible to identify the affected dial-peer. See the following log excerpt for an example:

  ```
  May 12 15:13:59.101:%SIP-5-DIALPEER_STATUS: VoIPdial-Peer <867> is Busied out May 12
  15:13:59.101:%SIP-5-DIALPEER_STATUS: VoIPdial-Peer <577> is Busied out May 12
  15:14:59.626:%SIP-5-DIALPEER_STATUS: VoIPdial-Peer <867> is Up May 12
  15:14:59.626:%SIP-5-DIALPEER_STATUS: VoIPdial-Peer <577> is Up May 12 15:14:59.626:
  VoIP dial-Peer <856> is Up
  ```

  There is no simple method in IOS to correlate the dial-peer interface index with dial peer tag. Customers are getting above messages on the Syslog, but they are unable to find out which dial peer is affected. We need to change this behavior and should be able to see the dial peer TAG in the syslog message.

  Conditions: Getting this message when SIP OPTION PING is enable on the dial peer.

  Workaround: To find out which dial peer the index number belongs, please enable SNMP trap on router using below command: snmp-server trap link ietf. We can see the index number mentioned in error is mapped to which dial peer using below debug. debug snmp packets

- CSCug90054

  Symptom: The FTP ALG is on by default. The user should be allowed to disable the FTP ALG via configuration.

  Conditions: FTP traffic will go through FTP ALG when the traffic is Natted.

  Workaround: There is no workaround.

- CSCuh47047

  Symptom: An IOS router may fail IKE Main Mode negotiation if the peer device sends both the seconds and kilobytes Life Type with their respective Life Duration attributes.

  Conditions: This condition can occur when an IOS router is the responder for an IKE session, and the peer proposes both seconds and kilobytes Life Duration in its SA proposal.

  Workaround: The workaround is to remove one of the Life Type attributes from the peer device configuration.

- CSCuh56175

  Symptom: One way audio after about 22 minutes with SRTP-RTP interworking.

  Conditions: This symptom is observed in Cisco IOS Release 15.3.2T.

  Workaround: Use one codec on the SRTP to RTP legs. (Make calls all G711 or all G729, not one leg G711 and the other G729)

  Symptom: One way audio after about 22 minutes with SRTP-RTP interworking.

  Conditions: Running 15.3.2T.

Workaround: Use one codec on the SRTP to RTP legs. (Make calls all G711 or all G729, not one leg G711 and the other G729).

- CSCuh73422

  Symptom: ASR1k With MAP-T Configs crashes.

  Conditions: When Ping Initiated to public IPV4 Address, ASR1K crashes with Core dump, and the packet was translated but the packet causes an ICMP error message to be generated, and in some cases of ICMP error generation, the box could crash.

  Workaround: There is no workaround.

- CSCuh87195

  Symptom: A crash is seen on a Cisco router.

  Conditions: The device crashes with gw-accounting and call-history configured. The exact conditions are still being investigated.

  Workaround: Perform the following workaround: 1) Completely remove gw-accounting 2) Disable call-history using the following commands: gw-accounting file no acct-template callhistory-detail

- CSCuh95992

  Symptom: Packets drops with SIP BPA.

  Conditions: This condition is observed with SIP traffic and BPA configured for NAT.

  Workaround: There is no workaround.

- CSCui10109

  Symptom: When provisioned, Fax CM tone is not suppressed on a receiving GW leading to G3 fax-relay failures.

  Conditions: When fax-relay sg3-to-g3 command is provisioned on a receiving gateway(TGW) and T.38 version 0 is provisioned, G3 fax failures are observed due to fax CM tone not being suppressed.

  Workaround: 1. Enable fax-relay sg3-to-g3 suppression on the emitting GW 2. use NSE based modem passthrough 3. Enable T.38 v3 on the emitting and receiving GWs to negotiate T.38 version 3.

- CSCui37509

  Symptom: Sub classification for HTTP content-encoding is not working if we add FNF with export per transaction configurations then remove them and add fnf with export per flow.

  Conditions: HTTP content-encoding with FNF transaction/ connection id configurations.

  Workaround: Add HTTP content-encoding with FNF connection id configurations.

- CSCui39989

  Symptom: PKI fails to validate (sub, peer) cert chain received from IKE.

  Conditions: - PKI hierarchy: root -> sub -> peer - root and sub locally trusted - IKE profile configured with "ca trust-point sub" only - chain-validation from sub to root

  Workaround: See CSCuh73796.

- CSCui48606

  Symptom: 3925 voice xml gateway crashed

  Conditions: vxml configured: vxml tree memory 500 vxml version 2.0

  Workaround: There is no workaround.

- CSCui49644

  Symptom: AToM(Ethernet over MPLS), FP get crash as below:

  ```
  #0 0x092698b4 in *__GI_raise (sig=6) at ../nptl/sysdeps/unix/sysv/linux/raise.c:64 #1
  0x0926b384 in *__GI_abort () at abort.c:88 #2 0x0b2e55b0 in binos_crashdump (stall=0)
  at infra/binos/./src/bassert.c:55 #3 0x0b5a8980 in
  btrace_APPLICATION_FATALED_OUT_LOOK_AT_SYSLOG_OR_TRACEFILE (i=<value optimized out>)
  at infra/btrace/./src/btrace.c:2121 #4 0x0b5a8970 in
  btrace_APPLICATION_FATALED_OUT_LOOK_AT_SYSLOG_OR_TRACEFILE (i=0x0) at
  infra/btrace/./src/btrace.c:2115 #5 0x0b5a8970 in
  btrace_APPLICATION_FATALED_OUT_LOOK_AT_SYSLOG_OR_TRACEFILE (i=0x0) at
  infra/btrace/./src/btrace.c:2115 #6 0x0b5a8b60 in btracev_glob (module_id=94 '^',
  level=112 'p', flags=BTRACE_EMIT_CHECKED, str=0xe191b44 "\n(FATAL): Uplink array
  full", ap=0xbfc26e48) at infra/btrace/./src/btrace.c:2210.
  ```

  Conditions: AToM(Ethernet over MPLS) is configured, link or protocol flapping causes timing issue. It is hard to hit.

  Workaround: There is no workaround.

- CSCui54359

  Symptom: Fax relay is not used when t38 v3 were used for SG3 fax calls. Calls were processed with passthrough mode.

  Conditions: This symptom is observed when SG3 fax on both end and GWs were configured with H323 protocol and T38 v3 fax relay.

  Workaround: Use SIP protocol.

- CSCui59927

  Symptom: Memory Leak observed on the device due to IPSEC causing the free memory to deplete to an extent where box becomes unreachable.

  Conditions: IPSEC scaling being high.

  Workaround: Reduce Scaling of IPSEC sessions.

- CSCui61211

  Symptom: New NAT translations may not be created if there are bindings already created by old translations.

  Conditions: This happens when a NAT translation is unconfigured and re-configured with a new address.

  Workaround: There is no workaround.

- CSCui68757

  Symptom: Enhancement of icmp message rate-limit, for protection of QFP from ICMPv4 Attack.

  Conditions: In IPv4 ICMP, some types of ICMP packets will be generated in data plane. To protect QFP from IPv4 ICMP attack, we need a mechanism to do rate-limit of ICMP packets generated by data plane. There is existing IPV4 ICMP rate-limit mechanism, which is only for ICMP unreachable type. In this fix, we expand this rate-limit mechanism to cover all IPv4 ICMP packets which are generated by data plane.

  Workaround: There is no workaround.

- CSCui72473

  Symptom: When the Traffic is flowing through ATM1xOC3 the rate of flow fluctuates very faster and the counters don't match. <CmdBold> sh int atm0/3/0 | i pack <noCmdBold> Above command can be used repeatedly to check the rate.

  Conditions: The traffic should be flowing through ATM SPA.

Workaround: There is no workaround.

- CSCui73249

  Symptom: NHRP local (no socket) entry gets converted to a socket entry causing matching traffic to be blackholed .

  Conditions: DMVPN phase 3 network.

  Workaround: Configure 'ip nhrp server-only' or remove 'ip nhrp shortcut' on the hub router.

- CSCui76166

  Symptom: TTB Rx info not getting updated on one asr1k router serial interfaces - Bident.

  Conditions: ange of framing type.

  Workaround: Default the interface and re-configure OR OIR Biden.

- CSCui86755

  Symptom: Add local GM ACL on ASR and then remove it. Adding ACL and removing changes the flow priority, that does not work on ASR1K.

  Conditions: When ACL is changed on KS or GM.

  Workaround: If permit ACL is appended to KS ACL or ACL is removed from bottom of KS ACL, then there is no flow priority change, and issue is not observed there. Limitation with this workaround is Group config on KS has only one SA. Also, if Deny ACL is added there are few packet drops observed. Second workaround is manually clear getvpn registration on the ASR1K using "clear crypto gdoi".

- CSCui87023

  Symptom: Enlarge ALG pool limitation.

  Conditions: Use sh plat har qfp ac fea alg mem | in RPC.

  Workaround: There is no workaround.

- CSCui90139

  Symptom: ASR1K : Crypto Route not getting deleted on Responder

  Conditions: ASR1K : Crypto Route not getting deleted on Responder

  Workaround: There is no workaround.

- CSCuj09814

  Symptom: This happens when a NAT translation is unconfigured and re-configured with a new address.

  Conditions: This happens when a NAT translation is unconfigured and re-configured with a new address.

  Workaround: There is no workaround.

- CSCuj12429

  Symptom: GM re-registers to KS because it rejects the re-key from the KS.

  Conditions: Change re-key transport from unicast to multicast on the KS and then issue "crypto gdoi ks rekey".

  Workaround: 1. Do not issue "crypto gdoi ks rekey" on the KS after changing the rekey transport from unicast to multicast and wait for the next scheduled rekey. 2. Force the GMs to re-register after changing the rekey transport method. N / A

- CSCuj13596

  Symptom: Issuing a command crypto key move rsa aaa non-exportable" throws an error, Failed to move keypair aaa to device.

  Conditions: Before issuing the above command, generate the rsa keys with label 'aaa'

  Workaround: There is no workaround.

- CSCuj15540

  Symptom: Alignment errors reported on a router acting as a voice gateway.

  Conditions: This has been seen only on routers passing RTP packets. It could be occurring when voice phone call go through the router, and the router is passing RTP packets.

  Workaround: There is no workaround.

- 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: Gateway is getting below errors while parsing to header 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.

  Symptom: A memory leak is seen in the MALLOCLITE process: PID TTY Allocated Freed Holding Getbufs Retbufs Process 0 0 693368240 200430896 472464592 0 0 *Init* 0 0 0 0 13906024 0 0 *MallocLite* The memory continues to increase there.

  Conditions: This issue is seen on a device running voice services such as MGCP with dial peeers and FXO ports. The exact conditions are still being investigated.

  Workaround: There is no workaround.

- CSCuj30033

  Symptom: ATM interface - SPA-1XOC3-ATM-V2 - shows counters frozen when interface is shut down.

  Conditions: Running traffic over an ATM (SPA-1XOC3-ATM-V2) interface and then shutting down the interface - interface counters remain frozen and does not return to zero.

  Workaround: There is no workaround.

- CSCuj40010

  Symptom: When the primary peer becomes unreachable, the FlexVPN client establishes a tunnel with the backup peer as expected. However, if the primary peer becomes reachable again, the client attempts to build a new tunnel even though it has an existing active tunnel with the backup peer.

  Conditions: The Flex client is configured with multiple peers and peer reactivate is not enabled.

  Workaround: There is no workaround.

- CSCuj45655

  Symptom: When the router has an empty ACL, it fails to deny all traffic.

  Conditions: An empty ACL in the policy.

  Workaround: Ensure that you do not have an empty ACL in the class-map.

- CSCuj62593

  Symptom: Gateway crashes with MALLOCFAIL during ASR/TTS load.

  Conditions: During longevity load for five days, crash is seen almost 61 hours into the load with Cisco IOS Release 15.3(3)M, and almost 12 hours into load with Cisco IOS Release 15.2(4)M5, due to the non-optimal usage of memory.

  Workaround: There is no workaround.

- CSCuj64211

  Symptom: Call starts failing with below messages on the syslog : " FLEXDSPRM-3-TDM_CONNECT failed to connect voice-port (0/0/0) to dsp_channel(0/0/0) " " hwic_t1e1_wic_bp_disconnect: disconnect failed" .

  Conditions: E1 CAS configuration on VWIC3-1MFT-T1/E1 When calls comes on E1 CAS but no channel is available so PVDM3 plays a busy tone and creates a TDM connection EHWIC:44/25-->PVDM:82/05 . After 10 seconds this connection should drop but it does not break; so any new call that comes on EHWIC:44/25 fails and generates the following error : " FLEXDSPRM-3-TDM_CONNECT failed to connect voice-port (0/0/0) to dsp_channel(0/0/0) " " hwic_t1e1_wic_bp_disconnect: disconnect failed "

  Workaround: Reloading the router fixes the issue temporarily .

- CSCuj72215

  Symptom: Input queue of an interface fills up with RTCP traffic. Pings to the router will fail once the input queue is full along with any other traffic that should be process-switched.

  Conditions: The RTCP packets have been found to be associated with H323 but any voice protocol may be involved. The default input queue size is 75 on ISR routers. When the input queue fills up, the size (76) will exceed the max. This may look like an input queue wedge on the surface but for this bug, the packets should be drained once the call is torn down and the socket is removed. The RTCP packets should only be punted to the CPU for processing (and thus hit the input queue) when the RTP session isn't yet established and we don't have a socket. Once this establishment is done, RTCP traffic should be processed in the fast-path.

  Workaround: To alleviate the problems caused by filling up the input queue, the size can be increased with the following command at the interface level, <CmdBold>hold-queue <size> in<noCmdBold>. To stop the issue altogether, RTCP would be need to be disabled by the voice endpoints.

- CSCuj74574

  Symptom: Router acting as a PKI client fails to delete its expired identity and CA certificates after it has rolled over. So, the output of "show crypto pki certificate" shows that the router has two sets of certificates: One set of identity and CA certificates that is current and valid. Another set of identity and CA certificates that is old and expired. Both sets of certificates are bound to the same trustpoint.

  Conditions: The issue is seen primarily when the client router has enrolled to an IOS CA via and IOS RA router.

  Workaround: There is no workaround.. The old set of certificates get deleted eventually upon the next certificate renewal process initiated by the client router.

- CSCuj77998

  Symptom: All packets that need to be encrypted is dropped.

  Conditions: This happens when traffic is flowing for a long duration without any rekey when the crypto sequence number overflows.

  Workaround: Have a shorter rekey interval.

- CSCuj80245

  Symptom: No address prefix flow records is reported when packets get fragmented at Tunnel interface that is enabled with AVC flow monitor.

  Conditions: May occur when packets are fragmented due the maximum packet length limit, called the Maximum Transmission Unit (MTU). When packet size is bigger than the interface MTU, the packet is fragmented and is not monitored by AVC.

  Workaround: Increase the size of the MTU to accommodate larger packets. For example, configure an MTU of 3000 bytes with the following CLI: Device(config)# interface Gig0/2/1 Device(config-if)# mtu 3000

  Workaround: Config bigger "ip mtu xx" or config "ip tcp mss xx" on DMVPN tunnel interface to avoid fragmentation on Tunnel interface.

- CSCuj85993

  Symptom: A Cisco ASR1006 (RP2) running Cisco IOS-XE Version: 03.07.04.S (asr1000rp2-adventerprisek9.03.07.04.S.152-4.S4) crashes after a recent High Availability (HA) fail-over event.

  Conditions: High Availability (HA) fail-over is implemented with RP2 on the Cisco ASR. When a fail-over is initiated to the active RP2 module (for example by removing the active RP2 module), the ASR fails over fine, but once a hold resume is initiated on an existing call (that was preserved from the fail-over), the ASR reboots.

  Workaround: The crash is not observed on IOS-XE version 03.07.03.S.

- CSCuj88820

  Symptom: Router acting as a PKI client continues auto-enrollment to its CA even after the CA certificate has expired.

  Conditions: Client router is configured with 'auto-enroll' under its trustpoint.

  Workaround: Remove 'auto-enroll' from the trustpoint on the PKI client router, or delete the trustpoint in question on the PKI client router.

- CSCuj93565

  Symptom: This Error is seen when performing mdr %SPA_OIR-3-EVENT_DATA_ERROR: SPA OIR event data error - fail.

  Conditions: This issue is seen when SPA takes more time in the configuration replay and does not update the RP about the done message and does not change the State. Then RP's timer expires, crashes the SPA, and reloads the SPA.

  Workaround: There is no workaround.

- CSCuj96005

  Symptom: On CME unity connection SCCP integration, voicemail works properly on SIP phones but MWI on/off does not work after leaving/retrieving voice-mail. MWI works properly for SCCP phones.

  Conditions: CME 9.0 / 15.2(2)T and later and for more than 3 digit DNs.

Workaround: 1. Use 3 digit "voice register dn" 2. Downgrade to CME 8.8 / 15.2(1)T

- CSCuj96893

  Symptom: Cisco router hangs and it stops passing the traffic. Customer needs to reload the router to make it work until it hangs next time. It hangs sometimes once in month.

  Conditions: This issue is seen with more than one router.

  Workaround: There is no workaround.

- CSCul01335

  Symptom: FP may crash

  Conditions: On changing pap limit from 30 to 60 ith traffic.

  Workaround: There is no workaround.

- CSCul02583

  Symptom: Payload verification failed for fax calls; not receiving fax calls.

  Conditions: TGW is sending re INVITE due to not receiving fax calls.

  Workaround: Do not use trancoded call.

- CSCul05056

  Symptom: A Cisco router may crash when configuring NBAR or any other feature which enables NBAR internally. In the crash log file, the crash is shown as a STACKLOW condition. Examples of this are:

  ```
  %SYS-6-STACKLOW: Stack for process Config Probe running low, 0/12000 %SYS-6-STACKLOW:
  Stack for process SSH Process running low, 0/12000 %SYS-6-STACKLOW: Stack for process
  InitializeNbarAPI running low, 0/12000.
  ```

  Conditions: This crash is triggered by enabling NBAR directly or indirectly through another feature. Two such examples are configuring NAT on an interface or configuring NBAR on an interface. For example: (config)#interface gigabitethernet0/1 (config-if)#ip nbar protocol-discovery (config)#interface gigabitethernet0/1 (config-if)#ip nat inside. The router may not crash depending on how the configuration is done. For example configuring the feature over the console will not cause a crash. Configuring the feature over SSH, through FTP, Smart Install, etc though will cause the crash.

  Workaround: A possible workaround may be to configure the feature over the console or through telnet.

- CSCul07137

  Symptom: IFCFG timeouts will happen on Reload or Shut/No shut of Scaled Vlan Port.

  Conditions: Ethernet Line card with Scale QinQ having fixed outer vlan and range of VLAN configuration on reload or Shut/No shut, IFCFG timeouts are observed.

  Workaround: There is no workaround.

- CSCul12835

  Symptom: Crash with CGN/BPA configuration.

  Conditions: IP pool was extended, single bit in BPA was set. Not seen with 1000 users. Issue is seen with around 8000 users.

  Workaround: There is no workaround.

- CSCul13619

  Symptom: When incoming ESP packet has final destination as a local interface on the GM itself (including loopback), the packet is recirculated after decryption causing it to be dropped. If the decrypted packet is only a transit one, for example, it is for a host on a connected LAN, all works as expected.

  Conditions: This issue occurs due to getvpn, ipv6 and use of ingress ipv6 access lists.

- CSCul26686

  Symptom: Scaled vlan qinq configuration on SPA. If the TCAM of SPA becomes full and more qinq vlan is configured, then TCAM_VLAN_TABLE_FULL message is not displayed.

  Conditions: TCAM is full.

  Workaround: For verification whether a new entry has been added or not, check for TCAM entry using CLI on SPA console.

- 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.

- CSCul33043

  Symptom: Unable to get DSP resources for a Transcoded call.

  Conditions: During a mid-call when there is a change in codec or DTMF or Hold and Resume with SRTP-RTP call, then this issue is seen. This is applicable only with LTI transcoding.

  Workaround: There is no workaround.

- CSCul35051

  Symptom: IOS routers behind a NAT/PAT are not sending nat-t keepalives packets whenever the remote end is as well behind a NAT.

  Conditions: Have a VPN connection between a router and headed with both being behind NAT.

  Workaround: Use ISAKMP periodic keepalives (DPD) on the router that is behind the NAT/PAT.

- CSCul37689

  Symptom: With 76xx, customer associates more service instances of each access point to the same bridge domain to create a point to point local switching. Mac-learning in the bridge domain is disabled and therefore NOT limited by number of MAC addresses used. For asr1k, it is expected to implement same behavior under this feature.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCul40500

  Symptom: MD5 is used to sign the PKCS10 embedded in SCEP encrypted message whatever hashing algorithm is configured under the relevant trustpoint or whatever the best hashing algorithm reported by the SCEP GetCACaps message is.

  Conditions: Using SCEP for router enrollment.

  Workaround: There is no workaround.

- CSCul48967

  Symptom: After switch over to standby , IF-MIB count for cvCallVolMediaOutgoingCalls OID is less.

  Conditions: After Switchover.

  Workaround: There is no workaround.

- CSCul50570

  Symptom: A hardware interrupt causes service outage and a micro-code core is generated. This condition puts the router in an inoperable state. This issue would affect bundle interfaces such as MLPPP and GEC aggregate mode.

  Conditions: While processing dynamic reconfiguration events, one of the scheduling node is left in a committed but not forward state. When a flush packet is injected in a flush queue to complete the reconfiguration process, it causes a hardware interrupt when it traverses the node that was left in a non-forwarding state.

  Workaround: There is no workaround.

- CSCul65858

  Symptom: GARP for the NAT-inside-global-address is sent from a non-Active HSRP router. The problem is seen when one of the redundancy pair is reloaded and the interface comes up. Because of the behavior, traffic loss is seen on the NAT traffic. When receiving the GARP, active router shows the duplicate address message like below. %IP-4-DUPADDR: Duplicate address x.x.x.x on GigabitEthernetx/x/x, sourced by xxxx.xxxx.xxxx.

  Conditions: The problem is seen on ASR1K platforms.

  Workaround: There is no workaround.

- CSCul81725

  Symptom: cpp_cp_svr on ESP crashes.

  Conditions: When configuring MLPoEoPTA, the control plane events generated to the data plane cause the data plane to crash if the events are generated in a certain order. This is highly dependent upon timing between the control plane and data plane.

  Workaround: There is no workaround.

- CSCul83097

  Symptom: "dot1q tunneling ethertype 0x88A8" CLI works for port-channel, which crashes FP. This CLI is not supposed to work for port-channel on ASR1k.

  Conditions: There are no known conditions.

  Workaround: Do not use this CLI for port-channel.

- CSCul84373

  Symptom: Tech pubs needs to verify that there is no current documentation referencing the FPGA upgrade process for ASR1002-X utilizing the "upgrade hw-module subslot x/y fpd" command structure. This is replaced with the new "upgrade hw-programmable..." process.

  Conditions: This DDTS brings in the support for upgrading the board FPGA on ASR1002-X using CLI 'upgrade hw-programmable fpga filename bootflash:image.pkg r0'. FPD support for BUILT-IN SPA will no longer be required after this. Therefore, FPD is no longer supported for BUILT-IN SPA.

  Workaround: There is no workaround.

- CSCul86646

  Symptom: ESP reload when ping jumbo packet via gre tunnel

  Conditions: ping packet size > 9800, tunnel mtu>9216 receive side reloads.

  Workaround: Configure IP MTU < 9216 in tunnel.

- CSCul89581

  Symptom: Supervisor is not able to monitor Agent conversation Remotely where CCE-CVP is at higher version and RSM at 9.1(1).

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCul93523

  Symptom: CPP 0 failure Stuck Thread(s) detected.

  Conditions: Setting up about 2.2kps traffic with both nat/non-nat packets.

  Workaround: There is no workaround.

- CSCul94622

  Symptom: On an ASR router with ct3 SPA, Malloc Failures and SPA F/W download failures are seen.

  Conditions: SPA should have many channels configured (> 50 % of its max capacity) and SPA soft reload is done

  Workaround: There is no workaround.

- CSCul96421

  Symptom: Outbound calls over SIP trunk to provider fails.

  Conditions: SIP IP phone (99xx) ------> CME ---------> SIP Trunk --------> ITSP Cisco IOS - 15.3(3)M and 15.4(1)T versions.

  Workaround: Downgrade Cisco IOS version to 15.2(4)M.

- CSCul96947

  Symptom: Traceback appears on standby RP during SPA OIR.

  Conditions: T1 channels are configured. Then a random t1 channel is deleted, and spa soft oir is done.

  Workaround: There is no workaround.

- CSCul98774

  Symptom: ASR1K DSP MIB "cdspCardObjects" are not working after the RP2 switchover happens for various reasons.

  Conditions: When RP switch over happens.

  Workaround: Do a hw-module stop/start on the SPA-DSP cards

- CSCum04528

  Symptom: An ASR 1002-X router might crash and reload writing a core file in the process.

  Conditions: ASR1002-X running NAT with ALG traffic.

  Workaround: There is no workaround.

- CSCum05299

  Symptom: SIP phones not able to dial out when registered to CME 10.0 with IOS version 15.3(3)M1 With output "Ip Trust List Authentication failed for Incoming Request, method = INVITE" when debug ccsip all enabled in the router.

  Conditions: Voice router running in IOS version 15.3(3)M1, with IP address trust list enabled (default configuration) under voice service voip.

  Workaround: * Disable "ip address trusted authenticate" * Add SIP phone IP address to IP trust list. * Downgrade the IOS version.

- CSCum08864

  Symptom: When there is policy changed (either KS or GM) in Pre-PAL, ASR1K used to re-register. The reason is that in TCAM we can't insert or move SA. ACL merge was done in ACE driver, re-registration was triggered from there. Post-PAL, ACL merge intelligence is moved to Control plane, so ACL is changed, it does the change flow priority. The SA is inserted with second priority, ASR1K is not able to handle that.

  Conditions: ACL change on the KS or the GM.

  Workaround: There are 4 Workarounds : 1. Manually clear GetVPN registration on ASR1K using "clear crypto gdoi". 2. If permit ACL is appended to KS ACL or ACL is removed from bottom of KS ACL, then there is no flow priority change, and issue is not observed there. Limitation with this workaround is Group config on KS has only one SA. Also if Deny ACL is added there, few packet drops are observed. 3. EEM script which monitors Rekey Syslog and clears the registration. This is same as workaround 1, but automatically done. disadvantage of this workaround is that Rekey syslog is same during normal rekey and policy change rekey, so with normal rekey also re-registration will happen. Sample EEM script : event manager applet GM_RE_REG event syslog occurs 1 pattern ".*GM_RECV_REKEY.*" action 10 syslog priority warnings msg "EEM trigger workaround for CSCum08864" action 20 cli command "enable" action 30 cli command "clear cry gdoi" pattern "Are you sure you want to proceed" action 40 cli command "yes" 4. The ACL swapped on KS with new ACL and Rekey is done. The ASR1K GM will re-register, there is a small packet drop during re-registartion.

- CSCum11084

  Symptom: WCCP can redirect packets to WAE correctly, but GRE return packets from WAE are droped by ASR1k. "show platform hardware qfp active statistics drop" shows that the drop cause is TunnelUnsupportedConfig.

  Conditions: 1. configure WCCP on PE router of a MPLS VPN network 2. WAE is connected to WCCP router through MPLS VPN network.

  Workaround: There is no workaround.

- CSCum13378

  Symptom: An ASR1K configured as an IPSec endpoint may fail to reassemble fragmented ESP packets . During this failure state, the router will also log %ATTN-3-SYNC_TIMEOUT errors.

  Conditions: UDP packet of a specific size received on the clear side of the ASR is known to trigger this issue.

  Workaround: Use software crypto for large packets received on the clear side by configuring post-frag encryption - crypto ipsec fragmentation after-encryption. This will prevent the ASR from getting into the ATTN_SYNC state.

- CSCum16287

  Symptom: Mobility option is not available for ipv6 access-list configuration. This was disabled by mistake in RSL3.10 and later versions

Conditions: Mobility option is not available in IPV6 access-list CLI.

Workaround: There is no workaround.

- CSCum22661

  Symptom: When a Peer sends a certificate with no CDP, the IOS PKI client will try to retrieve the CRL through SCEP [GetCRL] directed to CA, based on enrollment url value, however in case of enrollment profile [with a valid enrollment url], it complains that the enrollment url is not present.

  Conditions: IOS PKI Client configured with an Enrollment profile, which has enrollment url and authentication url to communicate with the CA using SCEP.

  Workaround: a) configure the enrollment URL under the trustpoint directly instead of using it through enrollment profile or b) configure the CA to embed a CDP in the client certificates [an HTTP Server or SCEP URL]. Peer will need to be re-enrolled afresh. SCEP URL looks like: crypto pki server IOS-CA cdp-url http://10.106.72.139/cgi-bin/pkiclient.exe?operation=GetCRL [Note: Before typing in ? next to pkiclient.exe in the URL above, type Ctrl V]

- CSCum24009

  Symptom: Transfer scenarios fail with ANAT and VCC (No DSP) configured.

  Conditions: Issue is observed for DODO.

  Workaround: Apply DOEO configurations.

- CSCum25232

  Symptom: ASR1K fails to verify a message that is signed using a non-standard RSA key length (2024 for example). The failure is commonly seen during SCEP enrollment or when validating a peer certificate when RSA-SIG is used for phase 1 authentication.

  Conditions: The failure has been observed on ASRs using an integrated ESP.

  Workaround: There is no workaround.

- CSCum29065

  Symptom: Group override does not take effect for interface-config strings. Actual ordering of interface config strings on cloned V-Access does not correspond to the expected order based on AAA settings in IKEv2 profile.

  Conditions: User & group authorization configured in IKEv2 profile.

  Workaround: Move all config-string attributes to a single authorization source (user or group).

- CSCum32910

  Symptom: Chunk manager consumes memory with the allocated memory incrementing on SADB Peering Ch.

  Conditions: Leak when crypto is configured.

  Workaround: There is no workaround.

- CSCum37911

  Symptom: With TBAR enabled, dataplane traffic may be dropped in a GetVPN environment with mixed GMs (ASR and ISR) when there is a change in the NTP clock.

  Conditions: GetVPN Config with TBAR, and NTP clock is changed.

  Workaround: 1) Adjust the NTP server to the current clock or, 2) Re-register the ASR GM with the KS using 'clear crypto gdoi' or, 3) Disable TBAR.

- CSCum40306

  Symptom: Router crashes during call transfer in SRST mode.

  Conditions: Call transfer in SRST mode, including SCCP phones.

  Workaround: There is no workaround.

- CSCum42058

  Symptom: These logs come up every 7 seconds filling up logging buffer: 001628: Jan 4 11:48:18.658 pst: UDLD-3-UDLD_IDB_ERROR UDLD error handling failed to get IDB subblock (rcv) interface: Gi0/0/1.100 -Traceback= 1#bbfe8c0a51f338b185d077b248d1e545 :400000 13C8281 :400000 662BBEC :400000 662A4DE :400000 662A36B

  Conditions: Received UDLD packets with VLAN tag.

  Workaround: There is no workaround.

- CSCum43217

  Symptom: Continuous reloads of an ASR running IOS XE with core files being generated on the router.

  Conditions: ASR running IOS XE with SIP ALG enabled and SIP traffic being translated via NAT.

  Workaround: Remove SIP ALG translations under NAT using the command: no ip nat service sip tcp

- CSCum48124

  Symptom: Occasional crash/traceback and router reload when performing config-replace while both performance monitor/s (e.g. EzPM) and native FNF montor/s are assigned to the same interface.

  Conditions: Performing a config-replace to a clean config (i.e. doesn't assign performance monitors or native FNF monitors), while there are both performance monitor/s (e.g. EzPM) and native FNF monitor/s assigned to the same interface in the current running config.

  Workaround: First un-assign either or both the performance monitors and/or the native FNF monitors before performing the config-replace. In that case, the config-replace works ok.

- CSCum48166

  Symptom: 000175: Oct 30 11:05:09.413 KSA: ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1518: unkn -Traceback= 000176: Oct 30 11:05:09.481 KSA: ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1518: unkn -Traceback= 000177: Oct 30 11:05:09.485 KSA: %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 49595828. -Process= "DSMP", ipl= 0, pid= 304, -Traceback= 11:05:09 KSA Wed Oct 30 2013: TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x4110CA2C

  Conditions: Cisco IOS VoIP gateway experiences an unexpected reload while processing voice calls. This happens when the caller Id is enabled on the FXO port with the voice-port subcommand <CmdBold>caller-id alerting dsp-pre-allocate<noCmdBold> enabled.

  Workaround: 1. Disable the <CmdBold>caller-id alerting dsp-pre-allocate<noCmdBold> command. This will, however, not support caller Id on Old FXO cards where the Caller Id Type is set to Type I (i.e. caller Id reception before connect). 2. Disable the <CmdBold>caller-id enable<noCmdBold> command. This again will not provide the Caller Id feature, but prevent the router from unexpected reloads.

- CSCum49213

  Symptom: ESP crashes.

  Conditions: Using <cmd>debug platform hardware qfp active datapath trace packet</cmd> over an extended amount of time.

Workaround: Use <cmd>debug platform hardware qfp active datapath trace packet</cmd> for short periods of time.

- CSCum49437

  Symptom: ucode crash@ipv4_nat_cgn_mode_dp_rel_mem on changing nat mode

  Conditions: In a scaled setup on changing nat mode

  Workaround: There is no workaround.

- CSCum52078

  Symptom: DOEO call fails for ILBC codec(rtp-nte) with ANAT enabled.

  Conditions: This symptom is observed when following conditions are met: 1. DOEO call 2. ANAT enable at outgoing leg 3. ilbc codec is configure for outgoing leg.

  Workaround: This issue is not observed for DODO.

- CSCum54136

  Symptom: After a KS reload, or a network split or a coop configuration change or any condition that forces a GM to re-register to a different KS in a coop the snmpwalk for object cgmGdoiGmEntry will not return any values for that GM in the previously registered KS.

  Conditions: In a coop if the GM re-registers to a new KS the snmpwalk -v 2c -c wells old_KS_IP 1.3.6.1.4.1.9.9.759.1.2.2.1 command will not return information for that GM on the KS the GM was previously registered at.

  Workaround: There is no workaround.

- CSCum56514

  Symptom: A Cisco router running IOS XE may crash and reload after generating a ucode core file and logs similar to the following:

  ```
  Notice 1531: KRZ: SIP0: pvp.sh: Process manager is exiting: process exit with reload
  fru code Error 1530: KRZ: SIP0: cpp_cp: cpp_cp encountered an error -Traceback= Error
  1529: KRZ: SIP0: pman.sh: The process cpp_ha_top_level_server has been helddown (rc
  69)   Error 1528: KRZ: SIP0: pman.sh: The process cpp_cdm_svr has been helddown (rc
  69)   Informational 1526: KRZ: F0: cpp_ha: Shutting down CPP MDM while client(s) still
  connected   Informational 1525: KRZ: SIP0: cpp_cdm: Shutting down CPP MDM while
  client(s) still connected Informational 1527: KRZ: F0: cpp_ha: Shutting down CPP CDM
  while client(s) still connected Error 1524: KRZ: F0: cpp_ha: CPP 0 microcode crashdump
  creation completed.
  ```

  Conditions: A Cisco router running IOS XE and traffic passing through the NAT path.

  Workaround: There is no workaround.

- CSCum57306

  Symptom: SCB leak seen when the Refer Call with error condition is run under laod.

  Conditions: Refer Call flow which fails.

  Workaround: There is no workaround.

- CSCum60848

  Symptom: Under certain conditions, a DSP will hang in certain call scenarios including REFER passthrough.

  Conditions: Under heavy load.

  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.

- CSCum61622

  Symptom: Traceback may be seen with sip/sunrpc/rtsp/rcmd/msrpc.

  Conditions: Scaled ALG.

  Workaround: There is no workaround.

- CSCum66182

  Symptom: SNMP Query on the object dot3StatsDuplexStatus is shown as unknown.

  Conditions: While testing Ether-Like MIB for ASR1000-6TGE.

  Workaround: There is no workaround..

- CSCum66678

  Symptom: When per-tunnel QoS is configured on a DMVPN hub, the ESP memory may become exhausted due to a memory leak. This could cause the ESP to reload.

  Conditions: If there are a large number of DMVNP spokes and the spokes flap, then memory on the ESP is allocated and not freed. This could cause the memory exhaustion on the ESP and thus case the ESP to reload.

  Workaround: One could monitor the ESP memory usage and if it is getting low, then reboot the ESP during a maintenance window. The command "show platform software memory qfp-control-process qfp act brief | inc I/F" can be used to determine if memory is being consumed due to this issue.

  ```
  Example:    mcp6ru-14#show platform software memory qfp-control-process qfp act brief
  | inc CPP I/F DB             module                  allocated     requested
  allocs        frees
  ------------------------------------------------------------------------------    CPP
  I/F DB              128           48            5             0    <== normal
  condition is 5 allocs at bootup that is not freed    (one spoke flapped)      CPP I/F
  DB              8172          8076          6             0    <== 1 additional alloc
  of 8028 (2k spokes in network) - with this bug, this memory is not freed
  ```

- CSCum67150

  Symptom: Configure MAC Accounting both ingess and egress directions. Do a "no ip accounting on the egress"

  Conditions: Check for MAC accounting updates on the RP, the ingress side MAC update stop. The issue also happens other way round when Ingress config is removed, the Egress accounting stops working.

  Workaround: Need to Reconfigure the Mac Accounting for intended direction.

- CSCum68074

  Symptom: Many packets are dropped for NatIn2out cause.

  Conditions: PAT, interface overload.

  Workaround: PAT pool overload.

- CSCum68287

  Symptom: GM reloads unexpectedly when enabling V6-crypto map on an interface with VRF-aware GDOI configs on the latest XE3.12 throttle images.

  Conditions: Seen on all ASR platforms, with latest XE3.12 throttle base images. This is 100% reproducible and extremely service impacting. This happens only when you enable "ipv6 crypto map" which has a local GM deny ACL associated with it. Enabling v4-crypto map is fine.

  Workaround: Do not use the local GM ACL for IPV6 crypto map. This may not be a feasible workaround in the field.

- CSCum69152

  Symptom: SIP SRST and adding more than one alias commands, only 'alias 1' command creates a dial-peer. voice register global mode srst system message SRST Active max-dn 20 max-pool 20 ! voice register pool 1 id network 1.1.1.0 mask 255.255.255.0 alias 1 1111 to 4444 alias 2 2222 to 4444 voice-class codec 1 Only the alias 1 dialpeer gets created and calls to that extension will work (as long as you also have the correct translation rule as per docs).

  Conditions: CME in SIP-SRST mode.

  Workaround: Use translation-rules to achieve this behavior.

- CSCum69887

  Symptom: When there is SIP address in the message. NAT cannot handle the tcp sequence properly with LDAP ALG after pdu size has changed. NAT will not handle the delta value for the right ack message but thereafter messages, which may cause mis-acked message flows between two endpoints. Currently only seen with netmeeting.

  Conditions: Send LDAP traffic with empty comment item in LDAP ALG.

  Workaround: There is no workaround.

- CSCum71485

  Symptom: Increasing number of TEK generated every 30 secs.

  Conditions: 1. Change the Group Identity on the Secondary KS causing encryption failure, Change the Group Identity on the Primary KS. All the GMs are deleted from the KSs. 2. Restore the Secondary Key Server. Wait for it to come up as Primary for the Group : GETVPN-GROUP-1 3. Restore the Primary Key Server with Group : GETVPN-GROUP-1 4. This is creating a new TEK policy every 30 sec from the newly elected Primary Key Server KS2. The sequence number for rekey remains 1. 5. KS1 is restored to be the primary role. 6. After the existing TEKS from the KS2 are expired it behaves normally.

  Workaround: There is no workaround.

- CSCum73167

  Symptom: LDAP ALG will encode the packet even there is no need to translate them, this will not impact function, but it is not necessary.

  Conditions: LDAP ALG will encode the packet even there is no need to translate them.

  Workaround: Will not impact function.

- CSCum73445

  Symptom: cpp_cp_svr crash.

  Conditions: Problem has been intermittently seen when tearing down bundle type interfaces such as MLPPP and MLFR.

  Workaround: There is no workaround.

- CSCum75385

  Symptom: "show platform hardware qfp active datapath utilization" displays wrong data. When high priority traffic (ip precedence 6,7) is sent, the counters against "Input Non-Priority" rows increment. When low priority traffic (ip precedence 0,1,2,3,4,5) is sent, the counters against "Input Priority" rows increment.

  Conditions: This can occur when using esp100.

  Workaround: There is no workaround.

- CSCum78260

  Symptom: ASR1K GM1 did not have 1 recovery registration to group GDOI_GROUP_1.

  Conditions: Issue is newly seen only in ASR routers and not in ISR.

  Workaround: There is no workaround.

- CSCum78930

  Symptom: The ICMPv6 error packet (too-big packet) with icmpv6 echo reply as payload is dropped by ZBFW.

  Conditions: If the intermediate hosts generate icmpv6 error packets with icmpv6 echo reply as pay load without properly fragmenting the packets as per the mtu of the v6 packet flow, such icmpv6 errors packets are dropped.

  Workaround: Adjust the mtu of the v6 pack flow so that packets, especially the icmvp6 echo reply does not generate an error.

- CSCum79817

  Symptom: "488: Not acceptable media" message seen for DOEO ANAT calls with ILBC codec.

  Conditions: This symptom is observed when following conditions are met: 1. DOEO 2. ANAT calls 3. ILBC codec (Did not test for other codecs).

  Workaround: This symptom is not observed for DODO.

- CSCum80300

  Symptom: ASR1k running XE3.10 may crash in RP on executing the CLI "show crypto session".

  Conditions: More than 1000 crypto sessions and executing the cli "show crypto session".

  Workaround: There is no workaround.

- CSCum81717

  Symptom: 183 session progress is blocked by the sip gateway.

  Conditions: 183 session Progress is received with SDP and Require:100 rel header and "block 183 sdp absent" is configured.

  Workaround: There is no workaround.

- CSCum83957

  Symptom: A router may crash due to a bus error when running "show sccp connections sessionid".

  Conditions: This has been observed on a 3900e router running 15.3(2)T. SCCP features are configured on a router.

  Workaround: There is no workaround.

- CSCum88058

  Symptom: The following CLI does not work on ELC:- 1. no ip mac accounting ingress 2. no ip mac accounting egress.

Conditions: Configure the MAC accounting for any direction. Issue the corresponding "No CLI". Although No Visible Impact to the operations of the system, a required cleanup operation is not performed.

Workaround: There is no workaround.

- CSCum94408

  Symptom: Intermittently, if a root's CRL to validate Sub does not get downloaded [Internal or External failures], and the CRL by Sub gets downloaded, the following message is seen: [Debug crypto isakmp and Debug crypto pki m/t/v/c] ISAKMP (35845): adding peer's pubkey to cache ISAKMP:(35845): processing SIG payload. message ID = 0 %CRYPTO-3-IKMP_QUERY_KEY: Querying key pair failed.

  Conditions: This symptom occurs in Cisco IOS configured with the IKEv1, Authentication mode RSA-SIG [Certificates]. PKI Infrastructure is as follows: Root -> Sub -> ID - Root and Sub Trustpoint have "revocation-check crl none". - Sub has "chain-validation continue Root".

  Workaround: Disable revocation-check and Chain-validation under Sub Trustpoint.

- CSCum96156

  Symptom: IOS will fail to match the certificate map intermittently.

  Conditions: IOS PKI using certificate maps, to authorize the Peer certificates or override CDP. In this case: - if a certificate map is written on a PC, with upper case letters in them: Ex: crypto pki certificate map HR-Users 10 subject-name co ou = HR-Users - and this is a part of the configuration that is merged with the running config through IOS file-system [directly from flash or FTP/TFTP/HTTP etc], IOS retains the upper case letters. [contrary to certificate maps written through CLI, always converts everything to lower case letters].

  Workaround: A) - copy the certificate maps [that have upper case letters in them] to a notepad - remove the certificate maps [that have upper case letters in them] - paste the certificate maps, through IOS CLI - wherever these cert maps were being called, they will stay intact, and this change will take effect immediately or B) - The certificate map needs to enter IOS in a manner that IOS would insert it if you were to enter it in a CLI I.e. Make sure the external config generators generate the certificate map in such a way that everything is in lower case, and it has white spaces between DN OID, '=' and the value.

- CSCum99077

  Symptom: fman_rp process crash. RP card reload.

  Conditions: When routing loop occurs in network and caused massive routing information update, an internal logic error may be triggered.

  Workaround: Avoid routing loop.

- CSCun00783

  Symptom: Channel group with link id > 4 is not configurable.

  Conditions: While configuring the vlan based load balance.

  Workaround: Use only link id 1-4.

- CSCun01152

  Symptom: An IOS-XE router may reload unexpectedly when zone-based firewall is configured.

  Conditions: Zone-based firewall is configured. May be dependent on many active MSRPC sessions.

  Workaround: There is no workaround.

- CSCun04417

  Symptom: GTP U packet forwarding capability is downgraded.

  Conditions: 1 firewall session.

  Workaround: There is no workaround.

- CSCun08855

  Symptom: ASR router crash with iosd punting packet to port-channel with ERSPAN configured on the router.

  Conditions: Port-channel and ERSPAN configured on the router

  Workaround: There is no workaround.

- CSCun09640

  Symptom: The following errors are seen when adding a child policy to a parent policy while configuring hierarchical QoS. %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp: cpp_cp encountered an error %CPPOSLIB-3-ERROR_NOTIFY: F0: fman_fp_image: fman-fp encountered an error %PMAN-3-PROCHOLDDOWN: F0: pman.sh: The process cpp_ha_top_level_server has been helddown (rc 69) %PMAN-3-PROCHOLDDOWN: F0: pman.sh: The process cpp_cp_svr has been helddown (rc 134) This can result in a ESP (F Fabric) reload, causing a traffic outage.

  Conditions: 1. An interface with a service-policy applied. 2. Replacing the child policy on the parent hierarchical policy applied to the interface.

  Workaround: Remove the policy from the interface before making the changes to the child/parent policy then reapply the policy to the parent. OR If you issue the no command to remove the child policy from the parent and then query for pending configuration objects using the "show platform software object-manager fp active statistics" command to make sure there are no pending objects, then issue the service-policy to add the new child policy to the parent, you will not see the ESP crash.

- CSCun09753

  Symptom: Ping failed with input errors when HDLC interf MTU set/removed.

  Conditions: 1. set MTU (more than 2950) on HDLC interface, then remove MTU; 2. ping failed to peer HDLC interface.

  Workaround: There is no workaround.

- CSCun10918

  Symptom: Issue PPP subscribers cannot be terminated in ASR1K, due to object locked.

  Conditions: EVSI Delete Errors: Out-of-Order 0, No dpidb 0, Underrun 0, VAI Recycle Timeouts 90215 =======> large number of VAI recycle timeouts EVSI wrong dpidb type errors 0 EVSI Async Events: Total 92754, HW error 88050 =======> large number of HW errors as well.

  Workaround: Remove QOS of the ppp.

- CSCun13800

  Symptom: VG224 responds with a different RTP port each time for multiple StationPortReq messages from CUCM for the same call. Seen in 15.1(4)M7.

  Conditions: CUCM sending multiple StationPortRequest to VG VG224 registered SCCP to CUCM.

  Workaround: The same will be fixed 15.1(4)M8 and the VG will respond with same RTP port for multiple StationPortReq message for the same call.

- CSCun13999

  Symptom: Under interface superscription condition, we might see the following error message on router console: %CMCC-3-PLIM_STATUS: SIP0: cmcc: A PLIM driver informational error TXMC0 - txmcBufferOverflow, block 1f count c8.

  Conditions: When "fair-queue" is used in QoS policy-map, under interface subscription condition the flow-control between BQS and SPA might excommunicate, hence the error message is printed. %CMCC-3-PLIM_STATUS: SIP0: cmcc: A PLIM driver informational error TXMC0 - txmcBufferOverflow, block 1f count c8.

  Workaround: There is no workaround.

- CSCun17558

  Symptom: COS markings not seen properly on the dot1q interface.

  Conditions: The issue is seen if all these following conditions are met: 1, MPLS packets with fragment happened in data plane on the dot1q interface.

  Workaround: There is no workaround.

- CSCun20274

  Symptom: Standy RP source is not participating in clocking selection.

  Conditions: We must have the below specific netclk config on the ASR1k and need to perform RP-switchover. "network-clock select 1 BITS R0 <T1/E1> <Framing>" "network-clock select 2 BITS R1 <T1/E1> <Framing>".

  Workaround: Remove and re-apply the stby-network-clk Source with different framing. This bug CSCun20274 is specific to below combination. 1. You must configure NETCLK config on ASR RP-bits [Active and Standby RP bits] 2. Router must be capable of hardware redundancy. If the Customer is not using Netclk feature, you can ignore this.

- CSCun20279

  Symptom: At uRPF loose mode, the suppress drop counter on ASR1K will count packets even in case the packets are symmetric flow. ASR1K should not count symmetric flow packets as sdrop at uRPF loose mode.

  Conditions: uRPF loose mode.

  Workaround: There is no workaround.

- CSCun20776

  Symptom: An ASR router may display the following logs continuously:

  ```
  IOSXE-3-PLATFORM R0/0: kernel: Error -5 IOSXE-3-PLATFORM R0/0: kernel:
  /auto/mcpbuilds14/release/03.11.00.S/BLD-03.11.00.S/os/linux/drivers/binos/ds31408/ds3
  1408_driver.c:ds31408_ioctl (line 522): IDT_IOCG_INTR_STATUS failed, status -5
  IOSXE-3-PLATFORM R0/0: kernel: bullseye_altera_spi_rd_guts: Receiver-overrun error:
  Status = 0xffffffff IOSXE-3-PLATFORM R0/0: kernel:
  /auto/mcpbuilds14/release/03.11.00.S/BLD-03.11.00.S/os/linux/drivers/binos/ds31408/ds3
  1408_pll.c:ds31408_get_intr_status (line 76): DS31408 Read failed for 56.
  ```

  Conditions: An ASR router running IOS XE with traffic flowing through it.

  Workaround: There is no workaround.

- CSCun22771

  Symptom: An ASR 1002-X router might crash and reload writing a core file in the process.

  Conditions: ASR1002-X running IOS XE in a NAT-HA B2B scenario.

  Workaround: There is no workaround.

- CSCun24965

  Symptom: On the ASR1000 series router configuring a QoS service policy using the service-fragment type, the shaping value is not correct.

  Conditions: A QoS Service Policy is applied using the service-fragment keyword, the shaped value is not correct.

  Workaround: There is no workaround.

- CSCun26943

  Symptom: In an INTRA-box redundancy configuration, the STANDBY FP and ACTIVE FP may not be syncing dataplane HA records robustly. The easiest way for the customer to recognize if this *might* be happening is by examining the output of the show platform hardware qfp active system intra and the show platform hardware qfp standby system intra CLIs. If the output shows the counters " rx dropped" and/or "retx" continuously incrementing, then this problem may have been encountered.

  Conditions: DUAL FP systems with stateful HA features such as NAT configured.

  Workaround: There is no workaround.

- CSCun28965

  Symptom: 'show ip nat translation filter range [inside | outside] [local|glocal] <start-ip> <end-ip>' was not filtering the output as per the range specified.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCun30321

  Symptom: Major alarm observed on ASR1001.

  Conditions: After upgrade to XE3.10.2.

  Workaround: There is no workaround.

- 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.

- CSCun31359

  Symptom: 3900 running 15.3(1)T.

  Conditions: Memory corruption is happening while processing the sip-profile modify rule for History-Info header.

  Workaround: -Using history-info passthru feature (voice service voip -> sip -> history-info) -Using header pass-thru feature.

- CSCun32035

  Symptom: Configured following features as part of IWAN performance testing for UTAH platform 1. AVC 2. PFR 3. QoS 4. Appnav WAAS 5. DMVPN 6. Crypto. Make sure DMVPN and MPLS tunnel are up and performance monitor, WAAS and crypto are enabled for these tunnels. Router crashes with traffic profile.

  Conditions: Traffic profile includes, voice http media traffic. Crash is seen as soon the traffic is initialized at less than 15% of load.

  Workaround: There is no workaround.

- CSCun35149

  Symptom: Enable performance monitor on local switching interface

  Conditions: Two interfaces are connected as local switching.

  Workaround: There is no workaround.

- CSCun36785

  Symptom: ASR1002X production router acting as WAN-Aggregator reloaded unexpectedly after pushing the AVC configuration from Cisco Prime infrastructure through SSH session. The config push was successful onto the box, and the flow statistics were exported properly to the PI. However after Half an hour, the router reloaded with CPP mcplo_ucode crash and fman_fp crash The box is configured with IKEv2 DMVPN and basic NAT, along with BGP and EIGRP. We had around 4 static NHRP tunnels from different branch locations terminating onto this box. All traffic from the branches were encrypted, decrypted on this router, and NAT was applied to the decrypted traffic before sending it out of the Port-channel interface towards production network.

  Conditions: Seen on ASR1002X running CCO IOS-XE version 3.10.1 The Crash has occurred only once. Currently AVC configs has been backed out and the router is stable. This is seriously affecting the AVC deployment on the network

  Workaround: There is no workaround.

- CSCun37698

  Symptom: An ESP might crash.

  Conditions: The device has NAT and WCCP configured. It looks like WCCP fails to setup the output interface correctly. This leads to NAT accessing a bad location in memory which causes a crash. The exact conditions are still being looked at.

  Workaround: There is no workaround.

- CSCun40507

  Symptom: ECDSA Pairwise consistency test is missing from ic2m_rel3 code.

  Conditions: ECDSA Pairwise consistency test is missing from ic2m_rel3 code.

  Workaround: There is no workaround.

- CSCun44581

  Symptom: FOs of CFT features might not be released in case the feature has unregistered from CFT before the flow aged.

  Conditions: Feature of CFT (Stile,FNF,FME,CENT..) that allocated FO in the flow and then un-registered from CFT (i.e feature has been disabled) while another feature is still registered to CFT, the FO of that feature won't be released.

  Workaround: Stop traffic before disabling the feature or reload.

- CSCun47175

  Symptom: Memory leak seen during CC OIR scaled config - rem and insert CC check "show memory debug leaks" CLI output.

  Conditions: No Specific reproduction step, as the issue is seen only once. - memory leak seen during CC OIR scaled config - rem and insert CC.

  Workaround: There is no workaround.

- CSCun48994

  Symptom: The CP process crashes while collapsing a hierarchy layer node that had once exceeded 4000 entries. The collapse occurs when the number entries falls below 4000.

  Conditions: This problem occurs while collapsing a node that had once exceeded 400 entries. The problem is specific to MLPPP, MFR and GEC aggregate because these features require notification when a schedule ID changes. The schedule ID changes when a scheduling node is reconstructed. The issue hit when the operation involves both the flushing and SID notification.

  Workaround: There is no workaround.

- CSCun49087

  Symptom: ASR1002x crash.

  Conditions: Duty cycle testing with a lot of negative events in DMVPN setup.

  Workaround: There is no workaround.

  Symptom: ASR1002x crash.

  Conditions: Duty cycle testing with a lot of negative events.

  Workaround: There is no workaround.

- CSCun50243

  Symptom: When CED/ANSam/2100Hz answer tone is detected in the early media phase of the call, the gateway does not switchover and starts sending distorted audio to the originating fax. Fax transmission fails.

  Conditions: modem passthrough nse codec g711ulaw is used as the fax protocol. Fax -> VG224 --SCCP--> CUCM -SIP--> 3945 GW--ISDN T1 PRI-->PSTN 3945 IOS: 15.1.4M5 VG224:15.1.4M2.

  Workaround: - Use 'progress_ind' to strip PI=8 if the Early Media is opened via an ISDN ALERTING message: (config-dial-peer)#progress_ind alert strip - Check with Carrier if they can avoid opening early media for Fax/Modem calls. Early media cut-through for fax/modem calls is not supported. The expected flow transition to the Voice Band Data (VBD) mode or modem up-speed as we commonly call it, requires a VoIP call to be first established (call is connected). It is then, when normally a 2100Hz answer tone is detected as the media flows in both direction and triggers Voice Band Data (VBD) upspeed.

- CSCun51932

  Symptom: Incorrect internal and external Dialtone for CPTONE DE.

  Conditions: Cptone DE is configured under FXS ports

  Workaround: Step1: Router# test voice tone DE dialtone 1 425 0 -200 -200 -240 0 0 0 65535 0 0 0 0 0 0 0 Step2: Router# test voice tone DE 2nd_dialtone 1 425 0 -200 -200 -240 0 0 0 200 300 200 300 200 800 0 0 Step3: shut the voice-port Step4: Unshut the voice port

- CSCun55310

  Symptom: An ATM-port might show input-errors of type overrun.

Conditions: They get counted so, because they hit an on-demand AutoVC, where the nature of the packets (for example ILMI or BPDU) should not raise the VC.

Workaround: The concerning VC could be configured as permanent or the packets should be prevented on neighbor device as it is seen as unwanted or unexpected traffic.

- CSCun56044

  Symptom: When there is a small network flap, ASR sends below traps to the Monitoring tool. 1. When the adjacency goes down; 13.2.2014 04:25:08.430 CISCO-SESS-BORDER-CTRLR-EVENT-MIB Enterprise specific=3 enterprises.cisco.ciscoMgmt.ciscoSessBorderCtrlrEventMIB 47 csbAlarmSubsystem=signaling csbAlarmSeverity=0 csbAlarmID=47 csbAlarmTime=Thu Feb 13 02:25:08 UTC 2014 csbSBCServiceName=lah1-sbc1 csbAdjacencyState=detached csbAdjacencyType=sip csbAdjacencyName=Savonvoima-Lync csbAlarmDescription=This alarm is generated when an adjacency is attached to or detached from the sbe.

  Conditions: ASR Version: asr1000rp1-adventerprisek9.03.11.00.S.154-1.S-std.bin "snmp-server enable traps sbc adj-status" is added in the ASR configuration.

  Workaround: There is no workaround.

- CSCun58672

  Symptom: VTCP does not send tcp segments according adjustment mss.

  Conditions: tcp sync with mss 1460 from interface B, and Interface A sent out sync with mss 1390 tcp segments (tcp payload 1390) come from interface A observed tcpsegments with tcp payload 1460 sent out via interface B.

  Workaround: There is no workaround.

- CSCun62273

  Symptom: MODEM Relay cannot be configured on VG224.

  Conditions: VG224 used for modem relay calls.

  Workaround: There is no workaround.

- CSCun69811

  Symptom: Actually customer on active box would only like to "no activate" a single delegate registration entry below. subscriber sip: 999999@site.com sip-contact sip: 001999999999@10.0.0.1 adjacency CUCM-llab delegate-registration sip:test.site.com adjacency PSTN-lab-SIP-CONNECT-test-lab profile SIP-CONNECT_TIMERS activate

  Conditions: Sessions are deactivated and the stand-by router crashes.

  Workaround: "no activate" command must be executed at the "delegate-registration" sub section. This will prevent the deactivation of the sessions.

- CSCun78318

  Symptom: ACLs applied to the mgmte do not work on the new active RP after a RP switch over.

  Conditions: After a RP switch over as the old standby RP becomes the new active RP.

  Workaround: Remove then reapply the ACLs to the mgmte on the new active RP.

- CSCun82649

  Symptom: Under certain conditions the standby FP may crash when NAT BPA is configured.

  Conditions: Under certain conditions the standby FP may crash when NAT BPA is configured.

  Workaround: There is no work around for this.

- CSCun83231

  Symptom: After sub package ISSU operation is performed, ELC does not come up and following error messages are seen. *Mar 19 23:10:10.607 PDT: %PMAN-0-PROCFAILCRIT: SIP1: pvp.sh: A critical process mcpcc_lc_ms has failed (rc 127) *Mar 19 23:10:10.865 PDT: %PMAN-5-EXITACTION: SIP1: pvp.sh: Process manager is exiting: critical process fault, mcpcc_lc_ms, cc_1_0, rc=127

  Conditions: Issue is specific to ELC. Issue is specific to sub package upgrade. Issue is seen across all releases that support ELC. ELC means ASR1000 Ethernet Line Cards - These are: ASR1000-2T 20X1GE and ASR1000-6TGE line cards.

  Workaround: Consolidated upgrade can be performed.

- CSCun85761

  Symptom: L2 frame check failure when payload length increase with ldap alg.

  Conditions: Steps: ====== translate sipAddress into longer address length.

  Workaround: There is no workaround.

- CSCun85947

  Symptom: When there is a dialer interface getting dynamic IP, SIP control and media binding is failing with that interface.

  Conditions: IOS should be 15.1.2T or later (to configure binding at dial-peer level)

  Workaround: Configure static IP for the dialer interface.

- CSCun87352

  Symptom: The ESP module in an ASR1000-series router may reload unexpectedly. In systems with an integrated ESP, such as the ASR1001 and ASR1002-X, this may result in a reload of the entire chassis.

  Conditions: This has been observed on an ASR1001 running 15.3(3)S2 (IOS-XE 3.10.2S). Flexible NetFlow is enabled. Exact conditions currently unknown.

  Workaround: Disabling Flexible NetFlow may prevent the crash.

- CSCun87685

  Symptom: ASR1006/15.4(1)S crashed while adding port and host specific deny statements on specifc lines for the WCCP-Redirect ACL.

  Conditions: Adding port and host specific deny statements on specific lines for the WCCP-Redirect ACL.

  Workaround: There is no workaround.

- CSCun89036

  Symptom: Traceback when IPV6 traffic is transiting through ATM sub-interface.

  Conditions: Configuration of "atm route-bridged ipv6" configured at ATM sub-interface level.

  Workaround: There is no workaround.

- CSCun90736

  Symptom: QFP crash.

  Conditions: Basic GTP tunnel setup.

  Workaround: There is no workaround.

- CSCun91199

  Symptom: NAT ALG not translating in case of multiple sip address in SDP.

  Conditions: Sip invite message containing oline and cline with different addresses and both need translation dynamic nat with acl configured.

  Workaround: Simplify the ACL associated with NAT mapping configuration.

  Symptom: NAT ALG not translating in case of multiple sip address in SDP.

  Conditions: Sip invite message containing oline and cline with different addresses and both need translation dynamic nat with acl configured.

  Workaround: There is no workaround.

- CSCun92199

  Symptom: Ucode crash with sip traffic.

  Conditions: After doing couple of events like redundancy reload multiple times and with SIP traffic

  Workaround: There is no workaround.

- CSCun96969

  Symptom: The ASR1002 running IOS_XE 3.7.0 (15.2(4)S) crashed after a configuration change inf FNF. %FMANRP_NETFLOW-3-INVALIDFLOWDEFCPP: CPP Flow definition can not be created 1 Mar 19 12:18:33 lns3 1596693: -Traceback= 1#fcbfdf6899eea283341cebf8c5320ad1 :10000000 6FBFE8 :10000000 6FC394 :10000000 5B9F54C fnf_config:9DB4000 1B270 fman_rp:ED4B000 1D0 764 fman_rp:ED4B000 1D0954 :10000000 3326E78 :10000000 330110C Mar 19 12:18:33 lns3 1596694:

  Conditions: An FNF record that includes one of the following key/non-key fields configured along with an extracted field will trigger the trace back. one or more fields derived from the below: match/collect routing source/destination [peer] as [4-octet] along with an extracted field such as : collect application http host Example: flow record test-rec match routing source as 4-octet collect application http host flow monitor test-mon record test-rec.

  Workaround: There is no workaround.

- CSCun97294

  Symptom: Core dump won't be generated after kernel crash in x86_64 platforms.

  Conditions: Kernel crash.

  Workaround: There is no workaround.

- CSCun97966

  Symptom: txnpMaxMtuExceeded message seen when packets are sent to crypto.

  Conditions: When nated packet is sent to crypto, txnpMaxMtuExceeded is seen for some packets. Applicable only for asr1k-2x, ESP100 and ESP200.

  Workaround: There is no workaround.

- CSCun99766

  Symptom: Router crashes while making changes to AppNav policy-map and/or class-map.

  Conditions: Multiple AppNav controllers are used. Sessions had been created and can be seen using "show service-insertion statistics sessions". AppNav policy-map and class-map is modified when live traffic are being redirected by AppNav. Policy-map / class-map change resulted in mismatch between AppNav Controllers.

Workaround: When using AppNav Controller Group with multiple ACs, avoid changing policy-map / class-map when there are active sessions present (use "show service-insertion statistics sessions")

- CSCuo02558

  Symptom: Crash in cpp_cp_svr when executing 'show platform packet-trace packet all'.

  Conditions: Crash can only occur when executing 'show platform packet-trace packet all'.

  Workaround: Display a single packet at a time using 'show platform packet-trace packet <num>' instead of using 'all'.

- CSCuo05333

  Symptom: Bogus counter reported by crypto engine.

  Conditions: When SHA384 algorithm, bogus counter is seen during show platform hardware crypto-device context output.

  Workaround: There is no workaround.

- CSCuo07408

  Symptom: One-way audio when using SRTP when the master key begins with 00.

  Conditions: Using any release that contains the fix for bug: CSCtj15884.

  Workaround: Put the call on hold and then resume. This will renegotiate the keys and restore two way audio.

- CSCuo09390

  Symptom: ASR1K crash on netflow configuration change.

  Conditions: When all current CVLA client features are unconfigured and registration happens from beginning for a new client, allocating initial chunk memory fails. Note: The following are the ASR1k features capable of using CVLA currently, FNF NBAR CFT OneFW MCP Connected Enterprise (CENT) CPP Flow Metadata (FMD) CPP Flow Metric Engine (FME) AppNav vPath Flow Object/Service Controller

  Workaround: Do not unconfigure every existing CVLA feature at once. Leave at-least one feature configured so that when a new feature is configured, CVLA does not have to allocate the initial chunk memory again. Leaving out atleast one CVLA feature configured will avoid the crash. Note: The following are the ASR1k features capable of using CVLA currently, FNF NBAR CFT OneFW MCP Connected Enterprise (CENT) CPP Flow Metadata (FMD) CPP Flow Metric Engine (FME) AppNav vPath Flow Object/Service Controller To view the list of features currently configured on your box to use CVLA, use the following show command "sh plat hard qf a infra cvla client handles"

- CSCuo20090

  Symptom: The saved ACLs applied to the mgmte from startup-config may not work after system reload.

  Conditions: After system reload.

  Workaround: Remove then reapply the ACLs to the mgmte after system reload.

- CSCuo26237

  Symptom: Trans on active and standby are not synced.

  Conditions: With AT&T set up

  Workaround: There is no workaround.

- CSCuo33697

  Symptom: ISSU breaks when we do a upgrade/downgrade from xe310 to xe312/xe313. Only seen when we do ISSU sub package upgrade from xe310 to xe312/xe313 ISSU sub package downgrade from xe312/xe313 to xe310 Another ISSU upgrade/downgrade cannot see this issue.

  Conditions: A definite spa type has different TDL enums across xe310 & xe312/xe313 which is causing ISSU breakage. ISSU upgrade/downgrade from all versions of xe310 to xe312 are discussed of them, we list out which are the ones that are affected because of this bug. xe3.10.0 <--------> xe3.10.1 No issue xe3.10.0 <--------> xe3.10.2 No issue xe3.10.0 <--------> xe3.10.3 No issue e

  Workaround: Only do a full package upgrade when you are upgrading/downgrading to/from above combinations.

- CSCuo38164

  Symptom: Traceback and log error noticed.

  Conditions: While initiating H323 call with SBC feature.

  Workaround: There is no workaround.

- CSCuo47620

  Symptom: Memory leaks during session tear down. The following error message is logged to the console after the address space limit is exceeded. on standby-ESP: %CPPDRV-4-ADRSPC_LIMIT: F1: cpp_cp: Address space limit.

  Conditions: When a policy with conditional policing enabled is removed, the traffic manager leaks 16 bytes of resource DRAM per target. The leak increases exponentially when tearing down more than 20000 PPP sessions. Though the system may still be in operation, the control plane performance becomes severely degraded causing subsequent configuration processing to become very slow.

  Workaround: There is no workaround.

- CSCuo55508

  Symptom: A cpp-ucode crash is encountered.

  Conditions: Using packet-trace to trace packets in a feature environment where packets are replicated using egress conditions. Use these commands: debug platform packet-trace, enable debug platform packet-trace packet 16 fia-trace, debug platform condition egress, debug platform condition start.

  Workaround: Do not use fia-trace.

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.3S

This section documents the open issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.3S.

- CSCtx72973

  Symptom: Config-sync failiure is seen when unconfiguring the crypto gdoi group.

  Conditions: Seen on HA setup.

  Workaround: There is no workaround.

- CSCtz07457

  Symptom: Traffic drop during rekey and "stats multi context read error " in logging.

  Conditions: 4k IKEv2 SVTI longevity test, IKE lifetime 2hrs and IPSec lifetime 1hr.

  Workaround: There is no workaround.

- CSCuc31430

  Symptom: Traceback when you unshut the access interface.

  Conditions: Only in scale configuration.

  Workaround: There is no workaround.

- CSCug19588

  Symptom: IKEv2 TPS performance degradation over time.

  Conditions: This occurs in the lab under extreme test conditions with traffic running during session bring-up.

  Workaround: Reduce traffic and or reduce session bring-up rate.

- CSCug27362

  Symptom: Packet drop occurs when IPSEC VTI IPv6 tunnels are configured on an ESP80. Also getting the following message when the problem happens: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.1 Thread:207 TS:00000001059562400712 %ATTN-3-SYNC_TIMEOUT: msecs since last timeout 1035639, missing packets 6040.

  Conditions: There are no known conditions.

  Workaround: The only workaround so far is to remove the IPSEC configuration between the tunnels.

- CSCuh54693

  Symptom: Crypto Socket remains CLOSED on DmVPN setup.

  Conditions: This symptom is observed when DmVPN with extended CLI mentions IKE profile as the ISAKMP profile.

  Workaround: Remove the IKEv2 profile configuration from the IPSEC profile.

- CSCuh97072

  Symptom: Under certain rare circumstance, ZBFW will not properly build the connection for the first packet of the flow. This causes subsequent packets to be dropped due to TCP state checking.

  Conditions: This was first observed when NAT, ZBFW and HA were all enabled on the ASR platform. This only affects ASR platforms.

  Workaround: Removing and re-adding the NAT configuration resolves the issue. Sometimes it requires re-adding the NAT configuration without any redundancy keywords before re-adding it with the redundancy keywords.

- CSCui20319

  Symptom: Pending issues/ack is observed on ESP

  Conditions: Must meet all following conditions: 1. When port-channel vlan loadbalacing mode is enabled on Port-channel EVC with large scale of EFPs on one port-channel (8000 in this case) 2. EFPs on Port-channel are assigned to different links. 3. When the efps and port-channel are remove using one command "no int port-channel x" 4. Then the scale config and link assignment are added back by copying back the scale config.

Workaround: Seperate EFP removal and port-channel link removal (remove efps, the remove int port-channel) seperate EFP config and port-channel link config (add EFP first, then add links to port-channel).

- CSCui43325

  Symptom: Traffic blackhole for v6 SSM groups after flapping bgp loopback interface on the egress PE.

  Conditions: BGP loopback interface flap.

  Workaround: Unconfigure-reconfigure the mdt default command under the v6 address-family for the vrf.

- CSCul65261

  Symptom: Write bus access failed with fpd upgrade.

  Conditions: FPD bundled upgrade.

  Workaround: There is no workaround.

- CSCum73773

  Symptom: QFP crash.

  Conditions: Remove ip nat setting mode and run "sh pl hard qfp ac statistics drop"

  Workaround: There is no workaround.

- CSCum84172

  Symptom: Incorrect NHRP mapping information for a hub can be propagated throughout the DMVPN network and cause data packet forwarding via a spoke-hub-spoke path even when a spoke-spoke direct path has been built and the sending nodes "thinks" it is sending on the direct path.

  Conditions: A DMVPN spoke node is mis-configured with the correct tunnel IP address, but the wrong NBMA address for a hub (hub1). In this case the incorrect NBMA address would be for a different hub (hub2). Hub1 is configured to be both a hub and a spoke. I.e. it can be the end-point for spoke-spoke tunnels.

  Workaround: Fix the spoke that has the incorrect mapping and then shutdown the hub (hub1) that "thinks" it is behind NAT. This hub must be left in a down state for long enough to ensure that any copy of the mis-configured mapping times out on all nodes in the DMVPN network. In most cases two times the NHRP hold time should be sufficient.

- CSCun13772

  Symptom: CPUHOG messages and watchdog timeout crashes are observed on an ASR1000 series router running DMVPN.

  Conditions: This has been observed on a router with a very large NHRP table (10-20k individual entries) with a very high number (thousands) of child entries per parent entry.

  Workaround: Reduce the number of child entries per parent entry through the use of supernetting.

- CSCun57777

  Symptom: Broadcast Packets are dropped after adding EVC config to ASR1002. The issue happens on and before 03.09.02. The issue doesn't happen on and after 03.10.00. After adding evc config, broadcast packets are dropped, L2BDReplicationStart is counted, and replication tree information disappears.

  Conditions: On and before 03.09.02.

  Workaround: To execute 'no shutdown' under service instance before configuration change.

- CSCun62181

  Symptom: ASR1002 running asr1000rp1-adventerprisek9.03.04.06.S.151-3.S6.bin crashes at crypto ipsec update peer path mtu

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCun79934

  Symptom: qfp ipsec debug message format changed

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCun89879

  Symptom: Some sip packets drop with B2B CGN BPA setup.

  Conditions: Some sip packets drop with B2B CGN BPA setup.

  Workaround: Reload router.

- CSCun91087

  Symptom: O2 router crashes with non-default firmware intermittently.

  Conditions: O2 router crashes with non-default firmware intermittently.

  Workaround: There is no workaround.

- CSCun97760

  Symptom: ASR running 15.2(4)S4 saw ESP crash due to corrupted H323 packet.

  Conditions: ASR running 15.2(4)S4 saw ESP crash due to corrupted H323 packet.

  Workaround: If customer don't need h.323 alg, a workaround is to disable h.323 alg: no ip nat service h225.

- CSCuo17719

  Symptom: An ESP crash is seen with IPv6 ping to or from an interface configured with IPSec and FNF.

  Conditions: The crash is seen when the size of the IPv6 ping is greater than the interface IPv6 MTU.

  Workaround: There is no workaround. However, this is not a common scenario for IPv6 as fragmentation is almost always handled by the sending host/application.

- CSCuo22610

  Symptom: ubr10k4 build breakage on mcp_dev.

  Conditions: mcp_dev ABS build

  Workaround: There is no workaround.

- CSCuo26216

  Symptom: Box is crashing.

  Conditions: Clearing trans with heavy traffic running though box.

  Workaround: There is no workaround.

- CSCuo31506

  Symptom: Traffic drop in getvpn and lisp scale setup.

  Conditions: Traffic is dropped after ipsec flap.

Workaround: There is no workaround.

- CSCuo45683

  Symptom: Tail dropping for PPPoEoA sessions used HW: SPA-3XOC3-ATM-V2.

  Conditions: wrong behavior or congestion although ATM interface load is clearly below any critical value conditions are not clear.

  Workaround: There is no workaround.

- CSCuo46913

  Symptom: A crash is seen causing a system reload. The crash occurs in the Crypto IKMP process: Exception to IOS Thread: Frame pointer 0x3CEFFB58, PC = 0x164CC518 UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Crypto IKMP

  Conditions: This issue occurred after the following debug: debug cry condition peer subnet XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX The exact conditions are still being investigated.

  Workaround: There is no workaround.

- CSCuo55610

  Symptom: Incomplete kernel core file with filename ending in .TEMP_IN_PROGRESS.

  Conditions: Active RP kernel core dump in dual RP2 systems.

  Workaround: There is no workaround.

- CSCuo56722

  Symptom: ASR crashed after modifying IPSec proxy IDs.

  Conditions: ASR with IPSec crypto map based tunnels.

  Workaround: There is no workaround.

- CSCuo61455

  Symptom: Crash of ASR1k running IOS-XE 3.10.2S or 3.11.1S with Carrier Grade NAT (CGN) configured.

  Conditions: ASR1k running IOS-XE 3.10.2S or 3.11.1S with Carrier Grade NAT (CGN) configured.

  Workaround: Disable CGN: "ip nat settings mode default".

- 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.

- CSCuo77017

  Symptom: the tcam resource has not released after 32k efp configured and deleted on the asr1001.

  Conditions: With a clear configuration running 3.13 img configure 32k efp check the tcam resource on the asr1k and delete the efp then check the tcam on the asr1k, you will find the resource has not been released

  Workaround: Reload the router or FP.

- CSCuo77698

  Symptom: When we tried to change slot of SPA-1X10GE-L-V2. Following messages can be seen continuously. after that SPA cannot boot up. Step1:use < hw-module subslot 0/3 shutdown> to power off SPA 2:unplug SPA from slot 0/3/0 then insert it into 0/1/0 ---------- *May 12 06:14:30.407: %FPD_MGMT-3-MAJOR_VER_MISMATCH: Major image version mismatch detected with 10GE I/O FPGA (FPD ID=1) for SPA-1X10GE-L-V2 card in subslot 0/1. Image will need to be upgraded from version 0.1292 to at least a minimum version of 1.9. Current HW version = 1.2. *May 12 06:14:30.408: %FPD_MGMT-5-UPGRADE_ATTEMPT: Attempting to automatically upgrade the FPD image(s) for SPA-1X10GE-L-V2 card in subslot 0/1. Use 'show upgrade fpd progress' command to view the upgrade progress ... *

  Conditions: This issue can not be reproduced by 100%. we tried to reproduce it with 3 other slots, the issue cannot be reproduced unless you unplug SPA from slot 0/3/0 then insert it into 0/1/0.

  Workaround: Change other SPAs.

- CSCuo79559

  Symptom: ASR1k crash due to memory corruption in CFT.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCuo83050

  Symptom: IPsec SA does not come UP.

  Conditions: isakmp profile configured under the ipsec profile configuration loaded to dmvpn hub with the use of configure replace.

  Workaround: There is no workaround.

- CSCuo85982

  Symptom: High RP and ESP utilization and generation of many large (~ 1 MB) logging files with names of the form "cpp_cp_F*".

  Conditions: IPv4 multicast packets received on interfaces configured for IP subscriber sessions.

  Workaround: There is no workaround.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.2S

This section contains the following topics:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.2S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.2S.

- CSCta15511

  Symptom: Unnecessary radius debugs are displayed on the console (one extra line for each MN call closure) when conditional debugs are enabled.

  Conditions: When the radius conditional debugs are enabled.

  Workaround: There is no workaround.

- CSCtf46011

  Symptom: With the c3845 gateway, insert mgcp gateway and one MGCP PRI, one MGCP CAS port, when resetting mgcp gw and PRI/CAS ports, or change device pool of MGCP PRI port, the MGCP PRI port will be in Unregister status. The call from/to this port will fail.

  Conditions: Not all the mgcp gateway has the issue. Only one hit the problem.

  Workaround: Click the MGCP PRI port and do reset.

  This issue is cosmetic. GW sends RSIP(forced) and RSIP(restart) without CUCM ack to the first RSIP(forced). The first and second events are processed. Within CUCM Realtime Information System (RIS) When child(12) was created, it creates PerfMon counter object that have the same name as the object created by child(11). This operation failed because child(11) has not stopped and the same named object is still in use by child(11). When child(11) stops it deletes the PerfMon counter object for this port. As a result, the GUI is showing device unregistered. The device is actually registered but the GUI has a pointer for an old perfmon instance for this device. The device is currently registered and perfmon will show it registered under new instance.

- CSCtk05154

  Symptom: Not all dtmf is detected by the receiving endpoint. PCM analysis will show two tones too close together to be detected as two.

  Conditions: Dial the same number rapidly. For example 99999999.

  Workaround: There is no workaround.

- CSCub14611

  Symptom: %IOSXE-3-PLATFORM: R0/0: kernel: physmap-flash.0: Chip not ready.

  Conditions: While doing redundancy force-switchover on ASR1006 (RP1).

  Workaround: Reload ASR1006.

- CSCuc56382

  Symptom: With MTU set lower, for a bigger IA prefix LSA (of 1600 bytes), fragmentation is not handled correctly if IPSec is configured. OSPFv3 adj flaps with "Too many retransmits". Flooding of this large LSUpdate is unsuccessful if IPSec is configured. Without IPSec, the issue is not seen.

  Conditions: With Ipsec Configured and with small MTU the problem can be seen.

  Workaround: The workaround is to set the mtu size to 1500 and it works fine. Only when it is set to 1300 or lower the issue is seen because of wrong handling of reassembly. Fragmentation is not correctly handled. Image tested : XE38 throttle release.

- CSCue18556

  Symptom: There is no RP CLI to dump drop counter due to High Priority Policer.

  Conditions: On configuring the High Priority Policer there is no RP CLI to dump drop counters.

  Workaround: Using the CC CLI. Caveat: CC CLI show "other system drop" "High Priority Policer drop count"

- CSCue29595

  Symptom: SRTP passthrough for h323 calls failing.

  Conditions: h323 calls are failing when both the legs are h323 and its SRTP passthrough.

  Workaround: There is no workaround.

- CSCue43682

  Symptom: Transcoding sessions are intermittently becoming stuck after call is cleared.

  Conditions: When transcoding configured in DSPfarm.

  Workaround: Reload Gateway.

- CSCue52655

  Symptom: No Video legs out put for DO-DO BWcac with multicodec call.

  Conditions: No Video legs out put for DO-DO BWcac with multicodec call.

  Workaround: There is no workaround.

- CSCue62227

  Symptom: SIP PSTN gateway may delay response to BYE message at end of a T.38 call.

  Conditions: Incoming call to SIP gateway goes out a PRI Call successfully switches no T.38 BYE is received by SIP gateway. 200 OK response is delayed by a few seconds.

  Workaround: There is no workaround.

- CSCuf51465

  Symptom: On ASR1000-2T 20GE Linecard, TCAM_VLAN_TABLE_FULL Error is not displayed.

  Conditions: when Maximum scale of 48K VLAN already configured and user attempts to add more than 48K VLANS on the card.

  Workaround: There is no workaround.

- CSCuf93471

  Symptom: After a brief unavailability of LDAP CRL, no new CRL fetches can be performed. The following messages are seen on the interface: ---- Mar 28 08:23:37.988: CRYPTO_PKI: Retreive CRL using LDAP DIRNAME Mar 28 08:23:37.988: CRYPTO_PKI: Failed to send the request. There is another request in progress.

  Conditions: This symptom was first seen in Cisco IOS Release 15.1(4)M6. The issue is not limited to this release.

  Workaround: Configure the "revocation-check none" command under the affected trustpoint. Reload the router.

- CSCug15520

  Symptom: Hit an ucode crash in lisp zbfw scaling case, scaling number is 500 lisp instances, 50k eid table, 500 pair zone. The crash is hit in unconfigure fw data stage. it is reproducible.

  Conditions: lisp fw, unconfig.

Workaround: There is no workaround.

- CSCug37057

  Symptom: RSVP hello stays in "PASSIVE".

  Conditions: Ospf send bdb packet error for incomplete adj.

  Workaround: There is no workaround.

- CSCug42064

  Symptom: TDoS with "silent discard" does not work with explicit cause-code configured. The silent-discard works when the "cause-code" is removed from the configuration. Ideally these should be mutually exclusive and "silent-discard" should have the highest priority irrespective. Steps to reproduce: 1. config ip add trust list with an IP address, as well as the silent discard option as well as the call reject cause code (other than default). 2. Send INVITE to CUBE from an IP that is not in the trusted list. 3. Expected behavior: CUBE should discard the INVITE silently, which is not happening currently. 4. If we remove the call-reject CC from the configuration, then silent discard is working as expected. These configs are no-ops./ mutually exclusive. This is seen in the N2 baseline image as well. Logs and configs attached.

  Conditions: Set the cause-code for TDOS.

  Workaround: The silent-discard works when the "cause-code" is removed from the configuration.

- CSCug48831

  Symptom: GM re-registers to the KS after not receiving a rekey. The KS doesn't reset the number of rekey Acks missed by the GM after the GM re-registers. This may result in the GM being deleted after missing 3 rekeys, even if it registered every time after missing those rekeys.

  Conditions: GM doesn't receive a rekey and re-registers to the KS when TEK is about to expire.

  Workaround: There is no workaround.

- CSCug55787

  Symptom: When 8-port CT1E1 has E1 card type and with 248 channel groups configured, OIR with 1-port, configured with 31 channel groups (E1), then OIR back with original 8-port will cause the first controller's channel groups failed to come up.

  Conditions: It happens when the OIR case. When OIR'ed to 1-port, card type E1 and configured with full 31 channel groups. Then OIR back to 8-port will cause the first controller's channel group failed to come up.

  Workaround: Remove the failed channel groups and reconfigure them.

- CSCug55996

  Symptom: memory leak and crash preceded with error messages like Apr 24 15:52:40.776: %DIALPEER_DB-3-ADDPEER_MEM_THRESHOLD: Addition of dial-peers limited by available memory.Memory leak due to skinny msg server and alloc_pc = asnl_get_new_evInfo.

  Conditions: 2951 router running 15.3(2)T.

  Workaround: There is no workaround.

- CSCug71832

  Symptom: I/O memory leaks occur with the following error messages: `SYS-2-MALLOCFAIL Memory allocation of 268 bytes failed from 0x6076C1C0, alignment 32 Pool: I/O Free: 3632 Cause: Memory fragmentation Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "SCCP Application", ipl= 0, pid= 234 -Traceback= 6082E5B4z 60761188z 607618A8z 60764930z 6237DFA4z 62379CB4z 623873A4z 62373474z 62374E64z 607FAE64z 607FAE48z`

Conditions: This symptom occurs due to a slow memory leak in the SMALL and MIDDLE buffers.

Workaround:There is no workaround.

- CSCug73829

  Symptom: Data Conversion Errors seen while configuration changes at Remote end device.

  Conditions: Data Conversion Error & traceback can be seen while doing configuration changes on remote end device.

  Workaround: There is no workaround.

- CSCug84557

  Symptom: CUBE SBC does not forward mid-call Re-INVITE in a glare condition.

  Conditions: This symptom is observed in a condition where both legs of a SIP call through the SBC sends in Re-INVITE within 100ms of each other. Instead of forwarding the first arriving Re-INVITE to the other leg and then rejecting the other with a 491 Request Pending response, SBC does not forward either of the Re-INVITE and gets into a deadlock condition leading to no audio and an eventual call tear down.

  Workaround: There is no workaround.

- CSCuh03476

  Symptom: Tracebacks seen while configuring APS parameters on a POS link.

  Conditions: During normal CLI configurations.

  Workaround: There is no workaround.

- CSCuh04779

  Symptom: Unable to import an ECDSA CA certificate.

  Conditions: IOS router running any version of code up through 15.3(2)T.

  Workaround: There is no workaround.

- CSCuh19561

  Symptom: IPsec tunnels may not come up in scaling test with only one CPU on CSR.

  Conditions: Config 1vCPU on CSR and bring up 100 ipsec tunnels.

  Workaround: Bring up less ipsec tunnels with 1vCPU. Or Config 2vCPU or 4vCPU when 100 or more tunnels scaling is needed on CSR.

- CSCuh23859

  Symptom: With Suite-B configured (i.e. esp-gcm / esp-gmac transform) on a GETVPN Key Server (KS), Group Members (GM) will see the following un-gated error message on the console when the KS policy ACL is changed or edited and a rekey is sent from the KS using "crypto gdoi ks rekey"... May 31 09:56:49.906 IST: *** SERIOUS ERROR: OVERLAPPING IV RANGES DETECTED *** When the GM receives the rekey, the policy is installed successfully. However, after this the GM re-registers twice and then these errors are displayed.

  Conditions: Suite-B is configured (i.e. esp-gcm / esp-gmac transform) on a GETVPN Key Server (KS), the KS policy ACL is changed or edited and a rekey is sent from the KS using "crypto gdoi ks rekey" This issue was seen with at least 50 Group Member (GM) instances using VRF-Lite on a ASR1K GM box and no more than 30 ACE's in the KS policy ACL, however this issue should also be seen on a ISRG2 GM box with less GM instances and less ACE's as well.

  Workaround: If a Key Server (KS) policy ACL must be changed or edited while Group Members (GM) have already registered and downloaded GETVPN Suite-B policy (i.e. esp-gcm / esp-gmac transform), issue "crypto gdoi ks rekey replace-now" instead of "crypto gdoi ks rekey" after

changing the KS policy ACL. (NOTE: a very small amount of traffic loss may be expected) If possible, do not change the KS policy ACL after a GETVPN network using Suite-B is up and running. NOTE: The fix requires both an upgrade of the KS and GM to properly work.

- CSCuh35993

  Symptom: Create an RRI route for deny ACL lines in the crypto map.

  Conditions: 15.x code and L2L ipsec tunnel.

  Workaround: There is no workaround.

- CSCuh43137

  Symptom: With Suite-B configured (i.e. esp-gcm / esp-gmac transform), GETVPN Key Sever (KS) shows TEK SPI's for deny ACE's when "show crypto gdoi ks policy" is issued while a Group Member (GM) does not show TEK SPI's for deny ACE's when "show crypto gdoi" is issued.

  Conditions: The command "show crypto gdoi ks policy" is issued with Suite-B configured (i.e. esp-gcm / esp-gmac transform) deny ACE's in the policy ACL for GETVPN / GDOI.

  Workaround: There is no functionality impact to the GETVPN Suite-B feature with this defect.

- CSCuh51171

  Symptom: While making Video call on CUBE with Multiple M line CUBE crashed due to memory corruption.

  Conditions: When multiple M line will be negotiated with early dialog update.

  Workaround: There is no workaround.

- CSCuh51607

  Symptom:Traceback occur.

  Conditions: Delete acl for IPSec with live traffic.

  Workaround: There is no workaround.

- CSCuh52011

  Symptom: SNMP Trap Informs to monitor GETVPN service. In each Trap Informs customer wants the <CgmGdoiIdentificationValue> attribut to be in ASCII string (and not binary value) when they use <crypto isakmp identity hostname> However IOS always sends an IP address identity (type and value) in the trap. They should have type 2 and the FQDN of the KS which is not the case.

  Conditions: GETVPN setup between KS and GM and crypto isakmp identity as hostname (FQDN)

  Workaround: There is no workaround.

- CSCuh54511

  Symptom: Memory leak in REGISTRATION Pass-through scenario.

  Conditions: REGISTRATION pass-thru with end-point authentication.

  Workaround: There is no workaround.

- CSCuh72004

  Symptom: On the Cisco ASR1000 Series Router, the FPD upgrade on the Fixed Ethernet Line Card (ELC) causes line protocol to stay down on its Interfaces. The Route Processor (RP) card on the router goes out of sync. The line protocol status on ELC-console is shown as 'up'; but, the RP is unaware of this. As per RP, all the 1G ELC interfaces are in 'down' state. 'Shut/no shut' of the affected interfaces interface-config does not resolve the issue.

Conditions: FPD upgrade of the DB-FPGA on the Ethernet Line Card, performed via the router command: "upgrade hw-module subslot <> fpd bundled reload" or "upgrade hw-module subslot <> fpd file <filename> reload" causes the issue.

Workaround: Reload the Ethernet Line Card by either a manual removal/insertion of the line card or via the router command "hw-module slot <> reload" This issue happens because the SPA is reloaded after a successful DB-FPGA(FPD) on a line card. However on ELC, SPA OIR is not supported since since it is just a logical subslot. Hence, after a FPD upgrade, the SPA is left in an undefined state causing line protocol to stay down. To resolve this issue, the card is restarted (slot reloaded). As a result of this fix, after a successful FPD upgrade the user would see the following messages on the RP2 console: `*<Date_Time>: FPD MSG HANDLER: upgrade result response from 0/0 received, card type=0x75F, fpd id=0x16, num retries=1, upgrade result=2, upgrade id=8 *<Date_Time>: %FPD_MGMT-6-UPGRADE_PASSED: DB FPGA (FPD ID=22) image in the BUILT-IN-2T 20X1GE card in subslot 0/0 has been successfully updated from version 1.12 to version 1.13. Upgrading time = 00:03:51.518 *<Date_Time>: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the required FPD images have been completed for BUILT-IN-2T 20X1GE card in subslot 0/0. Number of successful/failure upgrade(s): 1/0. *<Date_Time>: %FPD_MGMT-5-CARD_POWER_CYCLE: BUILT-IN-2T 20X1GE card in subslot 0/0 is being power cycled for the FPD image upgrade to take effect. *<Date_Time>: %SPA_OIR-6-OFFLINECARD: SPA (BUILT-IN-2T 20X1GE) offline in subslot 0/0 *<Date_Time>: %IOSXE_OIR-6-OFFLINECARD: Card (cc) offline in slot 0 *Oct 3 03:40:13.214: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled *<Date_Time>: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in slot 0 *<Date_Time>: %CMRP-5-PRERELEASE_HARDWARE: R1/0: cmand: 0 is pre-release hardware *<Date_Time>: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0 *<Date_Time>: %CMRP-5-PRERELEASE_HARDWARE: R1/0: cmand: 0 is pre-release hardware *<Date_Time>: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled *<Date_Time>: %IOSXE_OIR-6-OFFLINECARD: Card (cc) offline in slot 0 *<Date_Time>: %CMRP-5-PRERELEASE_HARDWARE: R1/0: cmand: 0 is pre-release hardware *<Date_Time>: %CMRP-5-PRERELEASE_HARDWARE: R1/0: cmand: 0 is pre-release hardware *<Date_Time>: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in slot 0 *<Date_Time>: %CMRP-5-PRERELEASE_HARDWARE: R1/0: cmand: 0 is pre-release hardware *<Date_Time>: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0 *<Date_Time>: %LINK-3-UPDOWN: SIP0/0: Interface EOBC0/1, changed state to up *<Date_Time>: %SPA_OIR-6-ONLINECARD: SPA (BUILT-IN-2T 20X1GE) online in subslot 0/0.`

- CSCuh78055

  Symptom: MN-BITS IN stays in Locked state even when MN-BITS OUT is removed.

  Conditions: MN-BITS IN stays in Locked state even when MN-BITS OUT is removed.

  Workaround: There is no workaround. But as a corrective action, removing and re-applying input source will bring the falsey BITS_IN source to QL-FAILED state; then the sync source is automatically shifted to next best available.

- CSCuh92837

  Symptom: When fax tones are detected in the early media phase of the call, the gateway does not initiate a fax mode switchover.

  Conditions: The call must establish early media, and fax tones must be detected in this phase of the call.

  Workaround: There is no workaround.

- CSCui02348

  Symptom: HP2 traffic gets throttled when multiple lower priority streams persent.

  Conditions: Test with image:XE310_THROTTLE_LATEST_20130622_141526.

  Workaround: There is no workaround.

- CSCui04655

  Symptom: Cisco IOS router with WEBVPN and anyconnect client using DTLS is not working and the traffic is dropped.

  Conditions: This is observed when WebVPN using DTLS is used.

  Workaround: Disable DTLS.

- CSCui04860

  Symptom: HA sync is not happening from active to standby.

  Conditions: This is observed when HA Sync-up is not happening for PKI Server on Cisco IOS Release 15.3(2.25)M0.1.

  Workaround: There is no workaround.

- CSCui06926

  Symptom: Initiator sends identity certificate based on "ca trustpoint" under the isakmp-profile. However, the responder does not do this. Instead it gets the identity certificate from the *first* trustpoint (out of the list of trustpoints) based on peer's cert_req payload in MM3.

  Conditions: This symptom is observed under the following conditions:

  1. IKEv1 with RSA-SIg Authentication, where each Peer has two certificates issued by the same CA.

  2. Each Peer has isakmp profiles defined that match on certificate-map and have "ca trustpoint" statements with self-identity as fqdn.

  Workaround: There is no workaround.

- CSCui14805

  Symptom: Dubious QL-SEC seen on 10M src of MN spa after cable removal and reloadng spa.

  Conditions: GPS 10M port connected to Symmetricom device.

  Workaround: Remove and re-apply the config to go QL-FAILED state. network-clock input-source 3 External 2/0/0 10m

- CSCui17100

  Symptom: Ucode crash seen.

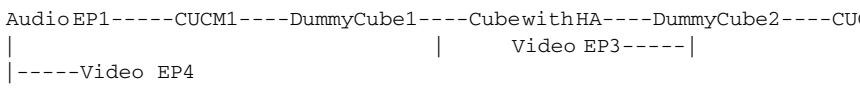
  Conditions: Crash seen when doing cc_oir with scaled EVC-EOMPLS config.

  Workaround: There is no workaround.

- CSCui19969

  Symptom: Oneway video seen after SSO for escalated video call with Asym.

  Conditions: One way video seen after SSO for escalated video call with asymmetrical PT inter working. Setup:-

  Workaround: There is no workaround.

- CSCui48145

  Symptom: On RP platform, the following multiple messages were observed after redundancy force-switchover:

```
   *Jul 19 19:30:58.303: %CMANRP-6-CMHASTATUS: RP switchover, received fastpath
\  becoming active event  *Jul 19 00:53:28.384: %IOSXE-3-PLATFORM: R0/0: kernel:
physmap-flash.0: Chip not     \  ready for buffer write. Xstatus = c4, status = c4
```

  This is not observed on ELC platforms. The root cause of the above messages on RP was found to be the following: Some revisions of the P30, P33, and J3 Flash memory devices can hang when an ERASE SUSPEND command is issued following an ERASE RESUME without waiting for the minimum delay time to elapse. The result is that when the ERASE appears to be complete (no bits are toggling), the contents of the Flash memory block on which the ERASE was executing could be inconsistent with the expected values. This causes ERASE operation to fail. This was fixed for RP via CSCub14611. However, the fix did not apply fro ELC platforms since ELC-specific changes use the CISCO_CONFIG_ELC instead of CISCO_CONFIG_MCP. This extends the fix for ELC platforms.

  Conditions: Redundancy force-switchover on RP.

  Workaround: There is no workaround.

- CSCui54042

  Symptom: ASR crashes when running command "no crypto pki certificate pool"

  Conditions: This has been seen on the ASR1004 running the following:

```
asr1000rp2-advipservicesk9.03.07.03.S.152-4.S3
asr1000rp2-advipservicesk9.03.07.03.S.152-4.S2
asr1000rp2-advipservicesk9.03.07.03.S.152-4.S1
```

  Workaround: Do not run the command "no crypto pki certificate pool"

- CSCui55472

  Symptom: While removing IPSEC configuration and unconfiguring, command no crypto pki server ra is issued followed by answer "yes", the router's CPU utilization reaches to 100% which degrades its performance badly, while the script keeps on running in background and finally this leads to failure/aborting of further listed test cases.

  Conditions: There are no known conditions.

- CSCui64059

  Symptom: Router crashes in call forward scenario.

  Conditions: Call forward enabled.

  Workaround: There is no workaround.

- CSCui65843

  Symptom: CUCM Single Number Reach outbound call to a cell phone carrier doesn't connect after the destination answers.

  Conditions: CUCM outbound single number reach via SIP trunk and CUBE ASR routes the call out to a SIP PSTN Service Provider. After the destination answers the call it gets dead air. CUBE ASR receives the 200 OK from the SIP carrier however does not relay this to CUCM. In the call flow we can observe the call attempts to cut early audio and there are repeated 183 Session Progress w/ SDP messages received from the carrier.

Workaround: Apply a sip profile that modifies the 183 response as following; voice class sip-profiles 100 response 183 sdp-header Audio-Attribute modify "a=recvonly" "a=sendrecv" Apply this SIP Profile globally or on any dial-peer facing CUCMs.

- CSCui70561

  Symptom: Low performance for AVC 2.0 on ESP100 setup.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCui74020

  Symptom: After configuring on ASR1k: cdp run ! interface gi0 dp enable ASR1k isn't able to find its CDP neighbor

  ```
  (e.g. a Switch): ASR1k#show cdp nei Capability Codes: R - Router, T - Trans Bridge, B
  - Source Route Bridge                   S - Switch, H - Host, I - IGMP, r - Repeater,
  P - Phone,                D - Remote, C - CVTA, M - Two-port Mac Relay   Device ID
  Local Intrfce     Holdtme    Capability  Platform  Port ID  while the switch can find
  its CDP neigbor(ASR1k): Switch#show cdp nei Capability Codes: R - Router, T - Trans
  Bridge, B - Source Route Bridge                   S - Switch, H - Host, I - IGMP, r -
  Repeater, P - Phone Device ID       Local Intrfce     Holdtme    Capability  Platform
  Port ID ASR1k             Gig 1/0/19        134           R I      ASR1006   Gig 0
  ```

  Conditions: CDP enabled globally and on Mgmt Interface.

  Workaround: There is no workaround.

- CSCui80093

  Symptom: CUBE not falling to FT mode for srtp-rtp call in no DSP case.

  Conditions: This is seen when DSP resources are shutdown/unavailable in the router.

  Workaround: Configure dspfarm profile in the router if available or do not configure "media flow-around" CLI. This issue is particularly observed when Flow-around is configured for srtp-rtp call and when there are DSP resources in the router

- CSCui80542

  Symptom: Sending a PING to an IPv6 EID from a Proxy ITR without specifying the source interface can cause a crash which resets the FO.

  Conditions: When sending an ICMPv6 packet, we try to set the source UDP port, and depend on the source interface supplied in the exec command to do that. When the source interface is not included in the ping command, the source UDP port is invalid, and a crash ensues when LISP attempts to use it.

  Workaround: Include 'source <interface>' to ping commands on the Proxy ITR.

- CSCui81336

  Symptom: After reload of DMVPN spoke fails MM-Key Exchange. Hub will show CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from x.x.x.x failed its sanity check or is malformed.

  Conditions: 1921 IOS router Use the; character at the beginning of the master encryption key. i.e. key config-key password-encryption <enter> new key:;cisco123 confirm key:;cisco123.

  Workaround: Change the key so that; is not the first character. #key config-key password-encrypt Old key:;cisco123 New key:cisco123 Confirm key:cisco123.

- CSCui84532

  Symptom: RP is again fragmenting it.

  Conditions: Giant pkts are sent from SPA after LAF.

  Workaround: There is no workaround.

- CSCui84553

  Symptom: Router crashes.

  Conditions: Crashes when router is configured with onefw,NAT and Qos.

  Workaround: There is no workaround.

- CSCui85237

  Symptom: Cisco router crashes.

  Conditions: This issue occurs when a single HTTP request is followed by more than one HTTP response.

  Workaround: There is no workaround.

- CSCui85371

  Symptom: Ikev2 session is NOT coming UP.

  Conditions: Ikev2 session is NOT coming UP. Loopback to loopback ping is not going through.

  Workaround: There is no workaround.

- CSCui86165

  Symptom: A GDOI / GETVPN Group Member (GM) with a GDOI Version which does not support the GETVPN Suite-B feature is allowed to register to a Key Server (KS) with Suite-B configured. This GM can then download Suite-B policy which will most likely fail to install on the GM.

  Conditions: GETVPN Suite-B is configured on the Key Server (KS). Group Member (GM) has a GDOI Version which does not support the GETVPN Suite-B feature, i.e. "show crypto gdoi feature suite-b" gives a "No" under "Feature Supported" ...

```
ISR4400# show cry gdoi feature suite-b        Version    Feature Supported
1.0.7           No
```

  Workaround: Do not configure GETVPN Suite-B policy or upgrade GM to an IOS version which supports GETVPN Suite-B.

- CSCui89230

  Symptom: 1.) When GETVPN is configured, issuing "clear crypto gdoi" on a Group Member (GM) which is in Receive Only mode (i.e. Inbound Only) transitions the GM SA's to Passive mode (i.e. Inbound Optional) instead of Normal mode (i.e. Both).

  2.) When GETVPN is configured for a Group Member (GM) and has "passive" configured under "crypto gdoi group ..." the following exit trace is seen in "show monitor event-trace gdoi exit all detail" when downloading a new SA mode from the Key Server (KS)... "Download GSA Mode: GM already in passive mode - update aborted" FAILED_TO_UPDATE_GM_SA_STATUS_AS_IT_IS_IN_PASSIVE_MODE As a result, if the installed SA's were not in Passive (i.e. Inbound Optional) mode (e.g. because "crypto gdoi gm ipsec direction both" was issued) when receiving a rekey, they would not transition back to Passive / Inbound Optional mode as they should (since the GM has "passive" configured).

Conditions:

1.) Issue "clear crypto gdoi" on a Group Member (GM) already in Receive Only mode (i.e. Inbound Only)

2.) Configured "passive" under "crypto gdoi group .." on a Group Member (GM) and the GM downloads a new SA mode from the Key Server (KS).

Workaround: There is no workaround.

- CSCui92587

  Symptom: CUBE offer dsp unsupported to UAS, eventhough UAC doesn't offer that codec. This issue is seen in both baseline and nitrogen2 image. Nitrogen2: CUBE is offering "mp4a-latm" codec in the mid-call to UAS, even though mid-call offer from UAC doesn't have the "mp4a-latm" codec which is wrong. In this case, "mp4a-latm" codec doesn't have fmtp attributes as well. Baseline: CUBE offers "aacld" codec in the mid-call to UAS, even though mid-call offer from UAC doesn't have "aacld" codec.

  Conditions:

```
NVITE (SDP) --------> | ----INVITE (SDP)-->      <--18x (rel SDP)------ |
<-----18X(rel SDP)   (MP4A-LATM codec is negotiated)                              |
----PRACK ------->                          |<----200OK PR------
|<---UPDATE (SDP)---                              | --491-------------> (CUBE is
sending this because PRACK/200OK transaction is
pending on UAC side) PRACK ----------------> |
<---200 OK PR --------|  ----UPDATE(SDP) -----> | -----UPDATE(SDP)-->
```

  (Here UPDATE from UAC, doesn't have "mp4a-latm" codec, but CUBE still sends "mp4a-latm" codec in the outbound offer that too without fmtp attributes, which is wrong as transcoder is not supported with "mp4a-latm" codec) | <--2OOOK((SDP with mp4a-latm codec). Here CUBE logs displays an IEC error code, and CUBE is not sending any response for UPDATE to the UAC. UPDATE from UAC kept on re-transmitting the UPDATE and the request is timed out)

  Workaround: There is no workaround.

- CSCui96084

  Symptom: CUBE sends incorrect Contact in the 183 response when translation profiles are configured on the out-leg.

  Conditions: Translation profiles are used only on the outbound dial peer. Remote party sends 180 Ringing.

  Workaround: Use a sip profile to modify the incorrect contact.

- CSCuj01244

  Symptom: CUBE crashes during T38 fax call.

  Conditions: This symptom is observed in an enclosed configuration.

  Workaround: There is no workaround.

- CSCuj02457

  Symptom: UC560 Crashed.

  Conditions: The most recent change before the crash was incoming dial plans.

  Workaround: There is no workaround.

- CSCuj02503

  Symptom: 'Internal_service' license state shows as 'Active, Not In Use' even after its expiry. The system Linux Shell cannot be accessed upon expiry of the 'Internal_service' 1 Day license which is expected. However if an new 1 Day license is installed again, the license state comes up as 'Active, In Use' but Lynx Shell cannot be accessed.

  Conditions: Install 1 Day 'Internal_service' license. Let the license expire then install another 1 Day 'Internal_service' license.

  Workaround: Configure and unconfigure the 'platform shell' configuration command to recover the license to proper working state.

  ```
  Router#config terminal Router(config)#platform shell Router(config)#no platform shell
  Router(config)#platform shell.
  ```
  Now the System Linux Shell would be accessible.

- CSCuj02519

  Symptom: Chunk memory leak in Crypto Proxy.

  Conditions: This is only seen with IPSEC HA configured.

  Workaround: There is no workaround.

- CSCuj05759

  Symptom: Customer has some VG350 and phones. They have FAC configured and all users need to enter the FAC code before make an external call. Customer are not able to hear the zipzip tone they used have before entering the FAC. User has cptone tw configured under voice-port.

  Conditions: On all stcapp voice-port.

  Workaround: Under voice-port, change "cptone tw" to "cptone us".

- CSCuj08162

  Symptom: Cisco IOS configured as a GETVPN Key Server (KS) crashes when the IPsec TEK ACL is removed for the group and a rekey is attempted.

- Conditions: This symptom is observed when a GETVPN Key Server (KS) is configured and the IPsec TEK ACL is removed. The IOS version has CSCuh43137 integrated.

  Workaround: There is no workaround.

- CSCuj12613

  Symptom: Duplicate digits received by 3rd party UA when RTP-NTE packets are sent from IOS SW MTP.

  Conditions: IOS SW MTP Originates RTP-NTE packets.

  Workaround: There is no workaround.

- CSCuj13388

  Symptom: This DDTS is filed for NAT and ALG DE to review the code and see if there are potential issue in HA.

  Conditions: Mixed traffic.

  Workaround: There is no workaround.

- CSCuj14019

  Symptom:%CMRP-3-UDI_AUTH: F0: cmand: Quack Unique Device Identifier authentication failed, show up.on ASR1001.

  Conditions: After reloading the box or inserting SFPs.

Workaround: There is no workaround.

- CSCuj140a5

  Symptom: There is a field that is not displayed.

  Conditions: Observed when the command show sip-ua registration passthrough status detail is used.

  Workaround: Used the command sip-ua registration passthrough status.

- CSCuj14655

  Symptom: Traceback seen while boot up

  Conditions: Load latest mcp_dev in 6RU-FP80 system.

  Workaround: There is no workaround.

- CSCuj23603

  Symptom: The ESP may crash in cpp_mcplo %CPPHA-3-FAULT: F0: cpp_ha: CPP:0.0 desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL id:2121 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x8

  Conditions: NAT is enabled and mode has been changed between "Classic"/default and CGN.

  Workaround: Reload box or at least CPP after changing mode.

- CSCuj24935

  Symptom: Flow entries are created with "no ip nat create flow-entries" cli.

  Conditions: UUT is configured more than 3 static mappings.

  Workaround: There is no workaround.

- CSCuj28985

  Symptom: FP Crash during Multiple PPP(PTA/LNS) Session Flaps.

  Conditions: "subscriber accounting accuracy" is enabled.

  Workaround: There is no workaround.

- CSCuj31165

  Symptom: crpcipSecGlobalActiveTunnels is incrementing endlessly.

  Conditions: crpcipSecGlobalActiveTunnels OID does not decrement when the current active tunnel is removed.

  Workaround: There is no workaround.

- CSCuj33901

  Symptom: ASR1000-RP2's actual ACTV/STBY LED state is incorrect. Although RP2 state is active, STBY LED light up. This issue is seen while using V04 RP2.

  Conditions: V04 RP2.

  Workaround: Refer to Field Notice FN63704.

- CSCuj37848

  Symptom: Hung RTP connections seen for DO-EO Basic ANAT calls.

  Conditions: CUBE preference is set to IPv4.

  Workaround: There is no workaround.

- CSCuj38450

  Symptom: The router sends IDLE ABCD of 0000 instead of 0001 under certain situations. Customer needs the IDLE bits to always be 0001 for his set up to work with voice.

  Conditions: The issue occurs in the following scenarios

  1. When the router is reloaded.

  2. When we issue a shutdown and no shutdown command under the E1 controller.

  3. When the voice-port is issued a shutdown and no shutdown command.

  Workaround: Remove and re-add the following commands to the configuration:

  ```
  connect BEO-Data E1 0/0/0 0 E1 0/0/1 0
  connect MFC#1 voice-port 0/1/0 E1 0/0/0 1
  connect MFC#2 voice-port 0/1/1 E1 0/0/0 2
  ```

- CSCuj39496

  Symptom: When configuring Input MPLS aware FNF (under interrface config --- mpls flow mon MON_NAME in) it can happen that FNF will cease to function due to cache entry leak/exhaustion.

  Conditions: This can only occur with Input MPLS FNF and moreover will occur only with certain labels. In particular it will occur for MPLS labels for which the output of show plat hard qfp active feature cef-mpls prefix mpls <LABEL NUM> does *not* have an IPV4 adjacency.

  Workaround: There is no workaround.

- CSCuj39901

  Symptom: Crash with "ip nat settings mode cgn" in the config.

  Conditions: None specifically.

  Workaround: Reload after changing settings.

- CSCuj40124

  Symptom: Cisco router crashes.

  Conditions: This symptom is observed when sending specific PCAP testing to the MQC mode.

  Workaround: There is no workaround.

- CSCuj44237

  Symptom: With Suite-B configured, that is, esp-gcm / esp-gmac transform on a GETVPN Key Server (KS), Group Members (GM) will see the

  ```
  "*** SERIOUS ERROR: OVERLAPPING IV RANGES DETECTED ***"
  ```
  un-gated error message on the console when the following is done:

  (1) GM registers to KS and downloads ACL1

  (2) KS configures ACL2 which is a subset of ACL1

  (3) KS issues "crypto gdoi ks rekey" & GM receives rekey successfully, downloading ACL2

  (4) KS configures the original ACL1 again

  (5) KS issues "crypto gdoi ks rekey" & GM the error message is seen After this, the GM begins to re-register.

  Conditions: Suite-B is configured, that is, esp-gcm / esp-gmac transform on a GETVPN Key Server (KS) with GM's registered The KS policy ACL is changed from ACL1 to ACL2 (where ACL2 is a subset of ACL1) & a rekey is sent from the KS using "crypto gdoi ks rekey" The KS policy ACL is reset back from ACL2 to ACL1 & a rekey is sent from the KS using "crypto gdoi ks rekey"

Workaround: If a Key Server (KS) policy ACL1 must be changed to ACL2 & then changed back to the original ACL1 while Group Members (GM) have already registered and downloaded GETVPN Suite-B policy, that is, esp-gcm / esp-gmac transform, do one of the following:

1.) Wait for the TEK's of the original ACL1 to expire after the first rekey before changing back to the original ACL1

2.) Issue "crypto gdoi ks rekey replace-now" instead of "crypto gdoi ks rekey" after changing back to the original ACL1.

3.) If the above two workarounds do not work, issue "clear crypto gdoi" on the GM's with the error or "clear crypto gdoi ks members now" on the KS to reset the entire group.

- CSCuj45298

  Symptom: With the ASR1k packet-trace feature, a packet may be shown as "Consumed Silently" in the packet state, where it really should be forwarded. This is only a problem with the packet trace output, and does not impact the actual forwarding functionality.

  Conditions: This can happen when packet-trace is tracing a tunnel encapsulated packet.

  Workaround: There is no workaround.

- CSCuj49523

  Symptom: On ASR1000-2T 20GE and ASR1000-6TGE line cards, on interfaces with MAC Loopback, the interface Counters are not updating correctly.

  Conditions: After setting the MAC loopback on the interface.

  Workaround: There is no workaround.

- CSCuj50054

  Symptom: RTP session for video doesn't get cleared up for DO-EO FA VCC call on ASR.

  Conditions: DO-EO FA VCC call.

  Workaround: There is no workaround.

- CSCuj51514

  Symptom: Ucode crash on clear nat translations.

  Conditions: Ucode crashes when doing clear ip nat translations * on a scaled setup

  Workaround: There is no workaround.

- CSCuj51538

  Symptom: Standby FP crashes

  Conditions: standby fp continuously crashes on configuring pap with NAT,NAT64 on same box.

  Workaround: There is no workaround.

- CSCuj51797

  Symptom: conference from EX90 is not recorded.

  Conditions: EX90 is an MCU for the conference with C40 & SX20.

  Workaround: There is no workaround.

- CSCuj52382

  Symptom: MAC acl drops on popinac with isis_frr configs.

  Conditions: This symptom is observed when verfiying the isis neighbors.

  Workaround: There is no workaround.

- CSCuj53771

  Symptom: Only audio is recorded for basic DO_EO video call.

  Conditions: This symptom is observed when the outbound leg is the anchor leg for a basic DO_EO video call, then only audio gets recorded for the EO leg.

  Workaround: It works fine for DO_DO and EO-EO video calls. Also, if we make inbound as the anchor leg for DO_EO video call, video is recorded.

- CSCuj56505

  Symptom: SCCM phone registration on CCM via ASR1k does not happen.

  Conditions: This symptom is observed when ASR1k is configured with NAT configuration.

  Workaround: There is no workaround.

- CSCuj57537

  Symptom: A CUBE router may reload when processing a SIP call.

  Conditions: This symptom is observed only in a CUBE HA pair.

  Workaround: There is no workaround.

- CSCuj62858

  Symptom: Active NAT tables in a VRF are cleared unexpectedly when unconfiguring a static NAT belonged to other VRF.

  Conditions: This symptom is observed when following conditions are met. - 'network' option is used in the NAT rule. - The NAT rule which is to be unconfigured has overlapped local/global addresses with other NAT rules.

  Workaround: There is no workaround.

- CSCuj67593

  Symptom: ASR1K:Mac-accounting counters are not updating after MDR on Gigabit Ethernet SPA module.

  Conditions: This symptom is observed after completion of Minimal Disruptive Restart (MDR) procedure for a GigE SPA module running XE3.8 or higher release.

  Workaround: Reload the SPA slots after the MDR.

- CSCuj68565

  Symptom: ASR1000-2T 20X1GE and ASR1000-6TGE Card status will remain unknown in any slot post insertion in slot4/5 of ASR1013 with ESP40.

  Conditions: Sequence of events needed: 1. Insert the ASR1000-2T 20X1GE and ASR1000-6TGE in Slot 4 or 5 of ASR1013 with ESP40 2. Remove the card 3. Insert in any other slot other than slot 4 and 5.

  Workaround: Wait for minimum 1 minute before reinserting the card in slot other than 4 and 5 (ie 1 min wait between step 2 and 3 of Condition above)

- CSCuj69001

  Symptom: Crash after adding the ACL with the ttl option to QoS policy.

  Conditions: Create a policy with ACL containing ttl option. AND Attach this policy to an interface AND Send non-ip traffic (mpls or l2) to this interface. This has been seen on ASR1002 running asr1000rp1-advipservicesk9.03.06.00.S.152-2.S after adding the following: permit icmp host x.x.x.x host x.x.x.x ttl gt 20

Workaround: Don't use an ACL with ttl option in QoS policy. OR Add IPv6 class-map also to QoS policy.

```
Example: Ipv6 access-list v6_acl   Permit ipv6 any any Class-map match-any v6_class
<---< Add this class to QoS policy   Match access-group name v6_class
```

- CSCuj71234

  Symptom: Tracebacks with the following signature "%QFPOOR-4-LOWRSRC_PERCENT" are seen on the console with negative percentage complaining of resource depletion.

  Conditions: These tracebacks are usually seen on a clean-up operation performed on a router i.e manual removal of all configs. But it's not limited to only this operation and could be seen with router configuration as well.

  Workaround: There is no workaround.

- CSCuj71839

  Symptom: CLI hang in SBC adjacency sip mode.

  Conditions: This symptom is observed when over 2000 sbc sip adjacencies are configured.

  Workaround: There is no workaround.

- CSCuj74513

  Symptom: The ha test case about 96k sessions of EoGRE can not support on esp40 currently.It hit the system limitation.

  Conditions: When it reaches the upper limit, the router crashes. The exmem not enough is not the root cause of crash, but a trigger event. After analyzing, the traceback was caused by the code defect which was fixed in code diff. The exception handling is not very robust for out of memory.

  Workaround: There is no workaround.

- CSCuj79195

  Symptom: ASR router crashes when platform hardware debug is enabled.

  Conditions: Platform hardware debug is enabled.

  Workaround: There is no workaround.

- CSCuj79732

  Symptom: H323 HA adjustment.

  Conditions: H323 HA adjustment.

  Workaround: There is no workaround.

- CSCuj80062

  Symptom: Unexpected RP reload in asr1k.

  Conditions: Stream of corrupted ATM cells on idle VCC due to SIP hardware failure.

  Workaround: There is no workaround.

- CSCuj82693

  Symptom: ESPs going offline and remaining in "disconnecting" state for a few minutes, until fman_fp and cppc_cp processes failures.

  Conditions: This symptom is observed when %CPPBQS-3-QMOVESTUCK: Fx: cpp_cp: QFP 0 schedule xxx queue move operation is not progressing as expected.

  Workaround: There is no workaround.

- CSCuj84219

  Symptom: Error messages shown on KS after SW upgrade to 15.2(4)M. Whenever a GM with multiple GDOI groups registers, an error message is logged on the respective KS: Oct 4 11:31:28.477 CEST: %CRYPTO-6-IKMP_NO_ID_CERT_FQDN_MATCH: ID of ce-de-xxxxx.wan.domain.net (type 2) and certificate fqdn with ce-de-xxxxx.

  Conditions: This symptom is observed when multiple GDOI groups with different GETVPN local-addresses configured on GM. GM/KS are ISR G2 routers running on 15.2(4)M code.

  Workaround: Configure "crypto isakmp identity dn", i.e. set the ISAKMP identity to the distinguished name (DN) of the router certificate. http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html#wp1060149

- CSCuj85408

  Symptom: For VPLS mstp test Bpdus are not receiving.

  Conditions: This symptom is observed when packet drops are seen.

  Workaround: There is no workaround.

- CSCuj86393

  Symptom: cpp_cp process crashes on ESP100, ESP100 or ASR1002-X.

  Conditions: Bring up 4k PPPoLNS sessions. Tear-down large number of sessions (eg. >3k) by performing "shut" on individual Dialer interfaces one-by-one on CPE.

  Workaround: There is no workaround.

- CSCuj87942

  Symptom: 488 based fallback with Flow-Around doesn't work in video call.

  Conditions: This symptom is observed when "media flow-around" CLI is configured.

  Workaround: There is no workaround.

- CSCuj91523

  Symptom: An ESP crash is seen. This will cause forwarding to stop for a few minute. It is observed after making some changes to Netflow and AVC.

  Conditions: The issue was first seen on 15.3(2)S1. This crash may happen if ALL following items are true:

  1.AVC monitor is configured. [It will implicitly start NBAR] It means You have configuration like:

  ```
  flow?record?type?performance-monitor?avc-mnitor
  match?application?name?account-on-resolution  <or>
  performance?monitor?context?art?profile?application-experience
  traffic-monitor?application-response-time
  ```

  2.NBAR MTP is enabled. It may be enabled implicitly as result of protocol pack replace: ip nbar protocol-pack <pp-file>

  Workaround: There is no workaround.

- CSCuj91680

  Symptom: ESP crashes running 3.9.1 when NAT enabled.

  Conditions: NAT must be enabled.

  Workaround: There is no workaround.

- CSCuj92836

  Symptom: The described issue is an XE only issue that impacts several AVC fields.

```
Fields list:  Field
Export id Introduced in RLS Fix RLS  connection sum-duration                      279
3.4                      3.10.2, 3.11.1  connection new-connections
278 3.4                       3.10.2, 3.11.1  connection client counter bytes network
long 41106 3.9                       3.10.2, 3.11.1  connection server counter bytes
network long 41105 3.9               3.10.2, 3.11.1 policy qos queue drops
42129 3.9                      3.10.2, 3.11.1
```

  These fields show incorrect value. Problem cause: When cache record is reused, these fields are not cleared. Since they are accumulative fields, they report constantly increasing values. Full fix for this issue is clearing these fields using general FNF mechanism that does it. Since this fix has ISSU impact, we will do it in 3.12. In 3.10.2 and 3.11.1 we will provide a partial fix that clears these fields differently.

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCuj94188

  Symptom: Unaccounted drops in Ethernet Line card for Multicast traffic.

  Conditions: When Multicast traffic is sent more than the ESP performance limit, due to ingress back pressure from ESP causes overruns in the Line card but these drops are not showed in the overruns

  Workaround: There is no workaround.

- CSCuj98769

  Symptom: ESP crash after entering "debug platform condition stop" on an ASR1k with ISG feature set enabled and active subscribers.

  Conditions:

```
ASR1k(config)#ip access-list extended SMTP
ASR1k(config-ext-nacl)#permi
ASR1k(config-ext-nacl)#permit tcp
ASR1k(config-ext-nacl)#permit tcp any any eq 25
ASR1k(config-ext-nacl)#end
debug platform condition ipv4 access-list SMTP
debug platform packet-trace packet 8192
debug platform condition start
debug platform packet-trace enable
show platform packet-trace summary
debug platform condition stop
```

  Workaround: There is no workaround.

- CSCul00473

  Symptom: If multiple variations of the same codec are offered and a voice-class is defined to allow said codec, only the first variation in the SDP message is retained, the rest are filtered-out.

  Conditions: Multiple variations of the same codec are offered and filtering with voice-class is enabled.

  Workaround: There is no workaround.

- CSCul02627

  Symptom: UEA: Log files are not generated with PTP configs.

  Conditions: Configure RSP2 as the slave and RSP1 as the master Go to shell using "request platform software system shell" cd /tmp/rp/trace ls -ltr. Notice that the log files related to PTP aren't present.

  Workaround: Reload RSP2.

- CSCul02786

  Symptom: The original issue fails silently and it is only detected via traffic or inspecting the hierarchy via the CLI, show plat hard qfp act feat qos que out int <ifname> hier detail. The QoS rates are in accurate due to a bad hierarchy. Subsequent crashes and the issue that is documented in this DDTS were regression from the original fix intended to build the hierarchy on ESP-100 correctly. All issues involved fair-queue in a flat or hierarchical policy when applied on the fly.

  Conditions: Applying fair-queue on the fly resulted in the bad hierarchy. As a result the provisioned services could not be guaranteed.

  Workaround: There is no workaround.

- CSCul03067

  Symptom: Tunnel interface QoS tail drop counter reported at physical interface. Service policy is applied on the tunnel 5432. --Drops are seen on the output of "show policy-map tunnel 5432" --Drops are seen on the physical interface over which the tunnel is built. --NO drops are seen on the Tunnel interface. --From the output below OQD is "0" for the tunnel interface.

```
BGL.Q.20-ASR1K-1# show platform hardware qfp active statistics drop
------------------------------------------------------------------------ Global Drop
Stats                          Packets                  Octets
------------------------------------------------------------------------TailDrop
753351           63281484    BGL.Q.20-ASR1K-1#show inter summary
<snip>  Interface                    IHQ       IQD       OHQ       OQD      RXBS
RXPS      TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------
---------------------------  * GigabitEthernet0/0/1          0         0         0
753351        0         0    735000     1094        0  * GigabitEthernet0/0/2
0         0         0         0   8648000     18016         0         0         0  *
Tunnel5432                    0         0         0         0         0         0
12697000     22674         0
```

  Conditions: When packets are dropped on a tunnel interface, the output of: - show platform hardware qfp act interface all statistics drop_summary - show interface summary would only show the dropped packets against the phsyical interface, which made it difficult to determine which tunnel the packets were being dropped on.

  Workaround: There is no workaround.

- CSCul04033

  Symptom: LDP stays down over Multilink when connecting to Juniper router.

  Conditions: Issue notice with latest IOS as same setup was working with 15.0(1)S1(3.1S) and earlier release.

  Workaround: There is no workaround.

- CSCul04434

  Symptom: Given a GETVPN GM that is configured with an ipv6 crypto map, if that crypto map is applied to two interfaces (one common identity, e.g. loopback) and if certain configuration operations are performed, the GM will loose connectivity to the ipv6 group. If the GM has dual-stack interfaces with both an ipv4 and an ipv6 crypto map. The IPv4 GETVPN functionality will not be affected while triggering the event documented in this defect.

  Conditions: Performing configuration operations that follow the patterns described below:

  IPv6 Crypto Map applied to two interface (E0/0 and E2/0, lets call them Primary and Secondary) At this stage all works well IPv6 traffic is encrypted between two test GMs.

  1. Shut down Secondary interface (E2/0)

  Result, no change in functionality GM can still exchange encrypted IPv6 traffic with peers.

  2. Remove the ipv6 crypto map from the Primary interface (E0/0, while E2/0 is in admin shutdown state).

  Result, IPv6 traffic is sent out in clear text

  3. Re-apply crypto map to the Primary interface (i.e. E0/0)

  Result, no change, packets are still being sent out in clear text, even though GDOI sees the E0/0 interface as associated with the cry map and group.

  4. Remove the crypto map from the Secondary interface which is still in shutdown state

  Result : No change in the behavior

  5. Remove and re-apply the crypto map on the Primary interface

  Result: GM re-registers

  Workaround: Remove the ipv6 crypto map from the Secondary Interface before shutting it down.

- CSCul04900

  Symptom: Hydrogen serviceability Feature crash in Xe 311 image As per crash decode snippet, serviceability/event trace code crashed

```
Traceback summary   -----------------   % 0x8a57439 : __be_strcmp   % 0x1372b17 :
__be_sympBuffCallingNumCompare   % 0x89884ce : __be_avl_search   % 0x1373a99 :
__be_symp_et_search_cover_buffer_in_filt_table   % 0x1373b99 :
__be_symp_et_insert_cover_buffer_to_filt_table   % 0x13754fc :
__be_symp_upd_event_trace_instance   % 0x10417a9 : __be_ccsip_api_call_setup_ind   %
0xf555a4 : __be_sipSPIContinueNewMsgInvite   % 0xf54cf8 :
__be_sipSPIHandlePostPreauthInvite   % 0xf52a20 : __be_sact_idle_new_message_invite
% 0xf523ad : __be_act_idle_new_message   % 0xf5127a : __be_sipSPISipIncomingMsg   %
0xf4f821 : __be_sipSPILocateInviteDialogCCB   % 0xf4e5b5 :
__be_ccsip_new_msg_preprocessor   % 0xf4c55a : __be_ccsip_spi_process_event   %
0xf4bedc : __be_ccsip_process_sipspi_queue_event Call flow : srv_dbg_cat_lvl_03 TC
execution.  ================================================      Topology
sipp----ASRCUBE----SIPP    Core file path
:/auto/tftp-rts/ASR-CUBE_RP_0_linux_iosd-imag_16315_1382531279.core.gz    Passed image
:15.4(0.19)S0.4  failed Image :15.4(0.19)S0.8
```

  Conditions: This symptom is observed under:

  1. Trace commands enabled at common_setup section, monitor event-trace voip ccsip fsm monitor event-trace voip ccsip msg monitor event-trace voip ccsip misc monitor event-trace voip ccsip api monitor event-trace voip ccsip global monitor event-trace voip ccsip limit connections 1000 monitor event-trace voip ccsip stacktrace 8 monitor event-trace voip ccsip history enable" monitor event-trace voip ccsip history clear" monitor event-trace voip ccsip all enable"

2. By default all feature codes and log level are enabled at particular TC setup section

3. Single audio call is established, after 4 to 5 sec. crash occurred.

Workaround: Passed image :15.4(0.19)S0.4

- CSCul06361

  Symptom: When subscriber session is created with 'ip subscriber interface' on subinterface in shutdown state, after bringing the subinterface up, the 'out' pkt counters are not increasing. Subscriber does not have IP connectivity, since traffic is going only in one direction.

  Conditions: ASR1k ISG running IOS XE 3.7.4.S (15.2(4).S4), with 'ip subscriber interface' created from subinterface in shutdown state.

  Workaround: Clearing subscriber session when subinterface is up/up will re-establish session with connectivity restored.

- CSCul06398

  Symptom: Reach max CPU utilization when rate is much below 500K CPS.

  Conditions: Do 500K CPS rate performance test on ESP80.

  Workaround: There is no workaround.

- CSCul07210

  Symptom: ASR1000-2T 20x1GE and ASR1000-6TGE cards can go into reload with certain combinations QinQ scale config.

  Conditions: Card reload with scale config.

  Workaround: There is no workaround.

- CSCul08311

  Symptom: SIP ALG will drop NAT traffic.

  Conditions: In a case, FQDN instead of IP address is included in the "c=" line of SDP in the 200 OK response, and SIP ALG will drop this message.

  Workaround: Turn off SIP ALG if SIP server (VCS) can support NAT traversal by itself. Another way is to let VCS fill IP address instead of FQDN in the "c=" line of SDP if possible.

- CSCul10907

  Symptom: ASR1002x or ASR1000 with an ESP100 may crash when Broadband MLPPP sessions with QoS applied are brought up or the sessions flap.

  Conditions: This issues causes a ASR1K crash (cpp_cp_svr) when a Broadband MLPPP bundle with QoS is applied is brought up or the session flaps. Problem is most prevalent on MLPPP Bundles with two or more member links. Affects MLPPPoE, MLPPPoA, MLPPPoEoA, and MLPPPoLNS.

  Workaround: There is no workaround.

- CSCul15647

  Symptom: Classification by ACL in QoS is broken when using it with IPSec tunnel.

  Conditions: Use ACL for classification in policy-map and apply a QoS to physical interface -qos pre-classify is configured under IPSec tunnel.

  Workaround: Apply a QoS to IPSec tunnel.

- CSCul16541

  Symptom: cpp_cp_svr crash with model F QoS and multiple PPPoEoA/PPPoA VCs on one or more ATM PVPs.

Conditions: While bringing up multiple PPPoEoA/PPPoA sessions with model F QoS on one or more ATM PVPs.

Workaround: There is no workaround.

- CSCul18092

  Symptom: The configured file name in "monitor pcm-tracer capture-destination <name> " is not used to create the file.

  Conditions: Only exists in O2 NIM-T1E1 module.

  Workaround: There is no workaround.

- CSCul18806

  Symptom: ELC MDR: Reconcile failed for int_num 0x1505F000 bitmap 0x00001E7F.

  Conditions: Observed during one-shot consolidated MDR.

  Workaround: There is no workaround.

- CSCul20010

  Symptom: The user will see the system shaping to too low a rate when a tunnel moves to a faster interface, and shaping to too high a rate when a tunnel moves to a slower interface.

  Conditions: Upon a dynamic move of a tunnel to a link with a different speed and the QoS configuration option "shape average percent" has been applied, then rates are not automatically re-calculated.

  Workaround: The workaround to this issue is to avoid "shape average percent" when possible. If not possible, then after a tunnel moves occurs modify the shaping percent by plus or minus.

- CSCul21158

  Symptom: ESP crashes for IOS-XE based platforms.

  Conditions: Crash may occur when executing the CLI command: show platform hardware qfp active infrastructure exmem map.

  Workaround: There is no workaround.

- CSCul22381

  Symptom: Unexpected tracebacks occur randomly at a very slow rate (i.e. once per day or even less). Normal processing will continue.

  Conditions: This issue is specific to ESP100, ESP200 or ASR1002-VE.

  Workaround: There is no workaround.

- CSCul22733

  Symptom: ASR router crashes.

  Conditions: The symptom is observed under the following conditions:

  1. Flow exporter defined with the Management interface GigabitEthernet0 configured as source.

  2. An FNF record is configured to collect URL name.

  3. FNF monitor using the above record and exporter is configured on an interface with MTU > 1500 bytes.

  4. A packet with URL > 1500 bytes hits the monitor

  Workaround: DO not configure the Management interface as flow exporter source.

- CSCul24332

  Symptom: 000080: *Nov 5 06:20:08.231 UTC: %OCE-3-MISSING_HANDLER_FOR_SW_OBJ_TYPE: Missing handler for 'non choice oce get next' function for type Loadbalance -

  ```
  Traceback= 1#fa53c8e50eb34ad6b14c6e73742aa633  :400000 8D10D1 :400000 33C98B4 :400000
  441693F :400000 6CEEAC2 :400000 33E118C :400000 33ADE6F :400000 3355C80 :400000
  335590D :400000 33A9B82 :400000 33A9299 :400000 33AF9C9 :400000 33AF82F :400000
  34A0183 :400000 349FF99 :400000 346EE86 :400000 1622694
  ```

  Conditions: In vrf Mgmt-intf, there are 8 prefixes referring to same adjacency.

  Workaround: There is no workaround.

- CSCul25109

  Symptom: After RP1 reload, the templates are not sent at the first interval even if the monitor is ready.

  Conditions: Affects features that make use of the High Speed Logger to export records to a off box collector. Generally, this will only happen when the route used by the exporter is slow to be established.

  Workaround: There is no workaround.

- CSCul25833

  Symptom: Issue with Dual Collector FNFV9 in ASR 1002-x only one collector is collecting and the second one is not.

  Conditions: Under flow-monitor provisioning.

  Workaround: Apply each flow monitor with a gap of 5secs. However, this will be customer impacting since many of this is controlled by scripts.

- CSCul27083

  Symptom: Ucode crashes.

  Conditions: Ucode crashes while doing RP switchover with 1000 ipv6_ipsec tunnels and acls with traffic.

  Workaround: There is no workaround.

- CSCul27444

  Symptom: The as1002-x crashes while processing the MLPoLNS configuration. The model F configuration that would cause the crash is attached to the DDTS.

  Conditions: When a grandparent policy is attached to a vlan sub-interface configured as a queue, it needs to be converted to a leaf node schedule when a session (MLPPP member link) is added to the vlan. During the transformation of a queue to a leaf schedule, all queues were not moved in the same event as required due to a hardware restriction.

  Workaround: There is no workaround.

- CSCul31100

  Symptom: COS markings not seen Proper on the dot1q interface.

  Conditions: The issue will be seen if any of following conditions are met:

  1. Crypto-Map implemented in Transport mode implemented on Tunnel.

  2. Fragment happened in data plane on the dot1q interface;

  Workaround:

1.Remove Encryption from the Tunnel or downgrade IOS to 15.0(1)S3 if the issue is happened with IPSec but no fragment;

2. No workaround if the issue is happened with big enough packet(need fragment);

- CSCul31192

  Symptom: ESP may crash @ipv4_nat_alg_prune_sd

  Conditions: seen with SIP traffic

  Workaround: There is no workaround.

- CSCul34313

  Symptom: Active FP crashes on removing nat mapping.

  Conditions: Dynamic acl using route-map.

  Workaround: There is no workaround.

- CSCul34776

  Symptom: After ISSU process AOR and dependent fields are not working. Also, sampler granularity may be different from the configured.

  Conditions: There are no known conditions.

  Workaround: Remove AVC configuration and apply it again after the ISSU process is finished Sometimes during ISSU process several flags may not be downloaded properly. These flags are AOR, dependent field flags, sampler granularity flag and enterprise number.

- CSCul39211

  Symptom: With an IOS router set as an EZVPN client, with either interactive (CLI) or HTTP-Intercept authentication enabled, if the user does not enter in proper credentials within 10 seconds, the router will resend AM3 to the EzVPN server. This causes a retransmission storm to trigger and quickly tear down the tunnel, which causes the authentication to fail.

  Conditions: IOS router acting as EzVPN client.

  Workaround:

  1) Have users enter credentials within 10 seconds of login prompt.

  2) Save credentials on router so users don't need to enter them every time.

  3) Downgrade to 15.1(4)M5 or earlier.

- CSCul41442

  Symptom: In the M train of IOS and the S train of IOS-XE the "media anti-trombone" feature added in 15.1(3)T CUBE does not appear as an option when configuring "voice class media" groups. It is not present as an option at the dial-peer level as well.

  Conditions: This symptom is observed in any non "T" train of IOS and IOS-XE. IOS Tested 15.2(3)T - Available as media option Tested 15.3(3)M - Not there IOS-XE Tested 15.1(3)T - Available as media option Tested 15.3(3)S1 - not there

  Workaround: Customer has to have a "T" train IOS of Cisco IOS Release 15.1(3)T or higher. Impacts customers ability to deploy Cube Enterprise solutions.

- CSCul43587

  Symptom: Ucode crash.

  Conditions: On removing at cgn mode.

  Workaround: There is no workaround.

- CSCul48822

  Symptom: While provisioning an ISG IP Subscriber session it is possible to leak an ESS segment chunk (IOSXE ESS SEG).

  Conditions: The memory leak may occur when there is an error provisioning an ISG IP subscriber session.

  Workaround: There is no workaround.

- CSCul48865

  Symptom: Some static vrf nat entries which are stored in the startup-config don't appear in the show running.

  Conditions: After reloading the router.

  Workaround: There is no workaround.

- CSCul51296

  Symptom: Connections timed out after RP switchover.

  Conditions: The symptom is observed when connection reset after RP switchover. Not able to establish new connections.

  Workaround: Re-enable Service Context. Problem happens in about 1 in 10 RP switchover on ESP20. This had not been with other ESP so far.

- CSCul54826

  Symptom: Software mode BFD session under p2mp ATM interface with vrf cannot be UP.

  Conditions: Software mode BFD session under p2mp ATM interface with vrf.

  Workaround: Change the session to Hardware offloaded mode.

- CSCul55038

  Symptom: In mpls-vpn scenario, when the size of packet coming from core network is bigger than mtu set on CE facing interface, the expected ICMPv6 TOO_BIG fail to return.

  Conditions: The symptom is observed when 1. packet is bigger than mtu on CE facing interface. 2. the packet comes from core mpls network and try to go through CE facing interface. 3. the issue is found on PE in mpls-vpn scenario.

  Workaround: Enable IPv6 on core facing interface, which is receiving the mpls packet to CE.

- CSCul59525

  ```
  Symptom: ASR1K cube running Cisco IOS Release XE3.8S, many hung calls are seen over a
  period of one week. There are three different symptoms of hung call legs.
  Example 1: One of the call leg is in stuck state Example 2: Both the call legs are
  active and connected and stuck for more than a week Example 3: Both call legs are
  stuck in disconnect state but one of the call is connecting and other leg is in active
  state.
  Topology: VzB ---sip----CUBE------sip------SME Cluster-----sip------Admin04
  cluster---------IP Phones
  |                            |
  |                ----------------sip trunk to fax server
  |                                                                        |
  ------------------SIP trunk to Unity connection vm
  ```

  Conditions: Though the reason for this issue is unknown, it is very random in nature. Hung calls are seen for a normal sip to sip calls going to IP phone, or calls that routes to unity connection voicemail and also stuck fax calls.

  Workaround: There is no workaround.

- CSCul61683

  Symptom: Error messages similar to below may be displayed on the console due to stale stats usage:

  ```
  SCOOBY-5-SERIAL_BRIDGE_EVENT_RATE:<Any_Message_Here>
  ```

  Conditions: There are no known conditions.

  Workaround: There is no workaround.

- CSCul63125

  Symptom: Inbound calls that are consultant transferred back out to the ITSP through the same CUBE experience no audio after transfer and drop 2 seconds after the transfer is complete. In the debugs the final Reinvite (DO) from CUCM gets a 100 Trying from the CUBE but no 200 OK response. In this scenario the CUCM sends a BYE 12 seconds later with a disconnect cause of 47.

  Conditions: The issue occurs on calls that ingress and egress through the same CUBE when a consult transfer is performed.

  Workaround: Ensure that MTP required is not checked on the SIP trunk in CUCM.

- CSCul64097

  Symptom: ZBFW SYN cookie counter shows positive number although the real number of half open sessions have dropped to zero. Since the counter is used to trigger SYN cookie once it is over the configured limit, this is causing the SYN cookie protection to always kick in regardless of the real situation, which drags down the network performance.

  Conditions: SYN cookie feature needs to be configured, and it is configured to protect per VRF or global number of half open sessions. The counter error only happens under some race condition which needs particular and supposedly high traffic load to trigger.

  Workaround: Disable the SYN cookie. The counter problem only happens under certain corner case. When the counter goes wrong, the SYN cookie protection logic could be triggered erroneously.

- CSCul64664

  Symptom: After VC goes down, the packets are received on xconnect interface are leaked.

  Conditions: This symptom is observed when VC goes down -Unicast packet with TTL>=2 are received on that xconnect interface -When having the route for the destination of the unicast packets.

  Workaround: Remove the route from the routing table -apply an ACL to deny these leaked packets.

- CSCul65547

  Symptom: When CUBE negotiated KPML and rtpnte and REFER received and passed across on that leg while originating Leg disconnecting the call and other leg still hung never cleared.

  Conditions: When CUBE negotiated KPML and rtpnte and REFER received and passed across on that leg while originating Leg disconnecting the call and other leg still hung never cleared.

  Workaround: There is no workaround.

- CSCul67310

  Symptom: ASR1K microde crash with either of the following errors

  ```
   SOR_CSR32_SOR_ERR_LEAF_INT__INT_SOR_OPF_GRANT_PTCL_UVF
  OPF_CSR32_OPF_LOGIC_ERR_LEAF_INT__INT_START_OF_BURST_MARKER_ERR
  ```

  Conditions: This issue ONLY affects on ASR1002x and ASR1K RP2/ESP100 based platforms running 15.2(4)S, 15.3(1)S, 15.3(2)S, 15.3(3)S, and 15.4(1)S based images. This issue can occur on platforms with scaled sub-interface or broadband session configurations when the number of

sub-interfaces or sessions on a interface is reduced from > 4000 to less than 4000 and moderate to heavy traffic flow is occurring at the time that the sub-interface or session count is reduced. If the the ASR1K is operating below this threshold or above this threshold this issue is not seen.

Workaround: There is no workaround.

- CSCul68308

  Symptom: CPUHOGs will be observed on the system.

  Conditions: When Ethernet line card is configured scaled QinQ configuration with inner vlan as a range with and without custom classification configuration, during Reload of linecard or Shut & no Shut of interface causes CPUHOG on the Linecard.

  Workaround: Instead of using single sub interface with Range of inner vlan, divide this inner vlan into multiple ranges and configure multiple subinterfaces on the same interface.

- CSCul68429

  Symptom: FP crash while testing PPoE sessions.

  Conditions: Applying nat settings to CGN mode.

  Workaround: There is no workaround.

- CSCul70833

  Symptom: Byte-based queue-limit does not work correctly when fair-queue is configured.

  Conditions: -Using fair-queue feature simultaneously. The issue can happen on ASR1k. The issue is found on 15.3(3)S.

  Workaround: Use packet-based queue-limit instead of byte-based queue-limit.

- CSCul74010

  Symptom: Memory leak in ASR in sip-kpml call-flow.

  Conditions: This issue is observed when sip-kpml is configured on dial-peers.

  Workaround: There is no workaround.

- CSCul78163

  Symptom: cpp_cp_svr process crashes.

  Conditions: On ESP100, ESP200 or ASR1002X platforms, when scaling over 4000 nodes on an interface or sub-interface and then nodes are removed or deleted so the total drops below 4000, the cpp_cp process can crash. This can also happen on all ASR1K platforms with ATM interfaces when moving ATM VCs from one COS to another COS and then deleting the ATM VCs at the same time.

  Workaround: Avoid scaling past 4000 scheduling nodes on the same interface or sub-interface on ESP100, ESP200 or ASR1002X when there is a chance the nodes can come and go causing the total to drop below 4000. Avoid deleting ATM VCs at the same time the VC is being reconfigure with a different COS value.

- CSCul80160

  Symptom: Ucode crash while disabling flow entry.

  Conditions: With nat outside mapping.

  Workaround: There is no workaround.

- CSCul81353

  Symptom: ASR1006 with RP2 running ES version based on Version 15.3(1)S crash with Segmentation Fault ---snip-- UNIX-EXT-SIGNAL: Segmentation fault(11), Process = CCSIP_SPI_CONTROL -

```
Traceback= 1#9821b08208133f5124c039ddebb8173b  :400000 347A664 :400000 7B14A0F :400000
7B0F5E7 :400000 8F6C8A :400000 9A8C4C :400000 9B6951 :400000 95F2A4 :400000 962772
:400000 BE9018 :400000 BE8E4F ---snip--
```

After the RP Switch over all the new calls were rejected with the following errors as well, which may be unrelated to the crash

```
--snip-- Dec  2 15:11:47: %VOICE_IEC-3-GW: SIP: Internal Error (INVITE, codec
mismatch): IEC=1.1.278.7.110.0 on callID 17334189  Dec  2 15:11:49: %VOICE_IEC-3-GW:
SIP: Internal Error (INVITE, codec mismatch): IEC=1.1.278.7.110.0 on callID 17334212
Dec  2 15:11:49: %VOICE_IEC-3-GW: SIP: Internal Error (INVITE, codec mismatch):
IEC=1.1.278.7.110.0 on callID 17334218 ---snip---
```

Conditions: After two weeks of uptime and during normal load condition.

Workaround: Reboot the box to recover from the situation. The core file writing is incomplete as

```
TEMP_IN_PROGRESS  ---- show stby-harddisk: all-----  142 2406627691 Dec 02 2013
14:11:14  00:00 /harddisk/core/kernel.rp_20131202191114.core.gz  149   79237120 Dec 02
2013 14:03:52  00:00
/harddisk/core/nyorbgdnesbc-dr_RP_0_linux_iosd-imag_6335.core.gz.TEMP_IN_PROGRESS
```

- CSCul83474

  Symptom: ESP crash.

  Conditions: This symptom is observed when executing "no ip cef load-sharing algorithm include-ports destination" with high throughput about 10Gbps.

  Workaround: There is no workaround.

- CSCul90782

  Symptom: When "show cube status" is issued on a 3925 or an RP1 platform, it shows the CUBE version to be 9.0, whereas it should be 10.0.0

  ```
  CUBE#sh cube status CUBE-Version : 9.0 SW-Version : 15.4.1.T, Platform
  CISCO3925-CHASSIS HA-Type : none Licensed-Capacity : 20  ASR1002-R1#show cube status
  CUBE-Version : 9.0 SW-Version : 15.4.1.S, Platform ASR1002 HA-Type : none
  Licensed-Capacity : 200
  ```

  Conditions: Some ISR G2 platforms or ASR1K platforms running CUBE on IOS/IOS-XE version 15.4(1)T/XE3.11

  Workaround: There is no workaround.

- CSCul93292

  Symptom: Ucode crash with alg traffic when there is flow passing through physical interface with nat configuration vasi interface with nat configuration in the same box.

  Conditions: Ucode crash with alg traffic.

  Workaround: Disable all the algs

- CSCul95089

  Symptom: AAA sessions are lingering for old connections.

  Conditions: Running Flex VPN server with accounting, clients are identified by email id.

  Workaround: There is no workaround.

- CSCul97315

  Symptom: ESP crashes when using IOS-XE packet-trace.

  Conditions: A crash will occur when using IOS-XE packet-trace to trace per packet data and an IPv6 fragment is encountered by packet-trace.

```
Example setup follows:    # enable packet-trace  debug platform packet-trace enable
# enable per packet tracing of 16 packets  debug platform packet-trace packet 16    #
enable tracing packets that enter g0/0/0 and start tracing  debug platform condition
interface g0/0/0 ingress  debug platform condition start
```

Workaround: Do not trace IPv6 traffic that is fragmented.

- CSCum09702

  Symptom: OSPF neighbors can not establish FULL adjacency over dmvPN tunnels.

  Conditions: This symptom is observed when dmVPN with OSPF is configured on IOS-XE platforms.

  Workaround: There is no workaround.

- CSCum10676

  Symptom: Router crashes during multicast replication.

  Conditions: There are no known conditions.

  Workaround: Following is the config to change the age timers. You can adjust this age time based on their requirement. ARP aging time config:

```
 -------------------  ASR(config)#int BDI164  ASR(config-if)#arp timeout ?
<0-2147483>  Seconds  ASR(config-if)#arp timeout 1800  ASR(config-if)#end      MAC
aging time config:  -------------------  ASR(config)#bridge-domain 164  ASR
(config-bdomain)#mac aging-time ?    <30-3600>  Aging time in seconds, default 300
seconds (or 1800 seconds for              overlay bridge domains)
ASR(config-bdomain)#mac aging-time 1810
```

  This problem will happen if the MAC entry is age out before the ARP entry of the given Host. So, if we configure the MAC age, slightly more than ARP age, then, the crash does not occur.

- CSCum13126

  Symptom: After initiating an RP fail-over either through redundancy force-switchover or by using test crash, MLPPP interface remains down though T1's are up. Either shut/no shut of 1 of the member links or clear ppp all brings the MLPPP interface back up.

  Conditions: Trigger: RP fail-over seems to be the Trigger, apart from which there do not have to be any associated config changes made.

  Workaround: There is no workaround.

- CSCum14041

  Symptom: QFP error logs not displayed on IOS console.

  Conditions: This symptom is observed in IOS-XE 3.10/15.3(3)S and forward releases.

  Workaround: There is no workaround.

- CSCum15364

  Symptom: Router crashes with basic call while MP4A-LATM codec is used.

  Conditions: This symptom is observed when MP4A-LATM codec is used in the dial-peers.

  Workaround: There is no workaround.

- CSCum40367

  Symptom: Traceback seen while adding fair queue on existing Subscriber child policy.

  Conditions: This symptom is observed with background traffic flow.

  Workaround: There is no workaround.

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.2S

This section documents the open issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.2S.

- CSCug27362

  Symptom: Packet drop occurs when IPSEC VTI IPv6 tunnels are configured on an ESP80.

  Conditions: Packet drop occurs when IPSEC VTI IPv6 tunnels are configured on an ESP80. Also getting the following message when the problem happens:

  ```
  %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.1 Thread:207 TS:00000001059562400712
  %ATTN-3-SYNC_TIMEOUT: msecs since last timeout 1035639, missing packets 6040
  ```

  Workaround: The only workaround so far is to remove the IPSEC configuration between the tunnels.

- CSCui43325

  Symptom: Traffic blackhole for v6 SSM groups after flapping bgp loopback interface on the egress PE

  Conditions: This condition is observed during BGP loopback interface flap

  Workaround: Unconfigure-reconfigure the mdt default command under the v6 address-family for the vrf

- CSCui53563

  Symptom: Crypto-Engine(h/w encryption) is inactive

  Conditions: This condition is observed during rp_switchover the HUB and pass the traffic to bringup the tunnels UP

  Workaround: There is no workaround.

- CSCui86755

  Symptom: Add local GM ACL on the Cisco ASR 1000 Router, and remove it. Adding the ACL and removing it changes the flow priority that does not work on the Cisco ASR 1000 Router.

  Conditions: When the ACL is changed on KS or GM.

  Workaround: There are 2 workarounds:

  1. If the permit ACL is appended to KS ACL, or if the ACL is removed from bottom of KS ACL, then there is no flow priority change, and the issue is not observed there. The limitation with this workaround is that the Group config on KS has only one SA. Also, if Deny ACL is added, some packet drops are observed.

  2. Clear the GetVPN registration on the Cisco ASR 1000 Router using the clear crypto gdoi command.

- CSCul29434

  Symptom: ELC MDR: %CWAN_HA-4-IFEVENT_BULKSYNCFAIL: receive failed ifevent: 10 err

  Conditions: This condition is observed during Consolidated MDR upgrade

  Workaround: There is no workaround.

- CSCul65261

  Symptom: write bus access failed with fpd upgrade

Conditions: This condition is observed during FPD bundled upgrade

Workaround: There is no workaround.

- CSCum08864

  Symptom: When there is policy changed (either KS or GM) in Pre-PAL, ASR1K used to re-register. The reason is that in TCAM we can't insert or move SA. ACL merge was done in ACE driver, re-registration was triggered from there.

  Post-PAL, ACL merge intelligence is moved to Control plane, so ACL is changed, it does the change flow priority. The SA is inserted with second priority, ASR1K is not able to handle that.

  Conditions: This symptom is observed when an ACL is changed on the KS or the GM.

  Workaround: There are 3 Workarounds:

  1. Manually clear GetVPN registration on ASR1K using "clear crypto gdoi".

  2. If permit ACL is appended to KS ACL or ACL is removed from bottom of KS ACL, then there is not flow priority change, and issue is not observed there. Limitation with this workaround is Group config on KS has only one SA. Also if Deny ACL is added there are few packet drops are observed.

  3. EEM script which monitors Rekey Syslog and clears the registration. This is same as workaround 1, but automatically done.

  Disadvantage of this workaround is that Rekey syslog is same during normal rekey and policy change rekey, so with normal rekey also re-registration will happen.

  Sample EEM script :

```
event manager applet GM_RE_REG
event syslog occurs 1 pattern ".*GM_RECV_REKEY.*"
action 10 syslog priority warnings msg "EEM trigger workaround for CSCum08864"
action 20 cli command "enable"
action 30 cli command "clear cry gdoi" pattern "Are you sure you want to proceed"
action 40 cli command "yes"
```

- CSCum09214

  Symptom: fp crash fround when "no ip nat create flow-entries"

  Conditions: ip nat settings mode cgn no ip nat settings support mapping outside ip nat settings pap limit 250 PAT for sip traffic 300cps no ip nat create flow

  Workaround: There is no workaround.

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.1S

This section contains the following topics:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.1S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.1S.

- CSCtb34814

  Symptoms: The following error message is reported just before a crash: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error There may not be any tracebacks given for the crash.

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCtw93694

  Symptom: No calls shown when the **show call active voice brief** command is run, however many active calls are running.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCtx20903

  Symptom: Tacacs authentication fallback is not working .

  Conditions: This symptom occurs in single connection TACACS host.

  Workaround: Disable the single connection.

- CSCty77441

  Symptom: Memory leaks are observed after unconfiguring BFD sessions.

  Conditions: This symptom occurs after BFD sessions are unconfigured.

  Workaround: There is no workaround.

- CSCtz19192

  Symptom: Router crashes with the following message: `Unexpected exception to CPU: vector 1200`.

  Conditions: This symptom occurs due to a change in the bandwidth or policing rate of the dialer interface.

  Workaround: Downgrade to Cisco IOS Release 15.1(4)M4.

- CSCtz76181

  Symptom: ASR1001 or ASR1002 may report the following message after booting IOS "%IOSXEBOOT-1-BOOTFLASH_FAILED_MISSING: (rp/0): Required Bootflash disk failed or missing, reloading system.

  Conditions: This Error message is due to the internal eUSB memory device rarely not responding to the initial accesses. A reboot will address the issue. This error can occur when a specific eUSB device is used. To check the installed eUSB, perform the following command:

  ```
  Router> show usb summary  Check if the following device is present:     USB Device: STEC USB 2.0    Bus: 01 Port: 01 Cnt: 01 Speed: 480    Vendor: 136b ProdID: 0003 Rev: 1.00
  ```

  Workaround: System reboot clears the condition.

- CSCub14611

  Symptom: %IOSXE-3-PLATFORM: R0/0: kernel: physmap-flash.0: Chip not ready

  Conditions: While doing redundancy force-switchover on ASR1006 (RP1)

  Workaround: Reload ASR1006

- CSCub62493

  Symptom: iWAG GTPv1 fails to setup PDP contexts when interacting with some vendor's ggsn products due to improper default QOS profile.

  Conditions: Problem happens when interacting with certain ggsn products which do not ignore the allocation and retention value in QOS Required.

  Workaround: Since the default QOS value cannot be changed now, the only workaround would be to see whether the specific ggsn product supports ignoring the allocation and retention value or the whole qos required.

- CSCuc33131

  Symptom: In some scenarios, retransmitted packets are not accounted against the retransmitted packet count metric.

  Conditions: If retransmitted packets have the same sequence numbers and same IP IDs, they are NOT treated as retransmitted packets. This can sometimes cause the retransmission packet count to be zero (0), incorrectly, even when there are retransmitted packets.

  Workaround: There is no workaround.

- CSCuc41531

  Symptoms: Forwarding loop is observed for some PfR-controlled traffic.

  Conditions: This symptom is observed with the following conditions: - Traffic Classes (TCs) are controlled via PBR. - The parent route is withdrawn on selected BR/exit.

  Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class** command (this fixes the issue until the next occurrence).

- CSCud49546

  Symptom: ASR1000 Router Processor crashes with punted fragment-bit set multicast packets.

  Conditions: This symptom occurs when the fragment bit is set in the multicast packets, and when these packets get punted to Router Processor.

  Workaround: There is no workaround.

- CSCud81114

  Symptom: MVPNv6 traffic is not received for a random set of MVRFs after MVPN is re-configured.

  Conditions: This issue is observed only when ALL VRFs in the system are un-configured and re-configured for MVPN.

  Workaround: One possible workaround is to clear IPv6 PIM control plane state using the **clear ipv6 pim vrf <name> topology** command for the selected states on the VRFs affected.

- CSCue39456

  Symptom: There is no command options and flags for enabling or disabling the EZchip provided debug levels

  Conditions: This condition is observed on the Popinac ELC

Workaround: There is no workaround.

- CSCue50255

  Symptom: ASR1K ucode crash with interrupt cause REM_REM_MISC_ERR_LEAF_INT_INT_REM_POP_REQ_TO_EMPTY_SCHED

  Conditions: Issue can be seen on when flapping a Multilink PPP or MLFR interfaces. Timing window to hit this issue is very small so not a common occurrence on a bundle flap.

  Workaround: There is no workaround.

- CSCue59998

  Symptom: Some kernel failure messages (e.g. COMRESET failed) may be seen on the console logs.

  Conditions: This symptom is observed when performing a soft OIR of the NIM-SSD module or after the chassis comes up following a power cycle.

  Workaround: There is no workaround.

- CSCue66938

  Symptom: esp-gmac 256 performance of 1400B packets is much less than esp-gcm 256, 20Gbps vs. 30.4Gbps.

  Conditions: suite-B transform set esp-gmac 256 vs. esp-gcm 256.

  Workaround: There is no workaround.

- CSCue75395

  Symptom: It is very difficult to debug empty video recordings

  Conditions: For all video recording calls

  Workaround: Do packet capture

- CSCue76102

  Symptoms: Redistributed internal IPv6 routes from v6 IGP into BGP are not learned by the BGP neighboring routers.

  Conditions: This symptom occurs because of a software issue, due to which the internal IPv6 redistributed routes from IGPs into BGP are not advertised correctly to the neighboring routers, resulting in the neighbors dropping these IPv6 BGP updates in inbound update processing. The result is that the peering routers do not have any such IPv6 routes in BGP tables from their neighbors.

  Workaround: There is no workaround.

- CSCue83683

  Symptoms: The Agent Greeting is not played out.

  Conditions: This symptom is observed with the Agent Greeting Call Flow using CVP.

  Workaround: There is no workaround with this build.

- CSCue86166

  Symptom: The interrupt infrastructure is in place; the userspace handling of interrupt delivery to Aggregation ASIC userspace driver code is not being done correctly.

  Conditions: This fixes the userspace handling of interrupt delivery to Aggregation ASIC userspace driver code

  Workaround: There is no workaround.

- CSCue89779

Symptom: A FlexVPN spoke configured with an inside VRF and front-door VRF may have problems with spoke-to-spoke tunnels if they are not the same. During tunnel negotiation, two Virtual-access interfaces are created (while only one is needed), the one in excess may fail to cleanup correctly. As a result, the routes created by NHRP process may lead to loss of traffic, or traffic may continue to flow through the Hub.

Conditions: This symptom occurs when the VRF used on the overlay (IVRF) and the VRF used on the transport (FVRF) are not the same.

Workaround: There is no workaround.

- CSCue92027

  Symptom: RP crashed due to redzone corruption.

  Conditions: crashing because of improper memory management.

  Workaround: There is no workaround.

- CSCue92733

  Symptom: An open routing application cannot install a route into the router.

  Conditions: This symptom is observed when the application sets up the route with Null0 as a next-hop interface.

  Workaround: There is no workaround.

- CSCue93599

  Symptom: Input characters can be dropped or garbled when copy/paste is used for module console input.

  Conditions: When copy/paste is used to send characters to the module console sessions, it is possible for characters to get dropped, or not displayed properly during the module session.

  Workaround: Manually enter any input needed on the module console rather than using cut/paste to send large amounts of text to the module console.

- CSCuf09198

  Symptom: After deleting a VRF, you are unable to reconfigure the VRF.

  Conditions: BGP SAFI 129 address-family is not configured, but unicast routes are installed into multicast RIB to serve as upstream multicast hop, as described in RFC 6513. This applies to vrfs configured before BGP is configured.

  Workaround: There is no workaround once it occurs beyond unconfiguring BGP. Configuring a dummy vrf multicast address-family under BGP before the issue occurs can prevent the problem from occurring.

- CSCuf47227

  Symptom: When the configuration option "file verify auto" is enabled and a local copy operation is done for a file that does not contain a signature, e.g. a log file or configuration back, the copy will fail.

  Conditions: file verify auto is enabled in running configuration.

  Workaround: Use copy or noverify or disable file verify auto.

- CSCuf52756

  Symptom: %IOSXE_RP_SPA-4-IFCFG_CMD_TIMEOUT: Interface configuration command

  Conditions: Observed tracebacks and traffic drop during MDR upgrade

  Workaround: There is no workaround.

- CSCuf53543

  Symptom: MPLS-TP L2 VCs are down after SIP reload and RP switchover

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuf56776

  Symptom: After a linecard is removed and reinserted (OIR), traffic may fail to pass through some virtual circuits which have been configured for pseudowire redundancy.

  Conditions: This symptom is observed when the first segment ID in the redundancy group is numerically greater than the second segment.

  ```
  PE1#show ssm id | inc 1st       1stMem: 16394 2ndMem: 12301 ActMem: 12301
  1stMem: 16394 2ndMem: 12301 ActMem: 12301  After the OIR is performed, it can be seen
  that the segments are reversed on the linecard.  ESM-20G-12#sh ssm id | inc 1st
  1stMem: 12301 2ndMem: 16394 ActMem: 12301       1stMem: 12301 2ndMem: 16394 ActMem:
  12301
  ```

  Workaround: There is no workaround.

- CSCuf56842

  Symptom: A reload may occur while using **show oer** and **show pfr** commands via SSH.

  Conditions: This symptom is observed when the **show pfr master application detail** command is used via SSH.

  Workaround: There is no workaround.

- CSCuf74266

  Symptom: ASR-CUBE: Crash observed with DSMP.

  Conditions: Load scenario issue is observed.

  Workaround: There is no workaround.

- CSCuf84655

  Symptom: One-way video is seen while CUBE is trying to negotiate packetization mode=1 for H264 video codec in both the legs and one video endpoint doesn't support packetization mode=1 for H264 video codec.

  Conditions: When there is DO-DO video call from a video endpoint which supports only Packetization Mode=0 for H264 video codec to a video endpoint which supports both packetization modes like 0 & 1.

  Workaround: Make an EO-EO video call from the endpoint which only support packetization mode=0,so that CUBE will negotiate packetization mode=0 for both the legs and two-way video will be seen.

- CSCuf86171

  Symptom: The DHCP snooping database agent can appear to get stuck when using FTP as the transfer protocol. In the output of 'show ip dhcp snooping database' the following is observed:

  ```
  Agent URL : <FTP URL> Write delay Timer : 300 seconds Abort Timer : 300 seconds  Agent
  Running : Yes Delay Timer Expiry : 0 (00:00:00)   <<<<< Delay timer is at zero, but
  process will never re-start Abort Timer Expiry : Not Running  Last Succeeded Time :
  02:09:53 PDT Thu Jun 6 2013 <<<<< Time will never update Last Failed Time : None Last
  Failed Reason : No failure recorded.  Total Attempts       :       12   Startup
  Failures :        0 Successful Transfers :       11   Failed Transfers :        0
  Successful Reads    :       1   Failed Reads    :       0 Successful Writes    :
  10   Failed Writes    :        0 Media Failures       :        0
  ```

Conditions: This was seen only when using FTP as the protocol to transfer the DHCP snooping binding database to an external server.

Workaround: Use another file transport mechanism like SCP or TFTP as a workaround to this issue. Once the issue is hit, the only known workaround is to reload affected device.

- CSCug08561

  Symptom: After a web-logon, users do not get the web-logon response page sent by the portal. If the web-logon is successful, users are not redirected to the web address which they have entered initially but are redirected to the portal for authentication.

  Conditions: This symptom occurs under the following conditions:

  1. Walkby feature is enabled with L4R & PBHK features applied to the lite session.

  2. User initiated the web-logon request.

  Workaround: There is no workaround.

- CSCug19697

  Symptom: "playout-delay fax" command does not change T.38 and modem Passthrough playout buffer to accommodate packet jitter.

  Conditions: This symptom occurs when the ability to reduce the default Fax playout is delayed.

  Workaround: There is no workaround.

- CSCug28860

  Symptom: Missing dial tone when pressing new call with existing two-way whisper call.

  Conditions: This symptom is observed with whisper intercom only.

  Workaround: There is no workaround, however you are able to make outgoing call without dial tone.

- CSCug29813

  Symptom: A path confirmation failure occurs for Dual Tone Multifrequency (DTMF) tones.

  Conditions: This symptom occurs in an SIP-SIP call flow in IPv4 and IPv6 scenarios.

  Workaround: There is no workaround.

- CSCug31123

  Symptom: PPPoE sessions are getting stuck.

  Conditions: This is a timing issue . Issue is seen with qos accounting and accounting accuracy enabled. This was observed on active under very high load with CoA requests and session disconnect for a session happening almost at the same time. This happens on new active after RP switchover , if the switchover happens when a session was getting established . This does not need a CoA request , but needs Rabapol pushed through per user profile .

  Workaround: There is no workaround.

- CSCug31717

  Symptom: On an ASR involving transcoded calls, hung data plane issue is seen during abnormal disconnect of the calls.

  Conditions: On an ASR involving transcoded calls, hung data plane issue is seen during abnormal disconnect of the calls.

  Workaround: There is no workaround.

- CSCug38621

Symptom: Router crashed at ccsip_spi_incoming_reg_contact_change

Conditions: When configuring "registrar ipv4:9.60.51.254" under "sip-ua"

Workaround: There is no workaround.

- CSCug50150

  Symptom:During MDR in a APS Setup, under certain conditions, IOSXE_APS-3-CCCONFIGFAILED, mesage is seen.

  Conditions:If the MDR of Protect interface is Started first followed by a MDR of the Working, then the above TB will occur.

  Workaround: Ensure that the working Interface is the first which goes through the MDR. IF the interfaces are on the SAME SIP, the traffic must be flowing through the Working interface, to ensure zero traffic drops.

- CSCug50340

  Symptom: PW traffic is not flowing after SSO/card reset the active PTF card.

  Conditions: The symptom is observed with the following conditions:

  1. Create a unprotected tunnel between the active PTF card and create a PW.

  2. Apply the table map. Bi-directional traffic is flowing fine.

  3. SSO/reset the active PTF card in node 106 (4/1).

  4. Now tunnel core port is in standby card.

  5. Observed bi-directional traffic is not flowing once the card becomes up.

  6. Again reset the active PTF card (5/4).

  7. Observe uni-directional traffic only is flowing.

  Workaround: Delete the PW and recreate it again. However, note that if you do an SSO/card reset, the issue reappears.

- CSCug50606

  Symptom: Sometimes, IPCP assigns an different address for clients from wrong address pool.

  Conditions: This symptom is observed under the following conditions: - **peer default ip address** command is configured on dialers. -There are some dialers on the Cisco router. -The issue could happen on Cisco IOS Release 15.2(4)M3.

  Workaround: There is no workaround.

- CSCug53310

  Symptom: ICMP v6 traffic is observed to drop

  Conditions: ICMP v6 traffic is observed to drop with cxsc configured under the zbfw policy-map. Drops are observed the zone is applied on a DMVPN tunnel.

  Workaround: There is no workaround.

- CSCug61559

  Symptom: Matching the last protocol under it's attributes will not work.

  Conditions: Using the default protocol-pack.

  Workaround: Currently there is no workaround.

- CSCug69107

  Symptom: Crypto session does not comes up in EZVPN.

Conditions: This symptom is observed when a Crypto session is being established.

Workaround: There is no workaround.

- CSCug72874

  Symptom: Group Member is registering the third Key Server in its list in a redundant KS scenario, when certificate of first KS has been revoked.

  Conditions: This symptom is observed under the following conditions: - GM has a list of 3 or more Key server - Certificate based authentication with OCSP validation - First KS certificate has been revoked.

  Workaround: There is no workaround.

- CSCug78227

  Symptom:

  ASR1001-5-DEV(config-sbc-sbe-sip-hdr-ele)# sip header-profile hprof2
  ASR1001-5-DEV(config-sbc-sbe-sip-hdr)# store-rule entry 1
  ASR1001-5-DEV(config-sbc-sbe-sip-hdr-ele-act)# condition request-uri sip-uri-user store-as uname Error: sip-uri-user is only valid for To, From and Request-Line

  Conditions: This symptom occurs when the following config is pasted into config terminal or on reading startup-config with following config

  ```
  ------------------------------------------------------------------------------------
  --------    sip header-profile hprof1     store-rule entry 1      condition
  header-name Allow header-value store-as Avalue     store-rule entry 2      condition
  request-uri sip-uri-user store-as uname
  ```

  Workaround: exit sbc, re-enter the specified store-rule/condition

  ```
  ------------------------------------------------------------------------------------
  --------    sip header-profile hprof1     store-rule entry 1      condition
  header-name Allow header-value store-as Avalue      exit     exit    exit   exit  sbc
  test   sbe    sip header-profile hprof1     store-rule entry 2      condition
  request-uri sip-uri-user store-as uname
  ```

- CSCug81812

  Asymmetric Payload Inter-working was introduced in XE310. Hence adding HA support for asymmetric payload inter-working here to provide complete solution as requested by some customers.

- CSCug82939

  Symptom: ICMP error packets having icmp message in the payload are being dropped when NAT64 and ZBFW are configured.

  Conditions: The configuration should include nat64 and zbfw.

  Workaround: There is no workaround.

- CSCug85947

  Symptom: OSPFv3 routes go missing after an NSR switchover.

  Conditions: This symptom occurs after an SSO.

  Workaround: Clear the IPv6 OSPF process.

- CSCug97383

  Symptom: Switch crashes with EOAM and IP SLA Ethernet-monitor configurations

Conditions: Occurs infrequently when EOAM configuration include VLANs. Does not occur if all EOAM configurations are configured with only Ethernet Virtual Circuits (EVC)

Workaround: There is no workaround.

- CSCug97910

  Symptom: High CPP_CP process CPU load on ESP100 caused by session counter collection.

  Conditions: ESP100 and ISG scale

  Workaround: Reduce number of counters associated with ISG session

- CSCug98810

  Symptom: show plat soft iomd [slot/subslot] connecti statistics will, under some circumstances, on the first execution will display random counters.

  Conditions: The first execution of the show plat soft iomd [slot/subslot] conn statistics.

  Workaround: Execute a clear plat soft iomd [slot/subslot] connect statistics command.

- CSCug99771

  Symptom: OSPF N2 default route missing from Spoke upon reloading Hub. Hub has a static default route configured & is sending that route over DMVPN tunnel running OSPF to spoke. When hub is reloaded, the default route is missing on Spoke. NSSA-External LSA is there on Spoke after reload, but the routing bit is not set. Hence, it is not installed in RIB on Spoke.

  Conditions: Default originated using command "area X nssa default-information-originate"

  Workaround: Removing & re adding "area X nssa default-information-originate" on Hub resolves the issue.

- CSCuh06821

  Symptom: Traffic drop after the sso

  Conditions: with RSP10g

  Workaround: There is no workaround.

- CSCuh07535

  Symptom: crypto context show command display unknown authentication and confidentiality output

  Conditions: sha256, sha384, sha512, gmac and gcm

  Workaround: There is no workaround.

- CSCuh14012

  Symptom: The crypto session remains UP-ACTIVE after tunnels are brought down administratively.

  Conditions: This symptom occurs in tunnels with the same IPsec profile with a shared keyword.

  Workaround: There is no workaround.

- CSCuh22742

  Symptom: Callflow: Verizon ? SIP trunk ? CUBE (ASR 1000)? CUSP ? Genesys ? Interactions IVR. CUBE does not ACK and BYE (glare handling case) after sending Cancel and receiving 200 Ok for cancel from CUSP.

  Conditions: Verizon cancelled the call 300 milliseconds (aprox) after sending the invite, it caused the 200Ok of the invite and the Cancel to cross wire between CUSP and Genesy. By that time CUSP had already sent 200 Ok for CANCEL to CUBE, thus CUBE did not respond to the following 200 OK (for Invite).

Workaround: There is no workaround.

- CSCuh24040

  Symptom: BGP routes are not marked Stale and considered best routes even though the BGP session with the peer is torn down. A hard or soft reset of the BGP peering session does not help. For BFD-related triggering, the following messages are normally produced with the BGP-5-ADJCHANGE message first, and the BGP_SESSION-5-ADJCHANGE message second. Under normal conditions, the two messages will have identical timestamps. When this problem is seen, the order of the messages will be reversed, with the BGP_SESSION-5-ADJCHANGE message appearing first, and with a slightly different timestamp from the BGP-5-ADJCHANGE message. In the problem case, the BGP_SESSION-5-ADJCHANGE message will also include the string "NSF peer closed the session" For example when encountering this bug, you would see:

  ```
  May 29 18:16:24.414: %BGP_SESSION-5-ADJCHANGE: neighbor x.x.x.x IPv4 Unicast vpn vrf
  VRFNAME topology base removed from session  NSF peer closed the session  May 29
  18:16:24.526: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME Down BFD adjacency
  down    Instead of:  May 29 18:16:24.354: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf
  VRFNAME Down BFD adjacency down  May 29 18:16:24.354: %BGP_SESSION-5-ADJCHANGE:
  neighbor x.x.x.x IPv4 Unicast vpn vrf VRFNAME topology base removed from session  BFD
  adjacency down
  ```

  Log messages associated for non-BFD triggers are not documented.

  Conditions: This symptom is observed when BGP graceful restart is used in conjunction with BFD, but it is possible (but very low probability) for it to happen when BGP graceful restart processing happens when any other type of BGP reset (eg: clear command) is in progress. Affected configurations all include: router bgp ASN ... bgp graceful-restart ... The trigger is that BGP exceeds its CPU quantum during the processing of a reset, and gives up the CPU, and then BGP Graceful Restart processing runs before BGP can complete its reset processing. This is a very low probability event, and triggering it is going to be highly dependent on the configuration of the router, and on BGP's CPU requirements. It is not possible to trigger this bug unless BGP graceful-restart is configured.

  Workaround: If you are engaged in active monitoring of router logs, and the bug is being triggered by a BFD-induced reset, you can detect this situation by watching for the reversal of log message order described in the Symptoms section, and then take manual steps to remedy this problem when it occurs. On the problematic router, issue **no neighbor <xxx> activate** command under the proper address-family will clear the stale routes. The other option is to manually shutdown the outgoing interface which marks the routes as "inaccessible" and hence not been used anymore. This prevents the traffic blackhole but the routes will stay in the BGP table.

- CSCuh27343

  Symptom: A CUBE router may reload

  Conditions: This is only seen on a router processing voice traffic

  Workaround: There is no workaround.

- CSCuh28721

  Symptom: icmp packet size 1439-1454 will be drop at next hop because the L2 frame size is bigger than 1518 , 1500 MTU acceptable frame size.

  Conditions: crypto map with NAT in between tunnel end point

  Workaround: There is no workaround.

- CSCuh31480

  Symptom: traceback observed when Interface Virtual-Access3(for ezVPN server) changed state to down on MCP_DEV(XE311)

Conditions: Interface Virtual-Access3(for ezVPN server) changed state to down.

Workaround: There is no workaround.

- CSCuh32177

  Symptom: The **no passive-interface <if-name>** command will be added automatically after configuring the "**ipv6 enable**" command on the interface even though the "passive-interface default" command is configured for OSPFv3. --- (config)#interface FastEthernet0/2/0 (config-if)#ipv6 enable (config-if)#end #sh run | sec ipv6 router ospf ipv6 router ospf 100 router-id 10.1.1.1 passive-interface default no passive-interface FastEthernet0/2/0 <<< Added automatically. ---

  Conditions: This symptom occurs when the "passive-interface default" command is configured for OSPFv3.

  Workaround: Adjust the configuration manually. In this example it would be "passive-interface FastEthernet0/2/0".

- CSCuh32439

  Symptom: traceroute to MIP mac address is failing

  Conditions: Portchannel traceroute to MIP mac address of egress interface failing

  Workaround: There is no workaround.

- CSCuh37664

  Symptom: Prefixes/TCs stay INPOLICY although some configured resolvers are above threshold

  Conditions: Policy uses non-default resolvers

  Workaround: Only a reload of the MC solves this issue.

- CSCuh38425

  Symptom: ASR1K fails to initialize with cpp_driver held down message

  Conditions: ESP-100, ESP-200 or ASR1002-VE configured with 40MB or 80MB TCAM devices manufactured by Renesas may fail to initialize.

  Workaround: There is no workaround.

- CSCuh40275

  Symptom: SNMP occupies more than 90% of the CPU.

  Conditions: This symptom is observed when polling the cefFESelectionTable MIB.

  Workaround: Execute the following commands: snmp-server view cutdown iso included snmp-server view cutdown cefFESelectionEntry excluded snmp-server community public view cutdown ro snmp-server community private view cutdown rw

- CSCuh41597

  Symptom: Memory leak is seen when SDP passthru is configured.

  Conditions: When SDP passthru is configured.

  Workaround: There is no workaround.

- CSCuh43027

  Symptom: Prefixes withdrawn from BGP are not removed from the RIB, although they are removed from the BGP table.

  Conditions: A withdraw message contains more than one NLRI, one of which is for a route that is not chosen as best. If deterministic med is enabled, then the other NLRI in the withdraw message might not eventually be removed from the RIB.

Workaround: Forcibly clear the RIB.

- CSCuh43255

  Symptom: The BGP task update-generation process may cause the router to reload, in a rare timing condition when there is prefix flap and there is high scale of prefixes going through update-generation, including the flapping prefix.

  Conditions: The symptom is observed when the Cisco ASR router is acting as a route server for BGP along with having various route-server contexts. The router does not do any forwarding. It merely processes control plane traffic.

  Workaround: There is no workaround.

- CSCuh44420

  Symptom: When an IOS router with one or more mpls ldp neighbors undergoes an mpls ldp router-id configuration change when non-stop routing had been previously enabled and then disabled prior to the router-id configuration change, sessions will fail to become NSR ready once mpls ldp nsr is reconfigured.

  Conditions: This issue occurs when the mpls ldp router-id is reconfigured after mpls ldp nsr has been enabled and then disabled. After the router-id change, mpls ldp nsr must be reconfigured in order to encounter this issue.

  Workaround: Reload the standby RP.

- CSCuh44476

  Symptom: Some neighbors are not discovered and the VCs don't come up

  Conditions: SSO on box having VFIs with autodiscovery BGP and BGP signalling, with more than 2 remote PEs.

  Workaround: There is no workaround.

- CSCuh46006

  Symptom: Basically, the fix is originally committed in XE3.7 release. The requirement is that when VC type is 4 for both VPLS and VPWS, ASR1k needs push a dummy tag in outgoing packets before forwarding them to core network and pop a dummy tag in incoming packets coming from core network. Such fix also needs be committed to XE3.10 release.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuh46849

  Symptom: A Cisco ASR 1000 router may display the following log with a traceback: SCHED-3-UNEXPECTEDEVENT Process received unknown event (maj 80, min 0).

  Conditions: There is no known condition.

  Workaround: Reload the router.

- CSCuh49807

  Symptom: IPsec transform set with esp-md5-hmac is not supported in this release. When esp-md5-hmac is used, though the IPsec tunnel is established, traffic can not pass through the tunnel. Inbound traffic will be dropped with HMAC error. Outbound traffic will reach to the peer, but will be dropped by the peer with HMAC error.

  ```
  Error message : %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:000
  TS:00000002356612773534 %IPSEC-3-HMAC_ERROR: IPSec SA receives HMAC error, DP Handle
  5, src_addr 60.0.0.2, dest_addr 60.0.0.1, SPI 0xb98e9ee1
  ```

Conditions: Whenever esp-md5-hmac is used in an IPsec transform set.

Workaround: Use esp-sha-hmac, not use esp-md5-hmac.

- CSCuh53544

  Symptom: OSPF ABR router does not flush type-4 ASBR summary LSA after NSR swithover if the connection to ASBR is lost during NSR switchover.

  Conditions: This symptom is occurs when the VSS system acts as ABR and loses connection to an ASBR during NSR switchover. This configuration is not recommended and Layer 3 topology should not change during the switchover.

  Workaround: Clear ip ospf proc.

- CSCuh56327

  Symptom: IP SLA responder crash occurs on Cisco ASR 1002 router in Cisco IOS Release 15.2(4)S, Cisco IOS Release 15.2(4)S1, and Cisco IOS Release 15.2(4)S2.

  Conditions:This symptom occurs when ip sla udp jitter with precision microseconds, udp jitter with milliseconds and udp echo are configured on the sender device with the same destination port on Cisco ASR 1002 router.

  Workaround:Use different destination ports for udp-echo and udp jitter with millisecond precision than udp jitter with microsecond and optimize timestamp.

- CSCuh56534

  Symptom: bad ipcksum when tcp segment from inside

  Conditions: Send tcp segments from inside (sip ALG)

  Workaround: There is no workaround.

- CSCuh57439

  Symptom: The router crashes from some heap memory exception, such as "FREEFREE" or "BADMAGIC" within the checkheaps process.

  Conditions: The router has experienced heavy, likely prolonged voice traffic, especially CUBE (IP-IP gateway) calls.

  Workaround: There is no workaround.

- CSCuh62266

  Symptom: During normal operation, the Cisco ASR 1000 router may crash after repeated SNMP related watchdog errors.

  ```
  Jun 15 2013 10:43:30.325: %SCHED-0-WATCHDOG: Scheduler running for a long time, more
  than the maximum configured (120) secs. -Traceback= 1#6d024ee43b83b4f5539a076aa2e8d467
  :10000000 56A5348 :10000000 20F7D54 :10000000 2513910 :10000000 20F807C :10000000
  20EBE84 :10000000 2119BA8 :10000000 20EBE84 :10000000 2106C24 :10000000 20EBE84
  :10000000 213C9E8 :10000000 213CC34 :10000000 225B748 :10000000 222941C :10000000
  2214314 :10000000 224812C  -Traceback= 1#6d024ee43b83b4f5539a076aa2e8d467  :10000000
  21416F0 :10000000 2513910 :10000000 20F807C :10000000 20EBE84 :10000000 2119BA8
  :10000000 20EBE84 :10000000 2106C24 :10000000 20EBE84 :10000000 213C9E8 :10000000
  213CC34 :10000000 225B748 :10000000 222941C :10000000 2214314 :10000000 224812C
  ```

  Conditions: This symptom occurs while trying to obtain data from IP SLAs Path-Echo (rttMonStatsCollectTable) by SNMP polling operation.

  Workaround: There is no workaround other than to disable SNMP configuration from the router.

- CSCuh62529

  Symptom: ASR router crashes for media forking HA feature

Conditions: media forking feature crashed in B2BHA standby router

Workaround: There is no workaround.

- CSCuh62579

  Symptom: CUBE send 403 response for untrusted Requests by default. This request to make the TDOS feature enabled by default came from marketing for Ease-of-use to the customer.

  Conditions: Request should come from untrusted host.

  Workaround: enable silent-discard explicitly.

- CSCuh63727

  Symptom: Router may crash when unconfiguring large (8k) redirect ACL list in MASK config

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuh63837

  Symptoms: When ASR1k receives Account Logon from web portal and coverts lite sessions to dedicated sessions, ASR1k may show inconsistent session counters between PI and PD shim layer. Without this debuggability enhancement, we are not able to tell whether the problem resides on PI sie or PD side.

  Conditions: This condition is observed when converting lite sessions to dedicated sessions.

  Workaround: There is no workaround.

- CSCuh65933

  Symptom: When ingress-PE switch the encapsulation of multicast traffic from default MDT to data MDT, the first packets after switchover will be added two labels (including both default and data MDT labels).

  Conditions: When the traffic rate exceeds the threshold, the ingress-PE will switch to data MDT(encapsulate multicast packets into data MDT, instead of default MDT).

  Workaround: There is no workaround.

- CSCuh66373

  Symptom: KS not sending rekey to the registered GM

  Conditions: KS not sending rekey to the registered GM

  Workaround: If we enable retransmission on KS , rekey are received by the GMs.

- CSCuh66510

  Symptom: The router crashes during the display of history traces during execution of command 'show monitor event-trace voip ccsip history all'

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuh67288

  Symptom: Packets carrying IP Options and being encrypted end in a corrupted packet.

  Conditions: An IPv4 packet carrying IP options traversing a GETVPN GM with TBAR enabled. After encryption, the outer IP header is corrupted. This issue doesn't manifest itself if no IP Options are present on the original IP packet

  Workaround: There is no workaround.

- CSCuh68693

  Symptom: RP crashes [active RP, in the case of a dual RP setup] when the **show otv isis database standard detail** command is used to check details related to MAC addresses.

  Conditions: This symptom occurs in valid OTV configurations (OTV state is UP and AED State is Yes).

  Workaround: There is no workaround.

- CSCuh68741

  Symptom: Overlord crashing @ cvmx_clock_get_count on latest throttle image

  Conditions: Overlord with KWAAS installed and with specific configuration combination

  Workaround: There is no workaround.

- CSCuh70269

  Symptom: packet is dropped with reason of NatIn2out

  Conditions: PAT configuration

  Workaround: There is no workaround.

- CSCuh72756

  Symptom: When loading protocol-pack 6.0 or 6.1 a traceback might occur. There is no functionality impact.

  Conditions: When loading protocol-pack 6.0 or 6.1 on top of version 15.3(3)S with RP1 platform.

  Workaround: Currently there is no workaround.

- CSCuh72818

  Symptom: When inserting a SPA-4XT-SERIAL or after booting of a chassis containing SPA-4XT-SERIAL, the following messages are displayed:

  ```
  *Jun 18 17:18:31.741 EDT: %IOSXE-4-PLATFORM: R0/0: kernel: ERROR: No thresholds
  defined for slot 1, BW 150 (mbps) *Jun 18 17:18:31.741 EDT: %IOSXE-4-PLATFORM: R0/0:
  kernel: ERROR: SPA 1: get buf 56 thresholds failed
  ```

  These are only messages and have no affect on SPA functionality

  Conditions: Occurs during reload/bootup of chassiswhich contains the SPA-4XT-SERIAL or during insertion of this SPA.

  Workaround: There is no workaround.

- CSCuh73986

  Symptom: Dns response get dropped with no-payload configured and NAT FW

  Conditions: configure nat FW(dns inspect) send dns query from inside, server then reply the response

  Workaround: There is no workaround.

- CSCuh74735

  Symptom: intra mag roaming via dhcp request.

  Conditions: intra mag roaming via dhcp request.

  Workaround: There is no workaround.

- CSCuh74822

  Symptom: config / un config cause MAG config fail with MCSA

Conditions: There is no known condition.

Workaround: There is no workaround.

- CSCuh75315

  Symptom: RP crash occurs while removing nat configs

  Conditions: This condition is observed when you unconfigure 4k nat sessions from UUT

  Workaround: There is no workaround.

- CSCuh75393

  Symptom: When subject name is used as secondary under trustpoint for authorization without primary configured, it doesn't pick the correct value. Conditions: only subject name is configured as secondary without primary. Workaround: configure subject name as primary

- CSCuh76529

  Symptom: There is no known symptom.

  Conditions: Astro can require a core voltage of up to 1.00V. However, the voltage was defaulted to 0.9V for all Astro chips. If an Astro requires 1.0V is on a board, it is only operating at 0.9V and could fail to operate properly at speed.

  Workaround: There is no workaround.

- CSCuh76617

  Symptom: With MVPN BGP C-route signalling, some multicast states in the VRF might be left even when C-route state is withdrawn from BGP.

  Conditions: This typically happens when all the BGP sessions on the PE go down (for e.g. manual clearing of BGP via "clear ip bgp")

  Workaround:There is no known workaround.

- CSCuh78003

  Symptom:Complete traffic loss

  Conditions: This condition is observed when you clear Xconnect all, on the box where pseudowire redundancy is configured and no other network event before this trigger

  Workaround: Remove and reconfigure Xconnect service

- CSCuh80368

  Symptom: erspan performance downgrade in FP160

  Conditions: erspan under FP160

  Workaround: There is no known workaround.

- CSCuh80492

  Symptom: The system crashes, and it causes a reload. Messages that can be seen on the console indicate there is a "NULL pointer dereference" for example, BUG: unable to handle kernel NULL pointer dereference This is followed by a stack trace.

  Conditions: This crash is unlikely to happen in normal situations. The user would need to have shell access, and then access a task file under /proc (for example, /proc/29208/ns/ipc) which gives stats on the IPC namespace. The crash is cause due to the lack of proper locking semantics on the variables controlling the IPC namespace.

  Workaround: There is no workaround.

- CSCuh82492

Symptom: NBAR doesn't activate

Conditions: with NAT under SIP, DNS traffic

Workaround: disable alg

- CSCuh83891

  Symptom: getting crashinfoo while running NATFW scipt with mcp_dev image

  Conditions: Getting crashinfo

  Workaround: Tried with other mcp_dev image but getting same crashinfo.

- CSCuh86464

  Symptom: Observe SSS msg chunk memory leak

  Conditions: clear subscriber session all while scale sessions are coming up

  Workaround: There is no workaround.

- CSCuh87017

  Symptom: Hw-Sw: ASR1004 ASR1000-RP2 ASR1000-ESP20 asr1000rp2-adventerprisek9.03.09.01.S.153-2.S1 The ESP goes down logging messages similar to what is shown below:

  ```
  Jun 27 19:59:12.308: %CPPHA-3-FAULT: F0: cpp_ha:  CPP:0.0 desc:CPP Client process
  failed: cpp_cp det:HA class:CLIENT_SW sev:FATAL id:1 cppstate:RUNNING res:UNKNOWN
  flags:0x0 cdmflags:0x0  Jun 27 19:59:12.393: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_ha:
  cpp_ha encountered an error    -Traceback= 1#e1875e79d5b29fc4e498ecbc61cdf452
  errmsg:F6DB000 2230 cpp_common_os:FF5A000 C330 cpp_common_os:FF5A000 C130 :10000000
  6FA4 :10000000 12718 evlib:F435000 E3B8 evlib:F435000 10564 cpp_common_os:FF5A000
  12FF8 :10000000 F108 c:E51F000 1E938 c:E51F000 1EAE0  Jun 27 19:59:13.054:
  %PMAN-3-PROCHOLDDOWN: F0: pman.sh:  The process cpp_cp_svr has been helddown (rc 134)
  Jun 27 19:59:14.289: %PMAN-0-PROCFAILCRIT: F0: pvp.sh:  A critical process cpp_cp_svr
  has failed (rc 134)  Jun 27 19:59:18.422: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_ha:
  cpp_ha encountered an error -Traceback= 1#e1875e79d5b29fc4e498ecbc61cdf452
  errmsg:F6DB000 2230 cpp_common_os:FF5A000 C330 cpp_common_os:FF5A000 C130 :10000000
  6FA4 :10000000 12718 evlib:F435000 E3B8 evlib:F435000 10564 cpp_common_os:FF5A000
  12FF8 :10000000 F108 c:E51F000 1E938 c:E51F000 1EAE0
  ```

  Conditions: On issuing "sh ip nat trans" when there are a large number of static networks and static NAT mappings

  Workaround: Use AAA/Authorization functionality to restrict show ip nat translations OR clear ip nat translation from being issued

- CSCuh87618

  Symptom: Configured two APS groups (one for OC3/hdlc and other with OC12/PPP) between ASR1013 and ASR1006 using back to back connections. APS group 1 interfaces Inactive after RP-switchover

  Conditions: During ASR1013 Subpackage MDR

  Workaround: There is no workaround.

- CSCuh87919

  Symptom: Seeing PuntPerCausePolicerDrops on sending traffic through LISP router.

  Conditions: No traffic drops associated

  Workaround: There is no workaround.

- CSCuh88723

Symptom: Plim Ingress classification doesn't work on Clearchannel-SPAs. High priority traffic will continue to be treated as normal traffic and flows in Low Priority queue.

Conditions: With PLIM ingress classification, despite assigning "map ip dscp 16 - 31 queue strict-priority" traffic flows in Low Priority queue.

Workaround: There is no workaround.

- CSCuh90094

  Symptom: %MEDIATRACE-3-R_SNMP_COMM_STR_MISSING message is seen, suggesting to add 'snmp-server community public ro' command, but this command is already present on config.

  Conditions: There is some access-limit mechanism in place on the SNMP config, such as 'snmp mib community-map' command

  Workaround: Make sure the first community to appear in the config has no access-limit mechanism, or it has one that allows the router to query itself using SNMP.

- CSCuh90658

  Symptom: QFP crash

  Conditions:

  – create normal GTPv1 session and primary PDP
  – delete request with teardown false
  – update QOS with diff data TEID at both SGSN/GGSN, crash happened

  Workaround: There is no workaround.

- CSCuh91025

  Symptom: Unable to authenticate to Root CA if already authenticated with Sub CA of the Root CA

  Conditions: When authentication with SubCA is already successful, authentication with Root CA fails

  Workaround: Authenticate Root CA first and then SubCA.

- CSCuh91266

  Symptom: VTCP is not robust enough when received tcp segments with abnormal sequence id. This may result FP crash. We observed a TCP packet much older than the current window on customer network.

  Conditions: abnormal sequenced tcp segments received when vtcp buffering current flow

  Workaround: There is no workaround.

- CSCuh91563

  Symptom: ucode crash seen on unconifugring nat with nbar

  Conditions: Seen during a script run

  Workaround: There is no workaround.

- CSCuh92051

  Symptom: peruser v4ACL HA replication broken in mcpdev

  Conditions: When IPv4 and IPv6 profile for single user applied then v4 profile per user data not synced to standby.

  Workaround: There is no workaround.

- CSCuh93142

Symptom: "show hw-module subslot <> sensor" may show the rail-0 as "Margined"

Conditions: The output may show up on normal boot up of the BUILT-IN SPA of Ethernet Line Card.

Workaround: There is no workaround.

- CSCuh93572

  Symptom: Certain sequence of config/unconfig of PLIM commands resulted in error.

  Conditions:

  1. Add DSCP based Plim config.

  2. Mark certain DSCP value as high or low priority with PLIM config command.

  3. Delete the config added in step 1.

  4. Now try to add a TOS bases Plim config. It will through error stating "config done in step 2" must be deleted. But config in step 2 is a subset of config in step1. It should be enough if the config in step1 is removed to add any new plim config.

  Workaround: Remove the DSCP based config completely before adding any new TOS based config.

- CSCuh93698

  Symptom: The Calling-Station-Id is not sent in the accounting-request.

  Conditions: Easy VPN server or Flex VPN remote access is configured along with the **radius-server attribute 31 remote-id** command.

  Workaround: There is no workaround.

- CSCuh94035

  Symptom: A watchdog timeout crash is seen:

  ```
   Jul 14 10:52:08 CDT: %SYS-3-CPUHOG: Task is running for (126000)msecs, more than
  (2000)msecs (1058/14),process = EIGRP-IPv4. -Traceback= 0x62295A0z 0x5A4B9A8z
  0x5A46B10z 0x5A46D70z 0x59EDF2Cz 0x59EFE18z 0x59F0460z 0x59F0D80z 0x59F1094z
  0x59F3FD8z 0x59F4A9Cz 0x5A33D00z 0x5A3419Cz 0x5A071F0z 0x5A080B8z 0x5A43F24z  Jul 14
  10:52:10 CDT: %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  (1071/14),process = EIGRP-IPv4. -Traceback= 0x6CE1A74z 0x6CE106Cz 0x59F5C84z
  0x59EE020z 0x59EFE18z 0x59F0460z 0x59F0D80z 0x59F1094z 0x59F3FD8z 0x59F4A9Cz
  0x5A33D00z 0x5A3419Cz 0x5A071F0z 0x5A080B8z 0x5A43F24z 0x4DD9850z  Jul 14 10:52:10
  CDT: %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = EIGRP-IPv4.
  -Traceback= 0x5A4253Cz 0x5A4A054z 0x622077Cz 0x622482Cz 0x6229720z 0x5A4B9A8z
  0x5A46B10z 0x5A46D70z 0x59EDF2Cz 0x59EFE18z 0x59F0460z 0x59F0D80z 0x59F1094z
  0x59F3FD8z 0x59F4A9Cz 0x5A33D00z   %Software-forced reload
  ```

  Conditions: This issue has been seen with DMVPN and IPV4 / IPV6 EIGRP configured. A crash occurs while DUAL is updating the EIGRP Topology table

  Workaround: There is no workaround. Possibly downgrade to 15.2(4)M2 as the issue was seen after upgrading from this version.

- CSCuh94799

  Symptom: When a Port-channel interface with a carrier delay of 0 milliseconds and one or more service instances configured is removed, an unexpected process termination occurs.

  Conditions: The issue will be seen only when there is both carrier delay ms 0 configuration and service instance configuration under a Port channel interface, and that Port-channel interface is removed using for example no interface Port-channel 1.

  Workaround: There are several work around:

  – Remove the service instance(s) from the Port-channel interface before deleting the interface.

  - Remove the carrier delay from the Port-channel before deleting the interface.
  - Configure a non-zero carrier delay instead of a 0 carrier delay.
  - Don't use carrier-delay on port-channel interfaces in conjunction with service instances. Instead use carrier-delay on port-channel member interfaces. The use of "lacp fast-switchover" on the port-channel interface can also help to avoid the need for carrier-delay in cases where redundant LACP member links are in use.

- CSCuh94879

  Symptom: IOS crash after configuring MHBFD template and map

  Conditions: configure: bfd-template multi-hop New-Temp no authentication sha keychain mhop-key-abc bfd map ipv4 4.4.4.4/32 1.1.1.1/32 New-Temp

  Workaround: There is no workaround.

- CSCuh95125

  Symptom: ESP-100 may crash continuously on an ASR1K box with cpp_svr crashes causing the FP to go down

  Conditions: Numerous QoS sessions with a single queue being created on an interface in a per-session basis on a Yoda platform (ASR1002-X/ESP100/ESP200)

  Workaround: There is no workaround.

- CSCuh95503

  Symptom: Observing iosd crash while removing match criteria from class map.

  Conditions: When multiple filters are matched in the same statement and any one of them is deleted the crash is seen.

  Workaround: There is no workaround.

- CSCuh95747

  Symptom: Hash table updated incorrectly when more than one interface assigned with ip address on wae

  Conditions: Apply ip and configs with uut and wae.

  Workaround: Issue not seen when there is only one interface assigned with ip address on wae.

- CSCuh96558

  Symptom: Router crashes when the command "show voip rtp forking" is issued during load.

  Conditions: Media Forking Enabled

  Workaround: "show voip rtp forking" CLI should not be used under load

- CSCuh96846

  Symptom: Peer destination SIP trunk doesn't establish trunk due to option ping failover towards CUBE. This occurs when the peer to CUBE sends CUBE OPTION PINGS with max-forwards set to zero. The response from CUBE is to incorrectly respond back with a 483 message to many hops. Unified Communications Manager does accept that as a valid response but other User Agents might interpret it incorrectly and not consider the peer active unless receiving a 200OK.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuh97122

Symptom: Potential starving of features to use recycle queue resources because AppNav queue is made high priority

Conditions: Large amount of traffic large enough to exhaust the AppNav recycle queues used by mpass infra

Workaround: There is no workaround.

- CSCuh97129

  Symptom: Losing Eigrp Extended comminutes on bgp l3vpn route.

  Conditions: When Remote PE-CE connection is brought down & only backup EIGRP path remains in the bgp table.

  Workaround: clearing the problem route in the vrf will resolve the issue.

- CSCuh98167

  Symptom: Spurious Accesses messages on router

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuh98929

  Symptom: IFNF support a single L3 byte counter for a connection. There are no separate counter for the connection client and server. This fix adds client and server counters

  Conditions: Current supported CLI: flow record test collect counter bytes long end With this fix, two additional counters can be collected: flow record test collect counter bytes long collect connection client counter bytes network long collect connection client counter bytes server long end

  Workaround: There is no workaround.

- CSCui01133

  Symptom: ATM autovc padi timeout

  Conditions: autovc scaling

  Workaround: There is no workaround.

- CSCui01834

  Symptom: FMAN-FP crash may occur while broadband sessions are torn down

  Conditions: When a large number of broadband sessions are being torn down, there is a possibility of a crash in FMAN-FP.

  Workaround: There is no workaround.

- CSCui02551

  Symptom: There are two possible symptoms for this problem, one is related to the "show" CLI and one is related to configuration (functional). 1) QoS Show CLI: Traceback on FP/ESP (in cpp_cp) when executing a "show plat hard qfp act feat qos ..." command. This is a non-functional problem. 2) QoS Configuration Error: Traceback on FP/ESP (in cpp_sp) when configuring QoS features. This is a functional problem.

  Conditions: Specific sequences of events are required to hit this problem. 1) QoS Show CLI (non-functional): Removing class(es) from attached service policies, attaching new targets, then issuing QoS platform show commands. 2) QoS Configuration Error (functional): Removing class(es) from attached service policies, attaching new targets, detaching "old" targets, re-adding same class(es) back to policy-map.

Workaround: Detach service policy from all targets before removing classes from service policy. The non-functional traceback

(1) is benign, no corrective action is needed. If the functional traceback

(2) has occurred, FP/ESP must be rebooted/reloaded to clear the QoS configuration error.

- CSCui06014

  Symptom: Creating 2000 GRE IPSEC tunnels (sample configuration shown below, repeated 2000 times) causes RP crash. interface tunnel10001 bandwidth 1000 ipv6 address 1003:0:0:1::1/64 ipv6 enable tunnel source Loopback10001 tunnel dest 1004:0:1:1::1 tunnel mode gre ipv6 tunnel protection ipsec profile hub10001

  Conditions: This symptom is observed under the following conditions: On ASR1K: Works fine when scaled up to 2500 sessions. At 4000, a crash is observed. The in between numbers are not available.

  Workaround: Bring up the tunnels in staggered manner (booting with the configurations can also cause the issue) by shutting down the interface and the start them in batches.

- CSCui06921

  Symptom: An FP crash and core file is generated.

  Conditions: This condition is observed when the engineering/debug command **sh pla ha qfp act datapath infra chunk basic <addr>** with an invalid address is passed

  Workaround: Do not use this debug command with an invalid address.

- CSCui06930

  Symptom: VC not coming up

  Conditions: VC not coming up with VPLS configs since vlan is down

  Workaround: Perform a shut/no shut of the vlan interface

- CSCui07422

  Symptom: A PLIM driver informational error TXMC - txmcBufferOverflow messages seen on the router.

  Conditions: Seen with the oversubscribed traffic and Shut/noshut on the interface.

  Workaround: There is no workaround.

- CSCui07997

  Symptom: Route over OSPFv2 sham-link shows two next hop.

  Conditions: This symptom is observed when the route entry is ECMP route between the sham-link and another path.

  Workaround: Break ECMP by adjusting the OSPF cost.

- CSCui91804

  Symptom: Certain connections are reset when active router is reloaded in HSRP pair.

  Conditions: This condition is observed when you reload an active router.

  Workaround: Keep the WAN interface down until Appnav Cluster converges and flow updates are completed.

- CSCui10537

  Symptom: When E1 interface have both channel-group and ds0-group, some ds0-group may not come up on the remote side (suppose it's argot), and voice call cannot be made.

Conditions: This happens when both channel groups and ds0-groups are configured on the same Fortitude card.

Workaround: Current work around is to always configure ds0-group first, then configure channel-group or tdm-group.

- CSCui11009

  Symptom: "clear controller wanphy x/x/x" command cannot clear counters of "sh controller wanphy x/x/x". This issue is seen on ASR1006.

  Conditions: When insert the SPA after the router is up.

  Workaround: Reload the router with the SPA. To-Recovery:

  1. Reload the router with the SPA

  2. "hw-module subslot x/x reload" can clear counters temporarily. But this way doesn't resolve this issue.

- CSCui11702

  Symptom: the sending out isis/NHRP control message packet over tunnel from asr1k don't have special TOS value (prec 6)in the tunnel header

  Conditions: ASR1k pre XE3.10 release, day-one issue.

  Workaround: There is no workaround.

- CSCui12023

  Symptom: OIR of Metronome-spa_BITSOUT results in QL-DNU at connected input source (Metronome-spa/Kingpin BITSIN).

  Conditions: OIR of Metronome-spa_BITSOUT

  Workaround: Remove and Re-apply BITSOUT clocking configuration.

- CSCui13781

  Symptom: FP may crash with HTTP and FTP traffic

  Conditions: Configured NAT , NBAR and appnav over gre tunnel and HTTP

  Workaround: There is no workaround.

- CSCui14692

  Symptom: Crash on C819G running 152-4.M1 due to memory corruption at vm_xif_malloc_bounded_stub.

  Conditions: This condition is seen due to recursive function call of fib code, NHRP, IP SLA etc. However, these might not be the only trigger.

  Workaround: There is no workaround.

- CSCui14753

  Symptom: Named IP ACL does not work for Hash assignment

  Conditions: Apply ip and acl configs on UUT

  Workaround: There is no workaround.

- CSCui15035

  Symptom: Path confirmation failure in T.38 Fax call with re-invite

  Conditions: Voice to fax switch over, T38 fax is not working.

  Workaround: There is no workaround.

- CSCui22356

  Symptom: During Sub package ISSU Upgrade is performed on ASR1002-X router after upgrading the standby RP (R0/1) with new RP subpackages, Switchover is forced from the active IOS process to the standby IOS process. During the switchover, new active performs configuration Bulk-Sync with the standby. During this Bulk Sync operation, the configuration related to the Interfaces is not synced to the standby due to Bulk Sync MCL failures. The following error message will be displayed when this error is present. Sample Error Message: <.....> Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check full list of mismatched commands via: show redundancy config-sync failures mcl Config Sync: Starting lines from MCL file: interface Tunnel150 ! <submode> "interface" - tunnel source GigabitEthernet0/0/0.34 <.....> Standby takes more time(~744 seconds) for reaching terminal State.

  Conditions: The symptom is observed after redundancy force-switchover step in ISSU upgrade procedure.

  Workaround: Perform a standby IOS reload. "hw-module subslot R0/0 reload"

- CSCui24927

  Symptom: Data rate for a QoS shaped MLPPPoA/MLPPPoEoA traffic class may exceed the configured QoS shape rate.

  Conditions: This issue will be apparent if a parent or child shaper is defined on the MLPPP bundle interface that is less than the configured PVC data rate.

  Workaround: The user can explicitly tell the shaper to account for the ATM Cell Overhead by appending the "account user-defined 0 atm" configuration option to the shaper configuration. Example: shape rate <rate> account user-defined 0 atm Note that if the session is already active when modifying the QoS policy-map, the session may need to be restarted for the QoS modification to take affect. This issue will be addressed in the upcoming XE3.8, XE3.10, and later releases. This issue will not be addressed in XE3.8 and XE3.9 and will require migration to XE3.10 or later releases to pick up this fix when available.

- CSCui25696

  Symptom: ASR 1002-X experiences a watchdog reset due to a kernel core dump triggered by a possible divide-by-zero condition.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCui26458

  Symptom: Call flow: Verizon -- CUBE -- CUSP -- Genesys/IVR, transferred with SIP Refer back to PSTN hair-pining the call on CUBE. When the call is put on hold to be transferred from IVR to PSTN, the codec negotiation fails, dropping the call with reason code 47 and hanging the UDP port used. All subsequent calls that try to re-use the same UDP port for RTP stream are dropped with reason code 47 and provision RSP failure is logged on show voip fpi stats

  Conditions: Hair-pinned calls that received multiple M-Lines on the SDP received from Verizon on the original SIP Invite.

  Workaround: There is no workaround. Reload of router is required to clear hung UDP ports.

- CSCui26516
- Symptom: Currently, SIP profiles copy variables data is available only in CCB, but not in SCB. Due to this limitation, copy variables doesn't work for the below cases. - out-of-dialog subscribe/notify pass-thru - in-dialog subscribe/notify after call is cleared (CSCug77212)

  Conditions: When sip profiles copy variables data is used along with in-dialog subscribe/notify.

Workaround: There is no workaround.

- CSCui27725

  Symptom: when ASR1000 connect with ISO HDLC equipment, the ATOM PW traffic could not transparent successfully.

  Conditions: in L2VPN ATOM PW configuration, AC on the PE is CISCO HDLC encapsulation, and CE equipment is ISO HDLC.

  Workaround:

  1. CE configure CISCO HDLC.

  2. CE configure as the FR, and PE configure as HDLC.

- CSCui28312

  Symptom: Router crash.

  Conditions: It only happens in rare cases on images supporting HA with IPv6 BSR configured. In this case it was found by quickly configuring and unconfiguring C-RPs. It is not clear whether this can happen in a normal use case.

  Workaround: There is no workaround.

- CSCui29599

  Symptom: erspan performance downgrade in Kingpin

  Conditions: erspan on Kingpin

  Workaround: There is no workaround.

- CSCui32105

  Symptom: In rare occasions the standby RP on a dual RP system may crash after performing a switchover. The crash occurs due to an invalid message being sent from the RP to the RRP. The following tracebacks may be observed:

  ```
  Jul 22 15:12:50.058 UTC: %COMMON_FIB-3-FIB_PATH_LIST_DB: Attempt to add empty path
  list 0/0: 7F0356E75750 -Traceback= 1#f7cffe13a57f1f88eefbd82deeaab4af  :400000 876363
  :400000 2C3B063 :400000 2C3AEA9 :400000 2C3CE05 :400000 2C2E3FF :400000 1728B37
  :400000 1727E94 :400000 1727A77 :400000 1727968 :400000 5E1FF6F :400000 6536C5D
  :400000 5E1A433 :400000 5E1A09F Jul 22 15:12:50.062 UTC: %FRR_OCE-3-GENERAL: try to
  delete unempty frr db_node. -Traceback= 1#f7cffe13a57f1f88eefbd82deeaab4af  :400000
  876363 :400000 2CDF48D :400000 2CDD509 :400000 16CA2BD :400000 16CA21A :400000 171C2EC
  :400000 3EB784A :400000 1729863 :400000 1728B46 :400000 1727E94 :400000 1727A77
  :400000 1727968 :400000 5E1FF6F :400000 6536C5D :400000 5E1A433 :400000 5E1A09F Jul 22
  15:12:50.065 UTC: %FRR_OCE-3-INVALIDPAR: invalid setup state -Traceback=
  1#f7cffe13a57f1f88eefbd82deeaab4af  :400000 876363 :400000 2CDD520 :400000 16CA2BD
  :400000 16CA21A :400000 171C2EC :400000 3EB784A :400000 1729863 :400000 1728B46
  :400000 1727E94 :400000 1727A77 :400000 1727968 :400000 5E1FF6F :400000 6536C5D
  :400000 5E1A433 :400000 5E1A09F
  ```

  Conditions: There exists a very small timing window where the MPLS forwarding infrastructure may send an invalid message to the standby RP. The condition may occur if a large number of L2VPN AToM pseudowires are flapped within a window at the same time as a RP switchover is performed.

  Workaround: There is no workaround.

- CSCui32300

  Symptom: Tracebacks on standby support on reload of LC containing Pb free Patriot SPA Where we see vc number mismatch tracebacks on standby when we do an LC OIR with ct3 spas inserted

- Conditions: Fix of CSCud67270 Traceback @ spa_choc_dsx_create_vcidb should be present and CT3 SPA should be there and its OIR should be done

  Workaround: There is no workaround.

- CSCui37419

  Symptom: ASR1k CPP ucode crash

  Conditions: Very big DNS packet are being processed.

  Workaround: There is no workaround.

- CSCui38316

  Symptom: The ESP crashes when updating a highly scaling configuration with a large number of flow-controllable nodes. The crash could be observed during dynamic reconfiguration such as changing the rates of a scheduling node, e.g. an ATM VC due to changing L2 shaping or QOS via MQC. The crash could also occur due to growing a scheduling node or moving an ATM VC from one class-of-service node to another. There are several other scenarios that could lead to a transformation of a hierarchy in order to lay out the tree correctly to meet the hardware requirements. One such example is applying a flat policy to or removing a child policy from a policy attached to an ATM VC.

  Conditions: While transforming a hierarchy, there are hardware primitives used to execute the update logic safely. One of requirements for this procedure is to move flow-control from the old tree to the new tree in a particular order to prevent packets from getting out of order. The BQS resource manager had a bug that caused the update to deplete internal flow-control IDs.

  Workaround: There is no workaround.

- CSCui39098

  Symptom: With XFP OIR, TX Power is stuck at -40db sometime and the link fails to come up

  Conditions: XFP OIR

  Workaround: Another XFP OIR.

- CSCui39527

  Symptom: Standby RP crashing when VRF transfer is done

  Conditions: EoGRE HA configuration

  Workaround: There is no workaround.

- CSCui40812

  Symptom: Call transfer using refer method on CUBE will fail, if end UA, which involved in transfer, tries to de-activate the media with c=IN IP4 0.0.0.0 and a=recvonly.

  Conditions: When a CUBE is trying to transfer the call using Refer method to a UA, and the UA responds with re-invite to de-activate the media with c=IN IP4 0.0.0.0 and a=recvonly, then CUBE will respond with 491. ========== 007326: Jul 26 19:48:02.028 UTC: //2336/171907168923/SIP/Error/sact_media_event_send_invite_response: Failure in media negotiation -- Sending 491 response

  Workaround: There is no workaround.

- CSCui41298

  Symptom: udp tunnel header udp_len is definitely 0, not correctly fixed

  Conditions: the tunnel intf is changed from un-udp tunnel to udp tunnel mode.

  (1) vxlan case, the nve will auto create a udp tunnel. the tunnel interface also have the processing with tunnel mode updation, so cause the tun_mode is wrong saved in the uidb subblock

(2) pmip udp tunnel case, the tunnel is created with udp mode, not changed from other tunnel mode. so the tunnel mode saved in the uidb subblock is correct. this is the reason why pmip udp case not expose this issue.

Workaround: There is no workaround.

- CSCui42810

  Symptom: Memory will be getting exhausted under load

  Conditions: in SIP-SIP call when offer is with inband to nte and later in answer it is falling back to inband to inband then there is a memory leak

  Workaround: Do not configure the nte in outbound dial-peer where it will be inband.

- CSCui42826

  Symptom: fman_fp crash seen with 1K tunnels and routemaps

  Conditions: while sending traffic with 1K tunnels and routemaps with ipv6 ACL

  Workaround: There is no workaround.

- CSCui43540

  Symptom: A random crash seen with l2vpn

  Conditions: when remote PE is going through ISSU and has vpws and vpls config

  Workaround: There is no workaround.

- CSCui43804

  Symptom: Traceback seen at ace_crypto_free_hw_spi.

  Conditions: Under load using static VTI.

  Workaround: There is no workaround.

- CSCui45213

  Symptom: Unable to configure interface Multilink greater than 65535. Previously able to configure Multilink interfaces in the range of 1 to 2147483647.

  Conditions: Unable to configure interface Multilink greater than 65535.

  Workaround: There is no workaround.

- CSCui46535

  Symptom: When testing IPSec site-to-site static VTI tunnel between two ASR1000 with ESP100 with a stateless traffic test tool, the tool is reporting that some of the test frames are being received out of sequence. The packet reordering is happening in both the encrypt and decrypt direction. It is observed with both fixed frame size and IMIX traffic. The rate of reordered frames increases with increases in the test traffic rates.

  Conditions: ASR1000 with ESP100, IPSec site-to-site static VTI tunnel.

  Workaround: There is no workaround.

- CSCui47602

  Symptom: traces @ IDMGR-3-INVALID_ID when queried for mplsTunnelTable MIB

  Conditions: GETONE SNMP query for non-existing mplsTunnelTable entries

  Workaround: Use GETNEXT queries instead of GETONE

- CSCui47798

  Symptom: packet lost over GRE tunnels

Conditions: ERSPAN configured on the device, ping the gre tunnel address there are packets lost

Workaround: Disable ERSPAN

- CSCui47819

  Symptom: Configure url tool ezpm and run traffic. Following fields have wrong values: connection to server netw delay sum, connection to client netw delay sum, connection client, server netw delay sum, connection application delay sum, connection application delay max, connection client server resp delay sum, connection server packets counter, connection initiator octets, connection client packets counter

  Conditions: When url tool is configured alone.

  Workaround: Enable other ezpm tool additionally.

- CSCui48950

  Symptom: %LINEPROTO-5-UPDOWN: is output after executing 'no shutdown'. The link state is changed from 'admin down' to 'down' by 'no shutdown'. In such case, this message shouldn't be output. The message is output only first time.

  Conditions: ASR1K

  Workaround: There is no workaround.

- CSCui49185

  Symptom: ASR1002x may crash

  Conditions: 100 Hub PE, 900 CE with 100 VRF, 100 multicast source, 210K route mldp over GRE, after long duration test with multicast traffic When we have mldp over GRE, with paths being added and removed, the counters of the number of paths in a cef path list are not updated correctly. When they wrap (256) this may cause a crash. The problem comes when we remove a path we do not decrement the counter properly, so we need to add/remove a path from a path list 256 times to see the problem

  Workaround: Do not modify paths in the way described in the conditions.

- CSCui50964

  VLAN stats are not getting collected by RP

  Symptom: VLAN Stats would not be displayed on RP

  Conditions: When Scaled Vlans are configured and multiple times shut no shut or configure and unconfigure of vlans causes VLAN stats not collected to RP

  Workaround: Reload of the line card.

- CSCui53561

  Symptom: Link interfaces of multilink bundles may not report any packet or byte counts in either direction. This behaviour may be seen in **show interface Virtual-Access <if number>** outputs, and in **show pppoe session packets** outputs.

  Conditions: This behaviour may be seen on ASR1000 routers, on broadband link interfaces. Broadband link interfaces affected may include PPPoE, PPPoEoA, and possibly PPPoA.

  Workaround: It may be possible to get similar stats through the show command **show platform hardware qfp active feature mlppp datapath bundle Virtual-Access <if number>**.

- CSCui55732

  Symptom: ignore-dtr command not present with 4xt-serial spa interfaces on ASR1k

  Conditions: There is no known condition.

Workaround: There is no workaround.

- CSCui57866

  Symptom: "Show plat soft flow fp active exporter name <name>" displays invalid source and destination addresses if using IPv6.

  Conditions: This is simply a display issue. The addresses are displayed in an IPv4 format. This fix checks the address type before displaying the addresses in the correct IPv4 or IPv6 format.

  Workaround: There is no workaround.

- CSCui58184

  Symptom: Configuration of an ISG Keepalive feature in an ISG policy on an IP subsciber session may result in the router generating keepalive requests to the subscriber even if there is some traffic on the subscriber session.

  Conditions: The ISG policy templates feature should be enabled and any ISG feature (other than Forced Flow Routing, Absolute Timeout and Idle Timeout) should be configured on the session level (not under a traffic class) along with the Keepalive feature in the ISG policy.

  Workaround: unconfigure ISG policy templates feature - unconfigure all ISG features (other than Forced Flow Routing, Absolute Timeout and Idle Timeout) on the session level (not under a traffic class) in the policy.

- CSCui58879

  Symptom: FP crashes

  Conditions: on changing tunnel mode to cgn

  Workaround: There is no workaround.

- CSCui59290

  Symptom: If CUBE received a REFER without Refer-To header , CUBE crashed in some platforms and there were trace backs in others.

  Conditions: When REFER without Refer-To header is received.

  Workaround: Refer-To is mandatory header in REFER Request. Hence might not encounter this case.

- CSCui61230

  Symptom: When a new PW is added under vfi context, it does not come UP

  Conditions: Seen for manual PWs (i.e config of the type "member 1.2.3.4 encapsulation mpls" under the vpls context)

  Workaround: "clear l2vpn service vfi name <name of VFI context>", or deleting and reconfiguring the PW fixes the issue.

- CSCui62441

  Symptom: Complete traffic drop for few seconds is seen after few mins of performing SSO switchover.

  Conditions: Issue is seen only after few mins of performing SSO switchover.

  Workaround: There is no workaround.

- CSCui64057

  Symptom: 'no ip address trusted authenticate' is configured, 403 for REGISTER failed to pass-through via cube

  Conditions: There is no known condition.

Workaround: There is no workaround.

- CSCui64796

  Symptom: cpp_cp_svr crash in LNS

  Conditions: while tearing down PPPoX sessions. On ESP=100, ESP-200 or ASR1K 2RU VE systems, if more than 4000 sessions are created on one interface and then all sessions on that interface are torn down, this leads to a cpp_cp_svr crash on the ESP. Workaround: none

- CSCui64953

  ASR1002-x crashed with rtsp alg

  Symptom: ASR1002-x crashed with rtsp alg

  Conditions: pa_remove fail, the memory will be double free in RTSP ALG, then cause ASR crash

  Workaround: There is no workaround.

- CSCui65881

  Symptom: The MLPPP bundle bandwidth is not updated which led to non-priority packet drops when traffic exceeds the current rate. In the case documented in this DDTS, a bundle rate is supposed to be set to 12M but it was instead set to 1.5M.

  ```
  Schedule specifics:     Index 1 (SID:0x0, Name: Virtual-Access339)       Software
  Control Info:         sid: 0x396eb, parent_sid: 0x38022, obj_id: 0x115e,
  parent_obj_id: 0x54         evfc_fc_id: 0xffff, fc_sid: 0x396eb, num_entries (active):
  2, service_fragment: False         num_children: 2, total_children (act/inact): 2,
  presize_hint: 0         debug_name: Virtual-Access339         sw_flags: 0x0883034a,
  sw_state: 0x00000905, port_uidb: 127126         orig_min  : 0                    ,
  min: 1536000               min_qos   : 0              , min_dflt: 1536000
  orig_max  : 0              ,     max: 1536000               max_qos   : 0
  , max_dflt: 1536000                     share     : 1         plevel    : 0, priority:
  65535  It should be set to 12M.  Index 1 (SID:0x0, Name: Virtual-Access45) Software
  Control Info: sid: 0x38026, parent_sid: 0x38023, obj_id: 0x189, parent_obj_id: 0x54
  evfc_fc_id: 0xffff, fc_sid: 0x38026, num_entries (active): 2, service_fragment: False
  num_children: 2, total_children (act/inact): 2, presize_hint: 0 debug_name:
  Virtual-Access45 sw_flags: 0x0883034a, sw_state: 0x00000905, port_uidb: 130692
  orig_min : 0 , min: 12288000  min_qos : 0 , min_dflt: 12288000  orig_max : 0 , max:
  12288000  max_qos : 0 , max_dflt: 12288000
  ```

  Conditions: The Bundle rate was not being updated when QoS events preceded the rate update from MLPPP. If the MLP event is processed before the QoS event then there is correct behavior, however if the QoS event is processed before the MLP rate update event then the MLP event is lost and never gets processed to update the bundle bandwidth. This results in tail drops when the interface becomes congested prematurely.

  Workaround: The workaround is to apply QoS after all member links have been successfully added to the bundle.

- CSCui67308

  Symptom: Router constantly crashing after enabling TE tunnel over BDI interface

  Conditions: when TE tunnel is exiting a BDI interface. This is not a supported design

  Workaround: Use physical interface for TE tunnels.

- CSCui69873

  Symptom: Crash in ospfv3_db_scope_str()

  Conditions: **Enable debug ospfv3 lsdb**

  Workaround: There is no workaround.

- CSCui70820

  Symptom: Some WCCP issues are not easy to reproduce.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCui75072

  Symptom: Traffic counter shows higher than expected value.

  Conditions: ISG policy templating ON and uni-directional TC in service policy

  Workaround: Use bi-directional TC in service policy

- CSCui75391

  Symptom: Sometime there will not be any output for the command "show sbc global sbe sip subscribers filter <prefix>".

  Conditions: Observed on a Cisco ASR1k platform configured as CUBE using the Service Provider (SP) feature set running IOS-XE version 15.3(1)S2.

  Workaround: The command output is not granular enough. For example: If we execute command like this then it works:

  ```
  #v1-z11#show sbc global sbe sip subscribers filter sip:1037@a.b.c.d #SBC Service
  "global" # #There are currently 2060 subscribers registered on this SBC. # #SIP
  subscribers: # #AOR:                    sip:1037@a.b.c.d #Subscriber Location[s]:
  sip:1037@x.x.x.x:5063 -> ENDPOINTS/PUBNET #                        Fast register
  active, fast time remaining 58 sec #Registrar adj:       SIPCORE #Time left:
  163 secs #Subscriber Category[s]: VRF Global IPv4 a.b.x.y  then we see expected
  information about "sip:1037@a.b.c.d" subscriber.  But if we execute:  #v1-z11#show
  sbc global sbe sip subscribers filter sip:1037 #SBC Service "global"
  ```
  we don't see anything. So the workaround is to use the first option.

- CSCui76564

  Symptom: A roaming mobile customer (e.g. iPASS, Boingo etc.) logs on via a Web-Portal-Page and the ISG doesn't send in the radius accounting-request packet the V-Cookie to the Radius Server.

  Conditions: Depends on ISG setup. In this case L & V Cookie must be send in accounting-request from ISG to AAA Server.

  Workaround: There is no workaround.

- CSCui77763

  Symptom: **show platform software memory qfp-control-process qfp active** is not working.

  Conditions: Execution of the show command.

  Workaround: There is no workaround.

- CSCui80058

  Symptom: On the ASR1000 platform, if ip tcp adjust-mss is configured on an interface with a crypto map, then the TCP MSS value is not adjusted for egress TCP flows that are encrypted.

  Conditions: This is only a problem when there is a crypto map configured on the same interface ip tcp adjust-mss is enabled.

  Workaround: Configure ip tcp adjust-mss on the ingress LAN interface when crypto map is configured on the egress interface.

- CSCui80961

Symptom: The output shows that the QM CPP DRAM increases but does not decrease when fair-queue is removed from a class before it is active in HW. show plat hard qfp act inf exmem stat user | incl QM Over time the system runs out DRAM causing subsequent configuration events that require CPP DRAM objects to fail.

Conditions: When fair-queue is removed from a class before it is activated in the hardware, the BQS RM was not freeing the WRED DRAM object used to store the fair-queue configuration. Over time, the system runs out of CPP DRAM. The error message described in the description is displayed and all configurations start failing. This conditions impacts the whole system as opposed to just queueing features.

Workaround: There is no workaround.

- CSCui81155

  Symptom: Packet trace showing incorrect ICMP type for ping terminated on router.

  Conditions: When using packet trace with IOS-XE and ICMP traffic is traced.

  Workaround: There is no workaround.

- CSCui82757

  Symptom: Session query responses in Lite sessions have inconsistent calling-station-ID behavior

  Conditions:

  1. Walkby feature is enabled with L4R & PBHK features applied to lite session.

  2. Session query to ISG.

  Workaround: Do not depend on Calling-Station ID.

- CSCui85019

  Symptom: When the command **show xconnect** is entered, it may result in a memory leak. This can be observed by entering the command **show memory debug leaks chunks** and seeing entries like this:

```
router#show memory debug leaks chunks Adding blocks for GD...                I/O
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  AA3F8B4     2348  6D0B528  97   Exec
PW/UDP VC event trace
```

  Conditions: This symptom is observed when one or more xconnects are configured with UDP encapsulation.

  Workaround: There is no workaround.

- CSCui85434

  Symptom: Transfer is failing with midcall invite.

  Conditions: CUBE not able to send out DO invite on to other leg in RE INVITE based transfer.

  Workaround: Issue fixed.

- CSCui86239

  Symptom: 6pe performance drop in xe310 release

  Conditions: observed on small packet(82 bytes)

  Workaround: packet size large than 82

- CSCui87915

  Symptom: VC is not going after the access interface is down

Conditions: Scalable eompls under port-channel and shut the member link

Workaround: There is no workaround.

- CSCui88210

  Symptom:QinQ inner vlan configuration on Native Asr1k Ethernet Linecard traffic would not pass

  Conditions:QinQ Sub interface configuration with inner vlan as ANY, Native Asr1k Ethernet Linecard traffic to that sub interface will be dropped in the linecard.

  Workaround: There is no workaround.

- CSCui88245

  Symptom: The CPP process could while adding fair-queue on the fly. This does not require scaling to occur.

  Conditions: When fair-queue is added on the fly while a default parent schedule is being deleted, a crash could occur because the RM cleanup code is destroying a wrong tree.

  Workaround: There is no workaround.

- CSCui89069

  Symptom: ISIS Flap on performing SSO

  Conditions: with "nsf ietf" configured and one or more loopbacks configured as passive interfaces

  Workaround: Two workarounds are available:

  1)use "nsf cisco"

  2) Continue to use "nsf ietf" but configure "ip router isis <process_name> " on the loopback interfaces.

- CSCui91255

  Symptom: After configuring static nat ping fails and ip nat translation is not shown in show ip nat translations

  Conditions: Core file generated after configuring static nat configuration

  Workaround: There is no workaround.

- CSCui91537

  Symptom: When new flows are established through an ASR configured with PAP; PAP does not allocate the new flows to GA that may have existing flows mapped it but their LA to GA mapping have not reached the limit as configured via the ip nat setting pap limit command, this causes an exhaustion of the pool and flows that require a translation are eventually dropped.

  Conditions: ASR running NAT PAP

  Workaround: There is no workaround.

- CSCui91855

  Symptom: vrf-mismatch is seen under "show service-insertion statistics connection summary" after ESP Switch over in same box

  Conditions: - Multiple ACs - At least 1 AC with dual FP - VRF configured - 1 VRF flows alive while reloading standby FP - Standby FP will come up with vrf mismatches

  Workaround: ignore the error the VRF mismatch affects flow sync only for a short moment after standby FP is online. After the standby FP is online, it will get flow syncs from active FP. In few minutes, all the flows will be synced to standby.

- CSCui91872

Symptom: When configuring the following commands on ASR1k platform: exception memory ignore overflow io frequency 30 maxcount 5 exception memory ignore overflow processor frequency 30 maxcount 5 following error occurs:

```
F340.09.25-ASR1000-1(config)#$re overflow processor frequency 30 maxcount 5
F340.09.25-ASR1000-1(config)# *Aug 22 12:54:24.920: exception configuration not
implemented *Aug 22 12:54:24.920:  PARSE_RC-4-PRC_NON_COMPLIANCE<
http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi?action=search&counter=0&pa
ging=5&links=reference&index=all&query=PARSE_RC-4-PRC_NON_COMPLIANCE> ;  `exception
memory ignore overflow processor frequency 30 maxcount 5'
```

Conditions: HW/SW: ASR1k/All IOS Non zero values in following commands: exception memory ignore overflow io exception memory ignore overflow processor example: exception memory ignore overflow io frequency 30 maxcount 5 exception memory ignore overflow processor frequency 30 maxcount 5

Workaround: There is no workaround.

- CSCui95380

  Symptom: sis neigh can not be setup and stuck at "init" status

  Conditions: when configured the MTU bigger than default value

  Workaround: There is no workaround.

- CSCui95632

  Symptom: Error message seen

  Conditions: while configuring multipoint on ATM interface.

  Workaround: There is no workaround.

- CSCui95988

  Symptom: Can not compile.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCui96679

  Symptom: On a Cisco ASR1k running the Cisco CUBE SP (Service Provider) feature set, IOS-XE version 15.1(3)S1, it is sometimes observed that a specific call transfer will have no way audio (dead air) upon the transfer completion.

  Conditions: The CUBE SP has at least three physical interfaces that terminate three different SIP trunks (for example to ITSP, SIP based IVR and to a Cisco Callmanager) and the problematic transfer call flow signaling traverses all three SIP trunks on the same CUBE.

  Workaround: If you have more than one CUBE available and if one of the transfer call leg traverses this second CUBE then the problem is not observed.

- CSCui97039

  Symptom: CUBE fails to send INVITE with credentials when ITSP sends 401 Unauthorized. CUBE instead sends 503 Service Unavailable.

  Conditions: "error-passthru" is configured under voice service voip.

  Workaround: Disable "error-passthru".

- CSCui97685

  Symptom: While testing "default_zone_basic_vrf_lite.tcl" script with latest mcp_dev "BLD-BLD_MCP_DEV_LATEST_20130821_003026" iam observing connectivity failure

- Conditions: Firewall and PBR interworking after CSCuh98033

  Workaround: There is no workaround.

- CSCui98934

  Symptom: ATM PVC gets stuck in "IN" state when SPA-24CHT1-CE-ATM is reloaded.

  Conditions: Occurs during SPA reload or SPA OIR

  Workaround: Reload router.

- CSCui99433

  Symptom:

  1. INFO not being responded by CUBE (in race condition)

  2. INFO not being passed to other leg (in race condition)

  Conditions: Race condition - Recvd mid-call RE-INVITE and INFO at almost the same time

  Workaround: There is no workaround.

- CSCui99856

  Symptom: sm_x_1t3e3: 802.3 pause frame support on mvl 2.6.32 kernel

  Conditions: during congestion case

  Workaround: limit the traffic from the host less than 45 mbps

- CSCuj00449

  Symptom: Hung sessions for protocol vilolations

  Conditions: CUBE handling of unsupported flows and violations/attacks

  Workaround: There is no workaround.

- CSCuj01420

  Symptom: ESP ucode crash observed with a SIPvicious packet observed %CPPHA-3-FAULT: F0: cpp_ha: CPP:0.0 desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL id:2121 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x8

  Conditions: The crashes are seen with SIPvicious packets

  Workaround: Disable the SIP ALG for this port using no ip nat service sip udp port 5060 no ip nat service sip tcp port 5060 .

- CSCuj03101

  Symptom: permit error all is not working

  Conditions: log dropped message is enabled

  Workaround: log dropped message is disabled.

- CSCuj03148

  Symptom: "show platform hardware slot r0 led status" may cause ASR1002X reload.

  Conditions: "show platform hardware slot r0 led status" command on standalone ASR1002X.

  Workaround: Not using the command.

- CSCuj04100

  Symptom: ASR1k crashed with error message CPPHA-3-FAULT F0: cpp_ha: CPP:0.0 desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL id:2121 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x8

Conditions: ASR1k running 03.10.00.S with configured zone based firewall

Workaround: There is no workaround.

- CSCuj04321

  Symptom: ASR crashed with CGN NAT configuration.

  Conditions: Seen with CGN BPA feature configured.

  Workaround: Removing the CGN BPA configuration, the router stops crashing.

- CSCuj05175

  Symptom: Crash with Unexpected exception to CPU: vector 400, PC = 0x6B09EF1C, LR = 0x8B78034

  Conditions: Interface is "no shut", and SIP bindings are in place on that interface: sip bind control source-interface GigabitEthernet0/0 bind media source-interface GigabitEthernet0/0

  Workaround: Unknown, may need bindings configured, so removal of them should keep the crash from occurring.

- CSCuj10937

  Symptom: TDL meta file compat check issue

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuj11301

  Symptom: Standby SBC ASR1k seeing "SNMP-3-INPUT_QFULL_ERR". SNMP input queue never drops, it continues to increase until it gets stuck at 1000, causing SNMP unresponsiveness to the device.

  Conditions: When polling ciscoSbcCallStatsMIB on Standby-RP ASR1k

  Workaround: "default snmp-server" to soft reset the SNMP Engine to make the ASR1K respond again (refresh the input queue); then apply SNMPVIEW configuration to block the MIB.

```
 ****************************************
snmp-server view cutdown iso included snmp-server view cutdown ciscoSbcCallStatsMIB
excluded snmp-server community <insert_your_community_string_here> view cutdown RO
snmp-server community <insert_your_community_string_here> view cutdown RW
****************************************
```

- CSCuj11722

  Symptom: ESP reload using packet-trace tool.

  Conditions: debug platform packet-trace enable debug platform packet-trace packet 16 show platform packet-trace packet all

  Workaround: Display packets individually rather than all at once: show platform packet-trace packet <0-8191>

- CSCuj14693

  Symptom: modify bearer request is dropped.

  Conditions: handoff from gtpv1 to gtpv2

  Workaround: SGW recreate session

- CSCuj16006

  Symptom: Egress TCAM Look up failure for Vlan Scale on 6 Port 10G ELC.

Conditions: 24k vlan scale across ELC & interface reset.

Workaround: There is no workaround.

- CSCuj17402

  Symptom: Lite session related traceback in CPP client.

  Conditions: ESP100, very high scale.

  Workaround: Reduce number of sessions.

- CSCuj17482

  Symptom: On a router running low on memory, an EFP is attempted to be deleted, but fails due to lack of memory. The second attempt at removing that same EFP causes the router to restart.

  Conditions: As a malloc failure caused the initial issue, the box must have a lot of configuration, and be using a lot of memory.

  Workaround: Do not over configure the router.

- CSCuj21230

  Symptom: ASR1k can't reconnect IPsec tunnels correctly. And we can't send traffic over these tunnels.

  Conditions: Disconnect and reconnect IPsec tunnels.

  Workaround: Clearing sa can recover the tunnels.

- CSCuj21502

  Symptom: show run only shows 191 na-dst-prefix-table out of 200

  Conditions: configured a lot of na-dst-prefix-table, specially, more than 191

  Workaround: none na-dst-prefix-table 192 to 200 seem to be working OK, but cannot be shown and cannot save them into startup-config.

- CSCuj22189

  Symptom:ASR crash immediately when we add "mpls ip" under the interface.

  Conditions:Hidden command "snmp-server hc poll" was already configured.

  Workaround: Ensure the hidden command "snmp-server hc poll" has not been configured. The crash info also shows that the crash always happens always the following changes .

  ```
  CMD: 'conf t' 15:33:05 CEST Mon Sep 2 2013 CMD: 'interface GigabitEthernet1/0/0'
  15:33:11 CEST Mon Sep 2 2013 CMD: ' mpls ldp discovery transport-address interface'
  15:33:21 CEST Mon Sep 2 2013 CMD: ' mpls ip' 15:33:40 CEST Mon Sep 2 2013  Exception
  to IOS Thread: Frame pointer 0x42201488, PC = 0x11F0DE04  UNIX-EXT-SIGNAL:
  Segmentation fault(11), Process = MPLS IFMIB Process -Traceback=
  1#6b213acfe4ab8a0e4e3d7d7ea5d15df7  :10000000 1F0DE04 :10000000 15FB4E4 :10000000
  15FB318 :10000000 15F8898 :10000000 15F8A1C
  ```

- CSCuj24461

  Symptom: ESP crash

  Conditions: NAT NBAR

  Workaround: There is no workaround.

- CSCuj24622

  Symptom: ISSU

  Conditions: There is no known condition.

Workaround: There is no workaround.

- CSCuj25418

  Symptom: The ESP-100 and ASR1K-2X crash when flat policies are applied on both the tunnel and the destination sub-interface. This issue is observed when QOS is applied first on the tunnel then on the sub-interface as follows:

  ```
  policy-map tunnel-shaper  class class-default    shape aver per 20  policy-map
  sub-int-shaper   class class-default      shape ave per 90  Be sure the tunnel is
  active and pointing to the sub-interface with QoS applied before applying the
  sub-interface policy. See the attached repro-steps for details.  int tunnel1
  service-policy out tunnel-shaper  int g2/3/0.100   service-policy out sub-int-shaper
  ```

  Conditions: When a sub-interface policy is applied after QoS is active on a tunnel, the tunnel is reparented from the current aggregation node to the sub-interface node. Since reparenting a leaf node requires adding a temporary node in the hierarchy to be able to move flow-control gracefully, the logic to detach the source leaf node from the temporary node was missing. As a result, the code generated a fatal error while attempting to free the temporary node before it is empty.

  Workaround: There is no workaround.

- CSCuj29429

  Symptom: FP100 test CPLD image with version 13012900 is added in hw-programmable package.

  Conditions: The FP100 test CPLD will be installed when the CPLD is upgraded.

  Workaround: Do not upgrade FP100 CPLD.

- CSCuj29469

  Symptom: Waas and pfr features don't interoperate

  Conditions: When both Appnav-waas and pbr/pfr are turned on

  Workaround: There is no workaround.

- CSCuj31151

  Symptom: If an impedance option is specified for an external clock in the network-clock **input-source** configuration, other configuration (such as hold-off or wait-to-restore) may fail to be applied.

  Conditions: This can be seen when using external clock inputs with an impedance option specified.

  Workaround: It may be possible to achieve the desired behavior using global configuration (for example global hold-off or wait-to-restore configuration), if not there is no workaround.

- CSCuj33916

  Symptom: For VC type 4 PW, Ethernet VLAN, with single dot1q header packet, if one configure rewrite pop 1, expected situation is to copy COS from this header into dummy tag. In reality, we hit a bug, when COS 0 is copied into dummy tag into CORE.

  Conditions: When transported traffic has outer vlan tag only, packet in MPLS core does NOT have copied priority field from dot1q header into MPLS EXP bits. Instead there is 0. When transported traffic has outer vlan tag and some vlan tags (QinQ) , packet in MPLS core DOES have copied priority field from outer dot1q header into MPLS EXP bits.

  Workaround: Configure input policy-map under service-instance, where each class match dot1Q COS and impose EXP bits.

- CSCuj39458

  Symptom: cvCallVolMediaIncomingCalls and cvCallVolMediaOutgoingCalls are showing 0 or wrong values

Conditions: Always

Workaround: There is no workaround.

- CSCuj42585

  Symptom: When a flat policy is applied to a MLPPP, MFR or GEC aggregation bundle, the current leaf schedule object is replaced with a new one. The code was not updating the cached object which resulted in accessing invalid memory when the bundle bandwidth is updated. The bandwidth is updated when a member link is added to or removed from the bundle. Configuration example: policy-map foo class prec1 bandwidth percent 10 interface Port-channel1 aggregate ip address 8.0.0.1 255.255.255.0 no negotiation auto lacp min-bundle 2 service-policy output foo

  Conditions: When a bundle schedule is replaced, the cached object was not being updated leading to interface bandwidth update event to access invalid memory. The problem is not easy to recreate as would require the QOS event for processing the flat policy to be interleaved with an interface bandwidth update event.

  Workaround: There is no workaround.

- CSCuj46180

  Symptom: echo request is dropped.

  Conditions: echo request without private extension IE

  Workaround: There is no workaround.

- CSCuj46330

  Symptom: Both ESP may crash

  Conditions: while disabling flow entries with running traffic

  Workaround: There is no workaround.

- CSCuj47795

  Symptom: When using ikev2 to establish an AES-GCM phase II, anti-replay remains disabled

  ```
  R1-HUB#sh crypto ipsec sa  | i trans|repl         transform: esp-gcm 256 ,
  replay detection support: N         transform: esp-gcm 256 ,
  Conditions: IKEv2   Suite B [ aes-gcm]
  ```

  Workaround: There is no workaround.

- CSCuj48314

  Symptom: REST API application will not connect with container

  Conditions: All

  Workaround: There is no workaround.

- CSCuj51645

  Symptom: Pause frames not getting generated for GE SPA

  Conditions: If enabled pause frame threshold on Gig SPA then flow control won't happen.

  Workaround: There is no workaround.

- CSCuj52287

  Symptom: ESP crashed with error message: `%CPPHA-3-FAULT: F0: cpp_ha: CPP:0.0 desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL id:2121 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x8`

  Conditions: The crash is caused by a defect in BFD though no BFD is configured on any interface

Workaround: There is no workaround.

- CSCuj58272

  Symptom: The CP process crashes when reparenting more than 128 entries from one tree to the other. A reparenting event could be stimulated by either an internal or external event but this issue is more likely to caused by an internal reparenting. An internal reparenting could occur when a leaf node is transformed into a hierarchy layer node or when de-aggregating an aggregation node after the schedule size is below the 4000 threshold.

  Conditions: When reparenting either a leaf or hierarchy layer entries, the resource manager was not clearing the counter that tracks the number of entries that need to be flushed after processing the first batch. This caused the code to run incorrectly to a point of completing the request prior to reprogramming the HW correctly. As a result some entries may be left in the source parent which cause a crash when the tree is freed before it is empty.

  Workaround: There is no workaround.

- CSCul10907

  Symptom: Cisco ASR 1000 Series Routers with ESP100 crash when Broadband MLPPP sessions configured with QoS are brought up or when sessions flap.

  This also applies to the ASR1002-X .

  Conditions: This issue is most prevalent on MLPPP Bundles with two or more member links. This issue also is seen with MLPPPoE, MLPPPoA, MLPPPoEoA, and MLPPPoLNS sessions.

  Applicable to Cisco IOS-XE Release 3.10.1S.

  Workaround: There is no workaround. Downgrade to Cisco IOS XE Release 3.10S.

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.1S

This section documents the open issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.1S.

- CSCtx72973

  Symptom:Config-sync failure is seen when unconfiguring the crypto gdoi group.

  Conditions: This symptom is observed on a HA setup.

  Workaround: There is no workaround.

- CSCuc24927

  Symptom: Segmentation fault on loading latest XE38 and XE37 image occurs

  Conditions: This symptom is observed when IMA, CEM, and Serial are configured on different controllers and try to load image. Some time observed when CEM on TDM and MLPPP QoS on OC3 IM is configured and do multiple reloads. When there is a segmentation fault, RSP will not come up, will go to rommon mode.

  Workaround: Do not combine IMA, CEM and Serial configs. If you test each feature individually it works fine.

- CSCue48456

  Symptom: Call is disconnected through CUBE.

  Conditions: Occurs on a video call where a mid-call re-INVITE occurs to modify the media stream.

Workaround: There is no workaround.

- CSCue59450

  Symptom: IOS XE Watchdog message seen along with RP and SIP crash

  Conditions: This symptom is observed when continuous ARP request on the interface having VRF Receive configured on it.

  Workaround: There is no workaround.

- CSCug19588

  Symptom: IKEv2 TPS performance degradation over time.

  Conditions:This occurs in the lab under extreme test conditions with traffic running during session bring-up.

  Workaround: Reduce traffic and or reduce session bring-up rate.

- CSCug84557

  Symptom: CUBE SBC does not forward mid-call Re-INVITE in a glare condition.

  Conditions: This symptom is observed in a condition where both legs of a SIP call through the SBC sends in Re-INVITE within 100ms of each other. Instead of forwarding the first arriving Re-INVITE to the other leg and then rejecting the other with a 491 Request Pending response, SBC does not forward either of the Re-INVITE and gets into a deadlock condition leading to no audio and an eventual call tear down.

  Workaround: There is no workaround.

- CSCuh27266

  Symptom: CPP core not generated when FP crash happen

  Conditions: This symptom is observed in a condition when you perform SPA OIR with Unicast/Multicast/Broadcast storm control on 32k EFPs

  Workaround: There is no workaround.

- CSCuh32580

  Symptom: unexpected crash after defaulting and reconfiguring the interface

  Conditions: This symptom is observed in a condition where a suspected trigger could be defaulting the interface multiple times configured lldp/cdp timers and re-configuring the interface

  Workaround: There is no workaround.

- CSCuh54693

  Symptom: Crypto Socket remains CLOSED on DmVPN setup

  Conditions: This symptom is observed in a condition when you use DmVPN with extended command to mention IKE profile as the ISAKMP profile

  Workaround: Remove the ikev2 profile configuration from the ipsec profile.

- CSCuh59992

  Symptom: Router Crash on executing the command "show ip eigrp events"

  Conditions: This symptom is observed in a condition when PID:RSP720-3C-10GE IOS:15.1(3)S5 crash occurs only if BFD is enabled on EIGRP and the eigrp configuration has more than one AS/VRF in the same address family. The crash is seen only on images having eigrp component version (reported in "show eigrp plugin') rel9 or older. Newer images does not crash.

Workaround: Right action to take now is to advise not to use the **show ip eigrp event** command for the time being. The command produces output interpretable only by cisco DE community. Another option is to upgrade to images having eigrp version rel 10 or newer.

- CSCuh70997

  Symptom: Memory leak observed in l2fib_nhop, l2fib_nhop_key,l2fib_nhop_update

  Conditions: This symptom is observed in a condition when you clear xconnect all - during longevity

  Workaround: There is no workaround.

- CSCuh73422

  Symptom: ASR1k With MAP-T Configs crashes.

  Conditions: This symptom is observed in a condition when Ping Initiated to public IPV4 Address, ASR1K crashes with Core dump, and the packet was translated but the packet causes an ICMP error message to be generated, and in some cases of ICMP error generation, the box could crash.

  Workaround: There is no workaround.

- CSCuh97072

  Symptom: Under certain rare circumstance, ZBFW will not properly build the connection for the first packet of the flow. This causes subsequent packets to be dropped due to TCP state checking.

  Conditions: This was first observed when NAT, ZBFW and HA were all enabled on the ASR platform. This only affects ASR platforms.

  Workaround: Removing and re-adding the NAT configuration resolves the issue. Sometimes it requires readding the NAT configuration without any redundancy keywords before readding it with the redundancy keywords.

- CSCui04262

  Symptom: An error syslog is seen on ASR1K BRAS running XE352.P3 Standby-RP, showing QOS service-policy installation failures:

  ```
  1. Jun 13 14:43:55.323 CEST: %QOS-6-POLICY_INST_FAILED: Service policy installation
  failed

  2. Jun 13 14:47:10.725 CEST: %QOS-3-INDEX_DELETE: class-group unable to remove index
  00B6AA60  3. Jun 13 14:47:10.726 CEST: %QOS-3-UNASSIGNED: A CLASS_REMOVE event
  resulted in an (un)assigned index for class-group
  target-input-parent$class-default$IPBSA>ci=3#qu=3#qd=4#co=4#pu=police#ru=200K#pd=po
  lice#rd=300K<_IN$class-default  4. Jun 13 14:47:10.727 CEST: %QOS-6-RELOAD: Index
  removal failed, reloading self
  ```

- Conditions: On ASR1K BRAS, running XE352.P3, Version 15.2(1)S2, CUST-SPECIAL:V152_1_S2_CSCUA32331_4 When churning PPPoE sessions with 2 unique ISG/Shell map services per session, and after a manual RP Failover is done, after a while the error will be seen.

  Workaround: There is no workaround.

- CSCui10507

  Symptom: The memory in the Radius Local Server Process increases until it's consumed:

  ```
  Bay-ISG3#show process memory sort Processor Pool Total: 10194931312 Used: 4187932720
  Free: 6006998592  lsmpi_io Pool Total:    6295128 Used:    6294296 Free:        832
  PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process  439   0
  1353539672400        448 2151487056          0          0 RADIUS LOCAL SER
  ```

  Conditions: This issue occurs with AAA and ISG sessions.

  Workaround: There is no workaround.

- CSCui20319

  Symptom: Pending issues/ack is observed on ESP

  Conditions: Must meet all following conditions:

  1. When port-channel vlan loadbalacing mode is enabled on Port-channel EVC with large scale of EFPs on one port-channel (8000 in this case)

  2. EFPs on Port-channel are assigned to different links.

  3. When the efps and port-channel are remove using one command "no int port-channel x"

  4. Then the scale config and link assignment are added back by copying back the scale config

  Workaround: Separate EFP removal and port-channel link removal (remove efps, the remove int port-channel) separate EFP config and port-channel link config (add EFP first, then add links to port-channel).

- CSCui37439

  Symptom: **show platform software ipsec FP active inventory** output not seen

  Conditions: This symptom is observed after FP upgrade.

  Workaround: There is no workaround.

- CSCui38300

  Symptom: High latency observed in customer network

  Conditions: Under certain conditions, particularly under forced test conditions, it is possible to create scenarios where flow lock contention will be very high because of NAT gatekeeper failures.

  Workaround: There is no workaround.

- CSCui48572

  Symptom: **show platform hardware qfp active infrastructure shared-memory process cpp-service-process?**.

```
ott-mcp-bld-12:134> mcp_gdb_core -c
/tftpboot/leolia/RZN001-ASR1004-1_ESP_0_cpp_sp_svr_7162.core.gz  Program terminated
with signal 11, Segmentation fault. #0  shml_dlmallinfo (hdl=0xbfa9ca88,
mi_ptr=0xbfa9caa4) at
cpp/oslib/shml/lib/binos/shml/../../cmn/src/../../cmn/src/shml_dlmalloc.c:2501 2501
avail  = chunksize(p);  ** backtrace follows  #0  shml_dlmallinfo (hdl=0xbfa9ca88,
mi_ptr=0xbfa9caa4) at
cpp/oslib/shml/lib/binos/shml/../../cmn/src/../../cmn/src/shml_dlmalloc.c:2501 #1
0x0f5fe238 in shml_mallinfo_from_base (appl_shm_base_addr=1879048192,
shml_minfo=0xbfa9caf8) at
cpp/oslib/shml/lib/binos/shml/../../cmn/src/../../cmn/src/shml_api.c:1165 #2
0x0f5cfd18 in cpp_shm_win_info (shm_appl=CPP_SHML_APPL_CGM, cpp_shm_minfo=0xbfa9cb38)
at cpp/oslib/lib/binos/src/../../binos/src/cpp_shm_mgr_binos.c:683 #3  0x0f5cfe40 in
cpp_shm_get_all_win_info (shm_info_cb=0xf5c7274 <cpp_shm_win_info_show_cb>,
user_ctx=0x10cc6ae8) at
cpp/oslib/lib/binos/src/../../binos/src/cpp_shm_mgr_binos.c:713 #4  0x0f5c77dc in
cpp_shm_mgr_show_cb (con=0x10514f00, cmd=0x10899cb0, eb=0xf5eb7e0 "", eb_sz=405) at
cpp/oslib/lib/binos/src/cpp_shm_mgr_ui_binos.c:231  (gdb) f 4 #4  0x0f5c77dc in
cpp_shm_mgr_show_cb (con=0x10514f00, cmd=0x10899cb0, eb=0xf5eb7e0 "", eb_sz=405) at
cpp/oslib/lib/binos/src/cpp_shm_mgr_ui_binos.c:231 231         rc =
cpp_shm_get_all_win_info(cpp_shm_win_info_show_cb, (void *)ui_ctx);  (gdb) p *cmd $30
= {   ui_request_data = {     command = "show platform hardware qfp active
infrastructure shared-memory process cpp-service-process ", '\0' <repeats 932 times>,
client_loc = {       fru = BINOS_FRU_RP,       slotnum = 0,       baynum = 0     },
client_type = UICLIENT_BSHELL_SCRIPTED,    ui_term_type = UITT_TTY,    ttynum = 0,
```

```
tty_name = "unknown", '\0' <repeats 24 times>,     user_name = '\0' <repeats 64
times>,     request_name = "show_cpp_shm_mgr_info_req", '\0' <repeats 486 times>   },
ui_request = 0x10899cb0
```

Conditions: There is no known condition.

Workaround: There is no workaround.

- CSCui61103

  Symptom: After an NHRP network spoke-spoke mapping entry refresh, the mapping entry is missing teh 'rib' or 'rib nho' flag settings and NHRP has cleared corresponding NHRP route or next-hop-override from route in the RIB. Data packets are forwarded via the spoke-hub-spoke tunnel path rather than the direct spoke-spoke tunnel path. Conditions: Running DMVPN Phase 3 on ASR1k or with IOS code 15.2(1)T or later. Data traffic loading spoke routers using spoke-spoke tunnel. Multiple NHRP network mapping entries for different subnets using the same spoke-spoke tunnel.

  Workaround: There is no workaround.

- CSCui61928

  Symptom: Chunk mgr process holds lot of memory and doesn't release it which may lead to insufficient processor memory

  Conditions: Constantly flapping static BFD session. Does not affect dynamic BFD sessions.

  Workaround: Either of:

  1. Preventing a constantly very fast flapping static BFD session,

  2. Removing BFD configuration

  3. Configure BFD dampening (in the BFD template mode)

- CSCui74609

  Symptom: After a RSP switchover the backup pseudowire state is down and never recovers to standby state.

  Conditions: This symptom occurs on CEM circuits in a SAToP environment after a SSO switchover.

  Workaround: There is no workaround.

- CSCui74757

  Symptom: ESP crashes running 3.9.1 when NAT enabled

  Conditions: This symptom occurs when Nat is enabled.

  Workaround: There is no workaround.

- CSCui80542

  Symptom: Sending a PING to an IPv6 EID from a Proxy ITR without specifying the source interface can cause a crash which resets the FO.

  Conditions: When sending an ICMPv6 packet, we try to set the source UDP port, and depend on the source interface supplied in the exec command to do that. When the source interface is not included in the ping command, the source UDP port is invalid, and a crash ensues when LISP attempts to use it.

  Workaround: Include 'source <interface>' to ping commands on the Proxy ITR

- CSCuj04178

  Symptom: Crash occurs at vpdn_apply_vpdn_template_pptp.

  Conditions: There is no known condition.

Workaround: There is no workaround.

- CSCuj19361

  Symptom: After the Lebowski module is reloaded from Switch command line, the Data Plane does not come up even though Control Plane is up.

  Conditions: Need to reload the Lebowski switch module from module Exec prompt.

  Workaround: Reload the switch by using the **hw-module subslot <> reload** command from host for reload.

- CSCuj23498

  Symptom: A crash is seen in the Crypto PKI-CRL process:

  ```
  Exception to IOS Thread: Frame pointer 0x3CC01C78, PC = 0x1309A558  UNIX-EXT-SIGNAL:
  Segmentation fault(11), Process = Crypto PKI-CRL -Traceback=
  1#b41b6cddd4ffa19c791ecae845f92f71  :10000000 309A558 :10000000 309A4C4 :10000000
  309EC80 :10000000 309F920
  ```

  Conditions: This device is using an LDAP server to provide PKI/Cert data to the DMVPN tunnels. The crash occurs after the CRLs are received and verified for insertion. Before the crash we saw alot of certificate invalid errors as well as some occasional looped chain messages:

  ```
  747    2922087633: 000118: *Sep  7 06:37:59.927 UTC: %ADJ-5-PARENT: Midchain parent
  maintenance for IP midchain out of Tunnel1, addr xxx.xxx.xxx.xxx - looped chain
  attempting to stack 748    2923902634: 000120: *Sep  7 06:38:01.742 UTC:
  %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from xxx.xxx.xxx.xxx is bad:
  certificate invalid 749    2923928634: 000120: *Sep  7 06:38:01.768 UTC:
  %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from xxx.xxx.xxx.xxx is bad:
  certificate invalid 750    2924094633: 000120: *Sep  7 06:38:01.934 UTC:
  %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from xxx.xxx.xxx.xxx is bad:
  certificate invalid 751    2924416638: 000121: *Sep  7 06:38:02.256 UTC:
  %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from xxx.xxx.xxx.xxx is bad:
  certificate invalid
  ```

  Likely the issue is related to the certificate is bad error but its possible the routing issue is also helping trigger the issue.

  Workaround: Since the issue appears to occur when verifying the CRL, we might be able to stop the crash by turning off CRL checking: "revocation-check none" We also might be able to decrease the chances of hitting this bug by using one CDP instead of multiple CDPs

- CSCuj25477

  Symptom: Traffic failure after LC OIR Conditions: hw-module mod 3 reset. after which traffic failure is seen. Workaround: As a workaround if we clear the cry session in peer end tunnels are coming up again

- CSCuj39478

  Symptom: ASR100x running IOS XE version 15.3(1)S configured as a CUBE Ent may occasionally and randomly crash with Segmentation fault(11) and RP with over may happen with the following trace backs on the console logs.

  ```
  Exception to IOS: Frame pointer 0x7F98F04FB980, PC = 0x3A534E6 IOS Thread backtrace:
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = IOSXE-RP Punt Service Process
  -Traceback= 1#9821b08208133f5124c039ddebb8173b  :400000 36534E6 :400000 203F6E8
  :400000 1A9972F :400000 1A2C3B4 :400000 1A52F50 :400000 6487473 :400000 6486359
  ```

  Conditions: There is no known condition.

Workaround: Since the crash is reported when port 26132 was used, by not using this port (udp port 26132 which was corresponding to the index 4874 in port_array). crash can be avoided. This can be done by changing the port range to something like 26134 to 32767 (currently it is 16384 to 32767) but this will reduce the number of CUBE calls from 4000 to around 1600 calls. In XE3.10.1, this port range is 8000 to 48199 by default, so we will have a bigger port range to start with, and in this case the port corresponding to index 4874 is 17748, so we will have to change the port range to 18000 ? 48199 using the configuration. In addition XE3.10.1 also allows configuration where the packets can be dropped in DP if no session exists in DP. This will not cause any one way audio as the IOSd is not really meant to process the media on ASR, and if there are any media issues those need to be addressed differently.

- CSCuj39496

  Symptom: When configuring Input MPLS aware FNF (under interrface config --- mpls flow mon MON_NAME in) it can happen that FNF will cease to function due to cache entry leak/exhaustion.

  Conditions: This symptom occurs when configuring Input MPLS FNF and moreover only will occur with certain labels. In particular it will occur for MPLS labels for which the output of **show plat hard qfp active feature cef-mpls prefix mpls <LABEL NUM>** does *not* have an IPV4 adjacency.

  Workaround: There is no workaround.

- CSCuj39901

  Symptom: Crash with "ip nat settings mode cgn" in teh config

  Conditions: There is no known condition.

  Workaround: Reload after changing settings.

- CSCuj52299

  Symptom: Outside to Inside connections fails for TCP traffic on ASR with static NAT entries (Intra-vrf)

  Conditions: This condition is observed on ASR with multiple static nat entries.

  Workaround: Remove and reapply affected static nat entry.

- CSCuj65601

  Symptom: Not able to login router via ssh and telnet with AAA

  Conditions: This condition is observed where in the tacacs server group should contain ipv6 source interface and need to removed and add ipv6 source interface. after that ssh and telnet is not working

  Workaround: There is no workaround.

- CSCuj66352

  Symptom: System crash in SNMP engine

  Conditions: This condition is observed when using **show subscriber session** command polling the ISG-MIB - Clearing subscriber

  Workaround: No SNMP polling

- CSCuj68932

  Symptom: L2TPv3 tunnel with digest fails to establish. Cisco IOS device gives the following messages when "debug l2tp all" and "debug l2tp packet detail" are enabled -

```
L2TP       _____:________: ERROR: SCCRQ AVP 59, vendor 0: unknown
L2TP       _____:________: Unknown IETF AVP 59 in CM SCCRQ
```

Conditions: This issue is observed when IOS device peers with non-IOS device that sends IETF L2TPv3 digest AVP (IETF AVP 59) in L2TP control message. This issue is present in S images starting from 12.2(33)XNC release and in T train from 15.3(2)T release.

Workaround: There is no workaround.

- CSCuj75952

  Symptom: ASR1K route processor reloads.

  Conditions: ASR1K is being used to terminate PPPoA sessions and Call Admission Control (CAC) has been enabled. The crash occurs during PPPoA session establishment if CAC determines that resources are low and HW assisted CAC needs to be enabled.

  Workaround: Disabling Call Admission Control is the only known workaround.

- CSCuj79195

  Symptom: Crash in ASR router when platform hardware debug is enabled

  Conditions: This condition occurs when platform hardware debug is enabled.

  Workaround: There is no workaround.

- CSCuj85408

  Symptom: For VPLS mstp test Bpdus are not receiving

  Conditions: When this condition occurs packet drop are seen.

  Workaround: There is no workaround.

- CSCuj91523

  Symptom: An ESP crash is seen. This will cause forwarding to stop for a few minute

  Conditions: An ESP on an ASR1000 crashed multiple times after making some changes to Netflow and AVC. The issue was first seen on 15.3(2)S1

  Workaround: This issue occurs with Flexible Netflow and AVC configurations. The exact conditions are still being investigated .

Caveats in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.0S

This section contains the following topics:

Resolved Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.0S

This section documents the resolved issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.0S.

- CSCtc17240

Symptoms: Some third party SIP PBXs may have interoperability problems with the authentication header of a Cisco SIP gateway.

Conditions: Per RFC 3261 section 25.1, the "nc" value, or nonce-count, should have lower case hex. This is defined as follows:

```
nonce-count       =  "nc" EQUAL nc-value nc-value          =  8LHEX  LHEX  =  DIGIT
/ %x61-66 ;lowercase a-f  A snippet of the offending messaging:  ...
cnonce="305EE7FF",qop="auth",algorithm=MD5,nc=0000000A
```

Workaround: There is no workaround.

- CSCti43486

  Symptom: Summary option was not available in **show crypto gdoi ks member**

  Conditions: New option added to this CLI.

  Workaround: There is no workaround.

- CSCtj24692

  Symptom: Nvram config file gets corrupted when a chassis is power cycled without a graceful shutdown.

  Conditions: Power cycle an ASR chassis without graceful shutdown.

  Workaround: Shutdown chassis using **reload** command and make sure RP gets to rommon before power cycling the chassis.

- CSCtl55445

  Symptom: CUBE logging the following message:

  ```
  %SIP-3-INTERNAL: Cannot insert call history entry for callID
  ```

  Conditions: Calling party cancels call before connection:

  ```
  INVITE     --------------->---------------->    100 Trying
  <--------------<----------------   180 Ringing    <--------------<----------------
  CANCEL     ---------------->---------------->    200 OK
  <----------------<-----------------    487 Request Cancelled
  <------------------<---------------       ACK
  ------------------->--------------->
  ```

  Workaround: There is no workaround.

- CSCto64199

  Symptom: Queuing has not shifted to other interface

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCto81601

  Symptom: If there is a problem with publishing the certificate revocation list (CRL), a major problem must exist and so that further publishing is suspended until the issue is addressed and the CA requires a shut/no shut. Currently there is no error message which suggests what happened with CRL. Need to add proper error messaging to make it more interactive

  Conditions: There is no known condition.

  Workaround: A "shut" / "no shut" on the CA server should result in the CRL being published again.

- CSCtx99353

  Symptom: Error message on router %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level The error message can lead the device to crash

Conditions: The symptom is observed when music on hold (MOH) is enabled.

Workaround 1: Remove the route list from the multicast MOH CLI, so that you can still have music on hold and can continue the feature.

Workaround 2: Disabling the MOH (but no music comes on hold).

- CSCty59423

  Symptoms: Memory leak seen with following messages:

  ```
  Alternate Pool: None  Free: 0  Cause: No Alternate pool   -Process= "VOIP_RTCP", ipl=
  0, pid= 299 -Traceback= 0x25B1F0Cz 0x25AB6CBz 0x25B1029z 0x46C02Ez 0x46C89Bz
  0x46BCC2z 0x471D12z 0x43EF59Ez 0x43DD559z 0x43DCF90z %SYS-2-MALLOCFAIL: Memory
  allocation of 780 bytes failed from 0x46C02E, alignment 32
  ```

  Conditions: The conditions are unknown.

  Workaround: There is no workaround.

- CSCty91566

  Symptoms: Potential memory leak is seen when handling DNS lookup response.

  Conditions: This symptom is observed when handling DNS lookup response.

  Workaround: There is no workaround.

- CSCtz13023

  Symptoms: A SIP gateway may crash with a bus error.

  Conditions: This symptom is observed when the SIP gateway is configured as a SIP registrar. The configurations for this are as follows: voice service voip   sip   registrar server

  Workaround: There is no workaround available at this time.

- CSCua78771

  Symptom: Error message display needs cosmetic changes to follow style.

  Conditions: This symptom is observed in rare situations, when a error message is displayed. Need to update the message format to follow style guidelines.

  Workaround: There is no workaround.

- CSCua80616

  Symptom: SPA handle invalid message seen after doing 'hw-module subslot x/y shut' on ethernet line card (ELC).

  Conditions: This symptom is observed when we have multiple ELC sources configured i.e. Primary & secondary network clock sources from ELC & we execute ELC shut using 'hw-m sub x/y shut' command, we see SPA invalid handle error message.

  Workaround: There is no workaround.

- CSCua90097

  Symptom: flexVPN client ikev2 sa stuck at IN-NEG with status description: Initiator waiting for AUTH response

  Conditions: This symptom is observed when flexVPN server initial **clear crypto session** command to clear 4K crypto sessions. After crypto session recovered, there is 1 ikev2 sa at flexVPN client stuck at IN-NEG status. At flexVPN server, there is no ikev2 peer

  Workaround: flexVPN client is able to use **clear crypto ikev2 sa psh <index>** command to delete stuck ikev2 sa

- CSCub05364

Symptom: Router acting as SRTP gateway crash

Conditions: This symptom is observed when a router printing the message SYS-4-CHUNKSIBLINGSEXCEED for "Srtp stream chunk" process prior to the crash

Workaround: There is no workaround.

- CSCub06422

  Symptom: Call flow: PSTN---pri---Voice Gateway---sip---SIP server After running fine for 6-7 days, calls through voice gateway fail (100% of the calls fail). On a call that comes in through the PRI, INVITE is sent with "m=audio 0..". Then, on getting "200 OK" from the other end, gateway disconnects the call.

  Conditions: This symptom is observed when router up and running for 6-7 days

  Workaround: Reload the router.

- CSCub18622

  Symptoms: Dynamic ACL does not get applied to the interface ACL, but the user shows up in the **show ip auth-proxy cache** command output.

  Conditions: This symptom is observed when auth proxy is configured on a tunnel interface.

  Workaround: Move the auth-proxy rules onto a physical interface.

- CSCub19185

  Symptoms: Path confirmation fails for a SIP-SIP call with IPV6 enabled.

  Conditions: This symptom is observed when UUTs are running Cisco IOS Release 15.2(2)T1.5.

  Workaround: There is no workaround.

- CSCub50350

  Symptom: Remote loopback messages under **show interface** and **show controller** output are not set correctly.

  Conditions: This symptom is observed when remote loopback configuration.

  Workaround: There is no workaround.

- CSCub56842

  Symptoms: The router stops passing IPsec traffic after some time.

  Conditions: This symptom is observed when the **show crypto eli** command output shows that during every IPsec P2 rekey, the active IPsec-Session count increases, which does not correlate to the max IPsec counters displayed in SW.

  Workaround: Reload the router before active sessions reach the max value. To verify, run the **show crypto eli** command:

  router#sh cry eli

  ```
  CryptoEngine Onboard VPN details: state = Active
  Capability    : IPPCP, DES, 3DES, AES, GCM, GMAC, IPv6, GDOI, FAILCLOSE, HA
  IPSec-Session :  7855 active,  8000 max, 0 failed .
  ```

- CSCub83722

  Symptom: Tunnel output rate packets are not incrementing.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCub98177

PPPoE session terminated by LAC with SSM DISCONNECT

Symptom: ASR1k as LAC running IOS XE RLS3.5.2 may disconnect PPP session by TermReq without visible reason, each time in **show pppoe stat** incrementing "SSM

Conditions: This symptom is observed in SSO mode during RP switchover

Workaround: There is no workaround.

- CSCuc09667

  Symptom: Router experiences crashes due to SIP due to a freed pointer in memory.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuc11170

  Symptom: GM removal did not work post COOP merge after experiencing a 3-way or more split

  Conditions: This symptom is observed when GETVPN COOP with 3-way (or more) Split and Merge, followed by any rekey or "gm removal"

  Workaround: There is no workaround.

- CSCuc25582

  Symptom: SIP secure phones drop calls when they Hold and Resume a call to a non-secure phone.

  Conditions: This symptom is observed under the following conditions:

  – CONDITION I (tested in lab): 8945 SIP Phone Reproduce steps: 3 phone A,B,C register to secure-SRST sip phone A B , sccp phone C. A,B in encrypted mode, phone C in non-secure mode. A call B, establish a secure call. B press transfer to C. After B and C establish a non-secure call, B press transfer. then B toast display "call transfered successfully!", but A and C do not establish a call. phone A and C should establish a non-secure call.

  – CONDITION II (Customer scenario): Secure SRST. SIP Phones registered to the router with secure and non-secure profiles. Call Flow: SIP Phone A (secure) ---> SIP Phone B (non-secure). A pressed Hold,Resume. SIP Phone A (secure) ---> SIP Phone C (secure) -----> Transfers call to SIP Phone B (secure). Phone A is not asked by router to stop transmitting SRTP and switch to RTP. Problem has been observed on 6941, 7962 and 8945 SIP phones.

  Workaround: There is no workaround.

- CSCuc25995

  Symptoms: A router unexpectedly reboots and a crashinfo file is generated. The crashinfo file contains an error similar to the following:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 04:52:23 UTC Wed Sep 19 2012 addr=0x4,
  pc=0x26309630z , ra=0x26309614z , sp=0x3121BC58
  ```

  Conditions: This symptom is observed when IPsec is used. More precise conditions are not known at this time.

  Workaround: There is no workaround.

- CSCuc29179

  Symptom: ASR1k filters out the ARP requests with its own source address. This leads to ping failure between two interfaces which belong to different vrf and own same IP subnet;vrf v1 1.0.0.1/24 and vrf v2 1.0.0.2/24, for instance.

  Conditions: - This symptom is observed when gig0/0/0 connected b2b to another interface on same router (with VRF configured on atleast one of the interfaces)

Workaround: - Configure some mac on gig0/0/0 and then unconfigure the mac.

- CSCuc31339

  Symptom: Console error message similar to the following:

  ```
  %ASR1000_INFRA-3-EOBC_SOCK: R0/0: linux_iosd-image:  Socket event for  EO0, fd 16,
  failed to send 1472 bytes; Resource temporarily unavailable
  ```

  Conditions: This symptom is observed when large number of feature configurations exist.

  Workaround: There is no workaround.

- CSCuc34574

  Symptoms: A pending-issue-update is seen at SSL CPP CERT on the Cisco ASR 1002, ESP-1000 platform.

  Conditions: This symptom is observed with the following configuration: show platform software object-manager fp active pending-issue-update Update identifier: 128 Object identifier: 117 Description: SSL CPP CERT AOM show Number of retries: 0 Number of batch begin retries: 0

  Workaround: There is no workaround.

- CSCuc44749

  Symptom: Audio distortion for MMOH stream produced by GW, when live-feed from FXO port is used

  Conditions: This symptom is observed when live-feed is implemented to produce MMOH stream in CME environment, where Live-Feed source is connected to an FXO port. File based MOH also to be configured, and the file needs to be in Cached state.

  Workaround: Remove the file based MOH or have a file based MOH which will not be cached.

- CSCuc58220

  Symptom: CME not pushing agent stats fields to tftp. (logged in and out times)

  Conditions: This symptom is observed when Benelli specific fields not getting pushed.

  Workaround: There is no workaround.

- CSCuc80859

  Symptom: Display related issue and some incorrect debug categorization

  Conditions: This symptom is observed when **debug ccsip feature <feature>** is configured.

  Workaround: There is no workaround.

- CSCuc99329

  Symptom: When we try to create or get a certificate with issuer-name same as that of any certificates that already exists, no new certificate is created and the existing one is used.

  Conditions: This symptom is observed in the following cases:

  – If the certificate server is created using an issuer or subject name when another trustpoint already exists with that same issuer or subject name.

  – If you try to authenticate a CA certificate with issuer or subject name same as that of any certificate that already exists.

  Workaround: Use different issuer-name for different trustpoints.

- CSCud01385

  Symptom: Continuous tracebacks is seen at nhrp_ipv6_mark_route

Conditions: This symptom is observed when traceback is seen at nhrp_ipv6_mark_route when "**no ipv6 unicast-routing**" command is issued on the hub while sending traffic from spoke to spoke.

Workaround: Do not issue **no ipv6 unicast-routing** command while sending traffic

- CSCud29930

  Symptom: An ASR1002-X Built-in SPA may record runts on its Gigabit Ethernet interfaces when using a SFP-GE-T (copper). This is not seen with an SFP-GE-S (fiber).

  Conditions: This symptom is observed when any frame that requires Ethernet padding to be added to make it 64 bytes.

  Workaround: There is no workaround.

- CSCud33882

  Symptom: SIP phones not registering to SRST when number cli with wild card configured under voice register pool.

  Conditions: This symptom is observed when you configure number cli with wild card configuration under voice register pool. number 1 900....

  Workaround: Create separate pools for all the phones without wild cards.

- CSCud36343

  Symptom: SRTP packets sourced from gateway / conference bridge have SSRC=0. This may cause audio / one-way audio issues.

  - Scenario 1 Signalization: E1 <> GW <> MGCP <> CUCM <> SIP / SCCP <> IP Phone Media: E1 <> GW <> SRTP <> IP Phone SSRC=0 sent by GW SSRC !=0 sent by phone
  - Scenario 2 Signalization: IP Phone 1 <> CUCM <> SCCP <> GW (conf bridge) |------<> IP Phone 2 |------<> IP Phone 3 Media: IP Phone 1 <> SRTP <> GW (conf bridge) <> SRTP <> IP Phone 2 |------------ <> SRTP <> IP Phone 3 SSRC =0 sent by GW (conf bridge) SSRC !=0 sent by phones

  Conditions: This symptom is observed on IOS 15.2(4)M1 IOS 15.2(4)M2 SRTP enabled

  Workaround: Disable SRTP or downgrade IOS to 15.2(1)T3

- CSCud37099

  Symptoms: When SIP KPML digits are being received by SIP-GW, they are not consumed even though it is configured to consume those KPML digits. This is causing the remote end point to hear unwanted DTMF tones.

  Conditions: This symptom is observed when SIP-GW negotiates KPML and receives KPML digits from SIP side.

  Workaround: There is no workaround.

- CSCud41708

  Symptoms: In a scaled GETVPN environment with a large number of GM's each in their own group, executing **show crypto gdoi gm** or **show crypto gdoi gm acl** commands produce empty output or cause CPU Hog backtraces.

  Conditions: This symptom is observed when a large number of GM's each in their own group and the **show crypto gdoi gm** or **show crypto gdoi gm acl** command is executed.

  Workaround: There is no workaround.

- CSCud42938

  Symptom: After a clear cry session, sometimes ident SM remains at responder side.

Conditions: This symptom is observed when a clear crypto session multiple times, crypto map deletes but ident remains due to race condition between new connections also coming up. Since map is removed and ident remains, the new connections now never comes up

Workaround: Router reboot

- CSCud49843

  Symptom: During call transfer, after entering the transfer number ,instead of "Ringout" it is displayed as "Transfer" in SRST mode

  Conditions: This symptom is observed during call transfer.

  Workaround: There is no workaround.

- CSCud51791

  Symptoms: Memory leak is seen on the router related to CCSIP_SPI_CONTRO.

  Conditions: This symptom is observed in CME SIP phones with Presence in running-configuration.

  Workaround: There is no workaround.

- CSCud52658

  Symptom: IKEv1 CERTREQ payloads exchanged by initiator and responder both contain all trustpoints and trustpools. This enhancement request is for limiting the size of the CERTREQ payload by not sending trustpools.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCud58633

  Symptoms: The "initial-contact" configuration option not needed, as the behavior is already enabled.

  Conditions: This symptom is observed when you use IKEv2, along with Cisco IOS Release 15.2(4)M.

  Workaround: There is no workaround.

- CSCud59210

  Symptom: Caller ID does not work for Inbound calls using FXO

  Conditions: This symptom is observed in IOS version 15.x.

  Workaround: There is no workaround.

- CSCud60826

  Symptom: PSTN -- T1 PRI --- IOS Gateway -- SIP --- CUCM --- Agent IP Phones One-way audio may be observed between a PSTN caller and an Agent IP phone connected via a SIP IOS Gateway such as ISR-G2 routers. The "tx" counter in the IP leg of "show call active voice brief" command will stop incrementing. Example : 11E4 : 446 583400ms.1 (22:38:27.944 UTC Sun Dec 9 2012) 510 pid:5555 Originate 2222 connected dur 00:00:33 tx:1295/207200 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0 IP <ip-addr:port> SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:65/65/65ms g711ulaw TextRelay: off Transcoded: No media inactive detected:n media contrl rcvd:n/a timestamp:n/a long duration call detected:n long duration call duration:n/a timestamp:n/a

  Conditions: This problem was observed when the gateway received "a=sendonly" in the SDP answer during Re-invite based media re-negotiation to put the call on hold. The media direction was updated to sendrecv mode in the subsequent call resume but the Gateway never transmits any RTP audio packets.

Workaround: Set "Duplex Streaming Enabled" service parameter in CUCM to "True". This mitigates the problem since the "a=sendonly" media direction attribute is not sent during call hold.

- CSCud60977

  Symptom: CRL file is not deleted when CS server is unconfigured manually by **no crypto pki server <name>**

  Conditions: CS server should be run before sever is unconfigured. crypto pki server <name> no shut

  Workaround: Delete CRL file manually.

- CSCud61517

  Symptoms: CUBE crashes during a blind-transfer scenario and when "media preference IPv6" is configured.

  Conditions: This symptom is observed when "media preference IPv6" is configured but is not seen when "media preference IPv4" is configured.

  Workaround: Configure "media preference IPv4".

- CSCud62138

  Symptoms: DTMF path confirmation fails with "MidCall failure using invalid c=FQDN with PRACK"

  Conditions: This symptom is observed when a router loaded with c2900-universalk9-mz.SSA.153-1.8.T

  Workaround: There is no workaround.

- CSCud62864

  Symptoms: When the Mid-call Re-INVITE consumption feature is active, CUBE consumes Re-INVITE which should change the media state from "sendonly" to "sendrcv". This results in a one way or no way audio on the call.

  Conditions: This symptom is observed when the CUBE Mid-call Re-INVITE consumption feature is enabled.

  Workaround: There is no workaround.

- CSCud63146

  Symptoms: In a GETVPN scenario, the GM fails to install policies on reload. A crypto map is applied on ethernet 0/0 while the local address of the crypto map is configured with ethernet 0/1.1

  Conditions: This symptom is observed after a reload. The GM fails to install policies from the key server.

  Workaround: Remove the crypto map configuration on the interface and reapply.

- CSCud64870

  Symptom: DMVPN hub ASR1004 may crash after the fetching CRL from MS CRL server.

  Conditions: The crash occurs when there are 5 CDPs for the hub router to fetch the CRL. Since there are multiple CDPs, the hub router fetches the CRL in a parallel way, which leads to a crash under a timing issue.

  Workaround: Setting up one CDP instead of multiple CDPs will greatly reduce the timing condition that leads to the crash.

- CSCud65119

  Symptoms: A crash may occur while using GETVPN with fragmented IPv6 traffic.

Conditions: This symptom is observed when IPv6 IPsec is used. This issue is triggered by fragmented IPv6 packets.

Workaround: There is no workaround.

- CSCud66955

  Symptoms: SPA-2CHT3-CE-ATM is flapping with Nortel Passport due to the fast bouncing of up or down 10s, after the interface is brought up.

  Conditions: This symptom is observed in E3 and DS3 mode.

  Workaround: There is no workaround.

- CSCud67105

  Symptoms: Virtual-Access is not removed when "clear ip nhrp" or "clear crypto session" are issued or when spoke-spoke FlexVPN session is gone. This is seen only in case of FlexVPN.

- Conditions: This symptom is observed when CSCuc45115 is already in image.

  Workaround: There is no workaround.

- CSCud67653

  Symptom: ASR1001 (1RU) builtin 4x1GE spa MIB poll for entSensorStatus returns a value of 3 which is "nonoperational" when CLI sensor reports no reading.

  Conditions: This bug is specific to 1RU (ASR1001) builtin spa 4X1GE. This symptom is observed when no reading is seen from output of show hw-module subslot all sensors

  Workaround: Possibly filter entSensorStatus value within customer NMS application.

- CSCud67779

  Symptoms: One-way audio is observed when a call goes through BACD and comes over SIP trunk.

  Conditions: This symptom is observed when a call comes through SIP trunk and is connected to an agent phone via BACD during the third call xfer, along with the "headset auto-answer" configuration in the ephone.

  Workaround: Remove the "headset auto-answer" configuration in the ephone configuration.

- CSCud68178

  Symptoms: The Cisco ASR 1000 series router and Cisco ISR 4400 series hubs crash.

  Conditions: This symptom is observed when the physical and tunnel interface are flapping.

  Workaround: There is no workaround.

- CSCud69592

  Symptoms: The Call Progress Analysis (CPA) feature does not work. Though DSP is allocated and programmed for the CPA functionality, no CPA events are detected and reported.

  Conditions: The symptom is observed for those call flows, where media bridging occurs after 200 OK responses.

  Workaround: There is no workaround.

- CSCud70629

  Symptoms: Incremental memory leaks are seen at IPSec background proc.

  Conditions: This symptom is observed with "clear nhrp cache".

  Workaround: There is no workaround.

- CSCud75278

Symptom: ATM event trace is holding too many memory (about 16M Bytes) even if ATM feature is not enabled.

Conditions: This symptom is observed when router is active

Workaround: Change the event trace size manually to a small value.
infra-asr1001-4(config)#monitor event-trace platform atm size ? <1-1000000> Number of entries in trace

- CSCud78362

  Symptoms: GW starts to drop calls randomly if you increase simultaneous calls beyond 350.

  Conditions: This symptom is observed if 350 calls are connected on GW, some doing digit collection using Cisco ASR(MRCPv2) and some playing media. Increasing a few more calls triggers the issue of call drops and total calls stay at only 350.

  Workaround: There is no workaround.

- CSCud78578

  Symptom: RP crashes after FP switchover

  Conditions: This symptom is observed when FP(FP80) reload with qos configs and traffic flowing in the background

  Workaround: There is no workaround.

- CSCud78618

  Symptoms: Router crashes.

  Conditions: This symptom is observed when applying IVRF configuration on IKE profile.

  Workaround: There is no workaround.

- CSCud78649

  Symptoms: The following error message occurs when activating SBC: "SBC: SBC ^T^U^\V not configured"

  Conditions: This symptom is observed when you run the activate command just after the media-address ipv4 ... command, as shown below:

```
ASR-1001-CCN-7(config)#sbc test
ASR-1001-CCN-7(config-sbc)#sbe
ASR-1001-CCN-7(config-sbc-sbe)#media-address ipv4 1.20.0.2 vrf vrfa
ASR-1001-CCN-7(config-sbc-media-address)#activate SBC: SBC ^A^T not configured
```

  Workaround: Exit SBC first, then enter SBC again and then run the activate command.

- CSCud79391

  Symptom: AVC functionality (performance monitor and media-net) was missing from advipservices image. It was only present in adventerprise

  Conditions: When loading an advipservices image, AVC functionality could not be configured.

  Workaround: There is no workaround.

- CSCud83835

  Symptoms: An IPsec VPN tunnel fails to be established. The debug crypto ipsec command shows no output when attempting to bring up the tunnel.

  Conditions: This symptom is observed when all of the following conditions are met:

  – The crypto map is configured on a Virtual-Template interface.

  - This Virtual-Template interface is configured with "ip address negotiated".
  - The tunnel is initiated locally (in other words, if the tunnel is initiated by the peer, it comes up correctly).

  Workaround: Downgrade to Cisco IOS Release 15.2(2)T3 or earlier releases or always initiate the VPN tunnel from the peer.

- CSCud85342

  Symptom: IKE responder fails to accept phase 1 proposal with rsa-sig authentication with public RSA keys and no trustpoints configured

  Conditions: An authentication mechanism of rsa-sig is configured and rsa-encr cannot be used due to hardware/software limitations

  Workaround: Use rsa-encr if supported, otherwise switch to using actual certificates with trustpoint or pre-shared keys.

- CSCud86240

  Symptoms: The Cisco ASR 1000 ESP crashes (ucode core file created) when compressed packets are sent on a Multilink PPP interface using the Cisco IOS XE 3.5 Release and earlier Cisco ASR 1000 software images. On Cisco IOS XE 3.6 Release and later on Cisco ASR 1000 software images a crash does not occur, but routed traffic on configured interfaces are not forwarded. However, local traffic between the peer routers may still be forwarded. In all releases, routed traffic will be dropped on any other interfaces (for example, PPP, Multilink PPP, HDLC, and so on.) configured for this mode of compression.

  Conditions: This symptom is observed if the legacy IOS compression feature compress [mppc | stac | predictor] is configured on any interface (for example, PPP, Multilink PPP, HDLC, and so on.). If this feature is configured on a Multilink PPP interface then the ESP crash can be encountered if using an Cisco IOS XE 3.5 Release and an earlier Cisco ASR 1000 software image.

  Workaround: Remove the compress [mppc | stac | predictor] feature configuration from all interfaces as this functionality is not supported on the Cisco ASR 1000 router. The software fix associated with this bug report will be removing this configuration option from the Cisco ASR 1000 router.

- CSCud87915

  Symptom: EzVPN client cannot access the Internet over the VPN. Access to Hub internal resources works fine. The ZBF firewall on the Hub drops the encryptred ESP(udp) traffic from self to out containing reply from the host on the Internet.

  Log on the hub:

  ```
  *Dec 28 15:34:51.189: %FW-6-DROP_PKT: Dropping udp session 8.8.8.2:0 8.8.8.1:53000 on zone-pair self-out class class-default due to DROP action found in policy-map with ip ident 0 source IP and port is incorrect.
  ```

  Conditions: This symptom is observed when EzVPN client behind NAT and source port is PATed - is not udp 4500. EzVPN client reaching the Internet with u-turn on the Hub. Hub has ZBF policy from self to outside permitting VPN traffic. Hub has CEF enabled.

  Workaround: Remove the ZBF policy from self to outside.

- CSCud88483

  Symptom: In a GETVPN and IPsec redundant configuration combination, if you reload a secondary group member in the topology it will cause TEK registration of the group member to be lost once the router comes back up and the HSRP does a state transition to standby.

  Conditions: The symptom is observed with a GETVPN with IPsec redundancy configuration.

Workaround: Wait for the next rekey or issue clear crypto gdoi.

- CSCud92596

  Symptom: when send traffic with vlan2 tag between 2 ixia ports through ASR 1004 as below. After show controller, could found "input vlan errors" counter increases without any packet drops. We also found when show interface, the value of "input errors" counter under related interface is 0.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCud94313

  Symptoms: PKI_INV_SPI messages are seen on the console.

  Conditions: This symptom occurs in a FlexVPN setup where Virtual-template is configured and IPsec drops are seen.

  Workaround: There is no workaround.

- CSCud94623

  Symptom: Spurious Memory Traceback related to VXML module seen

  Conditions: This symptom is observed after IOS upgrade to pi21/15.3(2)T build 153-1.11.T

  Workaround: There is no workaround.

- CSCud95387

  Symptoms: Call transfer with Trombone and ANAT fails.

  Conditions: This symptom is observed when CUBE is configured with ANAT and Antitrombone, and during call transfer, the call fails due to wrong media negotiation.

  Workaround: Disable ANAT.

- CSCud96896

  Symptom: "x Calls in queue" status is not displayed on all agents in the hunt group.

  Conditions: This symptom is observed when a particular agent is logged out, then the subsequent agents (i.e in the order in which they are configured a list member) do not get the status update.

  Workaround: Have all the agents logged in.

- CSCud97548

  Symptom: ptime value not sent in INVITE when VCC has multiple codecs

  Conditions: There is no known condition.

  Workaround: use sip profile to add ptime on outgoing SDP

- CSCue00040

  Symptom: **term length** command not obeyed by **show voip rtp conn** command

  Conditions: show command

  Workaround: There is no workaround.

- CSCue00726

  Symptom: There is no functional impact to the system performance, warning messages will be seen only during initialization of the router and there are no security concerns on these units:

  ```
  *Dec 16 17:58:02.432: IOSXE_PLATFORM-3-WDC_INVALID_LENGTH WDC length can not be
  determined: 65535  *Dec 16 17:58:10.703: PLATFORM_SCC-1-AUTHENTICATION_FAIL Chassis
  authentication failed  *Dec 16 17:58:10.703:
  IOSXE_AUTHENTICATE-2-AUTHENTICATE_FAILED. The platform authentication failed
  ```

Conditions: Programming of Quack & WDC (Watch Dog Certificate) was accidentally disabled in manufacturing during the regression testing. This caused units to ship without Quack & WDC programming. These messages show up at boot up for these specific units that had the quack disabled

Workaround: There is no workaround.

- CSCue03940

  Symptom: When an invalid SPI packet is received, the receiving gateway is unable to identify correctly that the packet is dropped due to the reason of invalid SPI. Instead, it gave a wrong reason that it is a non-IPSEC packet.

  Conditions: Problem happen when a router running IPSEC/VPN is receiving an invalid SPI packet.

  Workaround: There is no workaround.

- CSCue05798

  Symptom: Need to backout due to hardware limitation

  Conditions: Fix not needed due to hardware limitation

  Workaround: There is no workaround.

- CSCue14418

  Symptom: Only single L2TP IPSEC vpn client can connect to vpn when they are behind PAT device even though NAT DEMUX is configured.

  Conditions: This symptom is observed when VPN clients behind PAT device

  Workaround: There is no workaround.

- CSCue14586

  Symptom: After reload system may not be able bring up all ipsec tunnels at high scale (1k) group members.

  Conditions: This symptom is observed when ASR1K with GETVPN, 1k group members.

  Workaround: Issue a clear **clear crypto gdoi** to force re-registration and rebuild of tunnels.

- CSCue17371

  Symptom: NTE cannot passthrough

  Conditions: This symptom is observed during call transcoding.

  Workaround: There is no workaround.

- CSCue25575

  Symptoms : The crash is observed for SDP pass through or call forward or antitrombone cases.

  Conditions: This symptom is observed when a basic call involving SDP pass through or call forward or antitrombone cases.

  Workaround: There no workaround.

- CSCue32707

  Symptoms: "crypto pki export" in PKCS12 format may lead to router crash.

  Conditions: This symptom is observed in Cisco IOS Release 15.2(4)M2.

  Workaround: There is no workaround.

- CSCue33313

  Symptom: A Cisco ASR repeatedly produces a "no-input" event despite inputs provided by caller.

Conditions: This symptom is observed when IOS VXML GW running Cisco IOS Release 15.x. - Problem seems to be triggered by a "no-match' event prior to providing expected responses.

Debugs show the following order of events:

1. GW instructs TTS server to say "please say yes or no, or press digits 1 or two".

2. GW instructs ASR to recognize.

3. Customer says "one two three four" and the GW forwards this audio to the ASR.

4. ASR instructs GW "no-match".

5. GW instructs TTS server to say "no match event received please try again".

6. GW instructs ASR to recognize.

7. Customer says "yes", but the GW does not forward the RTP containing "yes" to the ASR server.

8. GW receives "no-input" event from ASR as a result of no RTP containing speech being sent to ASR.

9. GW instructs TTS server to say "no input event received please try again".

Steps 6 through 9 repeat until the customer hangs up the call.

Workaround: There is no workaround.

- CSCue34828

  Incorrect Incoming CLID through FXO port

  Symptom: Incorrect Incoming CLID through FXO port

  Conditions: `Jan 29 09:25:57.311: [0/0/1] Caller ID String 04 12 B0 31 32 B9 31 B0 32 34 20 B9 32 B3 B5 B3 38 B6 32 B5 DC Jan 29 09:25:57.311: [0/0/1] get_fxo_caller_id calling num=282 calling name= calling time=01/157 138:24 Jan 29 09:25:57.311: fxols_callerid_done: call being answered Expected -923 53 86 25 Received ? 282`

  Workaround: There is no workaround.

- CSCue35533

  Symptoms: Ping fails with security applied and IKE disabled.

  Conditions: This symptom is observed when the Cisco IOS Release 15.3(1.15)T image is loaded.

  Workaround: There is no workaround.

- CSCue36387

  Symptom: When IPv6 crypto is applied, the inbound interface counters associated with the crypto configuration are not updated correctly. There is no problem with the functionality but the counters are wrong

  Conditions: This symptom is observed when interface input counters using IPv6 crypto

  Workaround: There is no workaround.

- CSCue37000

  Symptom: GTP-U drops for communication that should not have been dropped. Swisscom agrees that this might be related to some timers and pending PDP sessions that need to be terminated. Since local tests with mobile devices were all successful, Swisscom wants and needs to go for 24 h test to see if the GTP-U drops really lead to a service impact for mobile users. To document this issue, a SR was opened: SR 624629207 ASR1K Release 3.7.2 -GTP U drops due to missing pinholes All log files and a PCAP file are attached to that SR.

  Conditions: There is no known condition.

Workaround: There is no workaround.

- CSCue37523

  Symptom: When IOS is a IPSEC QM (Quick Mode) responder for ipsec , and if it receives QM1 packet from Call Manager with missing ID payload, the packet is processed, but QM2 packet is not sent out to the Call Manager. It works fine when IOS is a initiator of QM.

  Conditions: This symptom is observed when IOS Responder to QM from call manager call manager doesn't send ID payload in transport mode in QM1.

  Workaround:

  1. Initiate traffic from IOS router so that IOS is a QM initiator.

  2. Change config of racoon client on call manager to send ID payload in QM1 as initiator. (support_proxy on)

- CSCue38057

  Symptom: OSPFv3 neighbor and IPSEC SA was not UP

  Conditions: This symptom is observed in 153-03S version OSPF neigbor and SA was down

  Workaround: included the IPV6 family for proxy

- CSCue39206

  Symptoms: ES crashes after the second 401 challenge.

  Conditions: This symptom is observed when the second 401 is received after SDP offer/answer with 183/PRACK is complete. This is a rare scenario.

  Workaround: There is no workaround.

- CSCue41031

  Symptoms: Exta IPsec flow is shown in the "show crypto session" output.

  Conditions: This symptom is observed with the Cisco ASR 1000 RP1 FlexVPN Client.

  Workaround: There is no workaround.

- CSCue43895

  Symptom: "show crypto gdoi gm dataplane counters" or "show crypto gdoi gm replay" shows negative and/or very large counters.

  Conditions: This symptom is observed when "clear crypto sa counters" is issued after "clear crypto gdoi dataplane counters" and/or "clear crypto gdoi replay counter" for a GETVPN / GDOI Group Member (GM) running IOS version 15.3(2)S/T or later with the "show crypto gdoi feature long-sa-lifetime" available.

  Workaround: Do not issue both "clear crypto gdoi dataplane counters" / "clear crypto gdoi replay counter" and "clear crypto sa counters" & if counters go negative or become very large, issue "clear crypto gdoi" to reset the Group Member (GM) (NOTE: GM will remove IPsec SA's and re-register, causing some traffic drop).

- CSCue44587

  Symptom: After the L2L tunnel has been up for some time, the route created by RRI will be removed from the ASR routing table, even though there is still a valid IPSec SA built for the destination subnet.

  Conditions: This symptom is observed when ASR configured with L2L tunnel to ASA, and RRI is enabled.

  Workaround: Configure a static route for the destination subnet on the ASR.

- CSCue46537

  Symptom: Whenever we clear the counters using "clear counters" it just happened to clear ONLY interface counters. Controllers counters NEVER GET CLEARED unless we do the reboot. In this case controller is SPA-2XT3/E3

  Conditions: This symptom is observed only on ASR1k

  Workaround: Reboot the router.

- CSCue48243

  Symptom: Undefined event displayed instead of an event related to registration.

  Conditions: This symptom is observed when show monitor event gdoi registration all CLI is executed.

  Workaround: There is no workaround.

- CSCue49575

  Symptom: MOH stops working intermittently

  Conditions: This symptom is observed when PARK softkey is pressed on phone and when a subsequent call is received on this phone and this call is placed on hold.

  Workaround: There are several workarounds like - placing a new call from this phone, Going off hook, receiving a new call on this phone etc..

- CSCue50484

  Symptom: Crypto Tunnel Socket remains OPEN after shutting the tunnel interface

  Conditions: This symptom is observed when Dual-DmVPN with ike-profile on the tunnel interface.

  Workaround: There is no workaround.

- CSCue51375

  Symptom: The dynamic monitor is populated with incorrect records and the performance monitor cache incorrectly includes encapsulated traffic.

  Conditions: This symptom is observed when GRE tunnel output interface is configured with a performance monitor on an ASR1000 series router, and the output physical interface from which the packets are transmitted is configured with a native FNF monitor.

  Workaround: There is no workaround.

- CSCue51886

  Symptoms: The SBC CUBE device rejects call connections.

  Conditions: This symptom is observed when the Chunkmanager holds a lot of memory and calls do not get processed.

  Workaround: Reloading the box helps to make the box stable.

- CSCue52845

  Symptom: If the peer does not respond to the R-U-THERE, IOS routers should retransmit it 5 times. However, DPD is retried 6 times.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCue52963

  Symptom: Some of the SPA goes "inserted (physical)" state after an ISSU upgrade. This issue is not specific to any particular SPA or SIP.

Conditions: This symptom is observed when an ISSU upgrade on a setup that has a high scale configuration. Altleast 2000 subinterfaces are configured in the router.

Workaround: This issue is not seen in the following scenario:

1) Before doing a load version from RP0(initial active), enter the following command: asr1000# show ipv6 route table | inc IPv6

2) Note down the number of IPv6 route tables in the system.

3) Do a load version.

4) Wait for standby to come up to Standby hot.

5) Enable the standby console from RP0 (active). asr1000#configure terminal Enter configuration commands, one per line. End with CNTL/Z. asr1000(config)# asr1000(config)#redundancy asr1000(config-red)#main-cpu asr1000(config-r-mc)#standby console enable

6) Log in to the standby console and enter the following command: asr1000-stby# show ipv6 route table | inc IPv6 Then, note down the number of IPv6 route tables in standby. If the number is lesser than the number noted in step 2, wait for some time and reverify till it reaches the number noted in step 2.

7) Issue ISSU runversion from RP0(active).

- CSCue53207

  Symptom: A record that contains certain derived fields (listed below) may be punted incorrectly to the route processor (RP) and lost.

  Conditions: This symptom is observed when Records can collect ?derived? fields; calculating derived fields is dependent on the values of other fields. The fields listed below are incorrectly defined as derived and dependent on other fields. When a record contains one of these fields and does not include its dependent fields, the record is punted to the route processor (RP) to complete the record processing. Punting these records might lead to record loss.

  Workaround: When configuring a monitor to collect one of the fields listed below, collect each of the dependent fields also. The list indicates the dependencies:

  1. 'connection delay application sum' is dependent on: connection delay response to-server sum connection delay network to-server sum connection server response sum

  2. 'connection delay application min' is dependent on: connection delay response to-server min connection delay network to-server sum

  3. 'connection delay application max' is dependent on: connection delay response to-server max connection delay network to-server sum

  4. 'connection delay response client-to-server sum' is dependent on: connection delay response to-server sum connection delay network to-server sum connection server response sum

  5.'connection delay response client-to-server min' is dependent on: connection delay response to-server min connection delay network to-server sum connection server response sum connection delay response to-server sum connection delay network to-server min

  6. 'connection delay response client-to-server max' is dependent on: connection delay response to-server max connection delay network to-server sum connection server response sum connection delay response to-server sum connection delay network to-server max

- CSCue59967

  Symptom: VPN led does not come up when an IKEv2 tunnel is active

  Conditions: This symptom is observed when IKEv1 is not affected only IKEv2.

  Workaround: There is no workaround.

- CSCue59994

  Symptom: Enrollment fails for trustpoints configured to use elliptic curve keys and a hash of sha384 or sha512.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCue61481

  Symptom: Show invntory doesnt show inventory info after hard online insertion and removal (OIR)

  Conditions: This symptom is observed after a hard OIR is performed.

  Workaround: There is no workaround.

- CSCue63742

  Symptom: Tracebacks are seen in a basic call scenario

  Conditions: This symptom is observed when CTI is enabled. CTI call flow.

  Workaround: Do not configure CTI (allow watch) in ephone-dn

- CSCue63807

  Symptom: SIP call during "Call Forward No Answer" option leaks the Transcoder resource used on CUBE Example call flow:

  ```
  Telco -> SIP Trunk (G711alaw/G729) -> CME -> SIP phone (G711ulaw) ->NOAN ->  CUE
  (G711ulaw)
  ```

  Conditions: This symptom is observed when SIP Call Codec mis-match between two legs of the call and invokes the local transcoder resource. Call forward No Answer (noan) feature

  Workaround: Reset the sccp session. #no sccp #sccp

- CSCue64455

  Symptom: RP crashes when configure debug condition on atm interface .

  Conditions: This symptom is observed when:

  1. debug plat condition inter atm0/1/1 vcd 0 when ATM SPA type is SPA-2CHT3-CE-ATM

  2.debug plat condition inte gi0/0/1 vcd 0 or debug plat condition inte gi0/0/1 vpi 1 or debug plat condition inte gi0/0/1 portvc

  Workaround:

  1.when interface is not atm type, not allow user config vcd ,vpi and portvc parameters to avoid the issue.

  2.Modify the NULL pointer access code when ATM SPA type is SPA-2CHT3-CE-ATM

- CSCue65405

  Symptom: SAs do not get installed in GETVPN GM.

  Conditions: The symptom is observed when the key server is configured with "receive-only" SAs.

  Workaround: Remove receive-only configuration at the key server.

- CSCue71410

  Symptom: Console corruption is seen sometimes when punt keepalive packet drop happens during bootup of router.

  Conditions: This symptom is observed when first punt keepalive packet is dropped and other console activity is going on at the same time.

Workaround: Punt keepalive messages can be disabled in the config, but it's not a recommended setting as it can mask punt failures.

- CSCue75022

  Symptoms: IPsec SAs are not getting deleted even after removing the ACL.

  Conditions: This symptom is observed with IPSec SAs.

  Workaround: There is no workaround.

- CSCue75072

  Symptom: Consult transfer with "remote optional-mandatory strength" fails as SDP precondition doesn't match.

  Conditions: This symptom is observed when consult transfer but not for blind transfer.

  Workaround: There is no workaround.

- CSCue77265

  Symptoms: Increment memory leaks are seen at IPSec background proc.

  Conditions: This symptom is observed when "clear cry session" is issued multiple times when bringing up the tunnel.

  Workaround: There is no workaround.

- CSCue80506

  Symptom: Traceback at DMVPN Spoke registration, DMVPN QoS policy not deployed to datapath component.

  Conditions: This symptom is observed when there is a routing issue such that the ASR1k acting as the DMVPN hub can receive spoke registrations but does not have a valid route to the spoke (i.e. the spoke's forwarding interface is Null0) and the spoke's QoS configuration include a queuing feature, then the QoS policy will fail to get applied and the ESP will be in a state that requires it to be reloaded to recover from this.

  Workaround: There is no workaround, but the following actions can get the router operational again.
  1. Correct routing issue and reload the ESP and/or

  2. Remove the QoS queuing feature and reload the ESP

- CSCue85737

  Symptoms: ASR with PKI certificate may crash when issuing show crypto pki certificate command.

  Conditions: This symptom is observed when the show crypto pki certificate command is issued on ASR with PKI certificate.

  Workaround: There is no workaround.

- CSCue87185

  Symptoms: The DF flag message is not received with "crypto ipsec df-bit copy".

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(2.3)T image.

  Workaround: There is no workaround.

- CSCue87438

  Symptom: The Conference List button is not working with CME registered phones when using the Spanish locale file. When the conference list soft key is pushed, nothing is seen. XML Parse Error is shown

  Conditions: This symptom is observed when Spanish locale is configured .

Workaround: There is no workaround.

- CSCue88077

  Symptom: Router reloads with traceback pointing to voip_rtcp_session.

  Conditions: This symptom is observed when SIP-H323 calls at 50 CPS in CUBE(Ent) configuration.

  Workaround: There is no workaround.

- CSCue88591

  Symptom: DSP error message printed on console, and crash takes place

  Conditions: This symptom is observed when DSP firmware (version:33.1.00) sends corrupted DSP error message to RP IOS which leads to crash: %SPA_DSPRM-3-DSPALARM: Received alarm indication from dsp (1/0/9). %SPA_DSPRM-3-DSPALARMINFO: 0008 0000 0080 0000 0000 0001 7F3B FEDF %SPA_DSPRM-3-DSPALARMINFO: -;???? %DSP-3-DSP_ALARM: SIP1/0: DSP device 2 is not responding. Trying to recover DSP device by reloading

  Workaround: Downgrade to XE36 which firmware version is 31.1.0

- CSCue89491

  Symptom: GM tries to Re register after the rekey mechanism change

  Conditions: This symptom is observed when the user change rekey transport type and wait for the schedule to take place. GM will fail to process the rekey and re-register.

  Workaround: After change rekey transport type, issue "crypto gdoi ks rekey" to send the rekey instead of wait for schedule rekey

- CSCue92951

  Symptom: Sh mem debug leak chunk shows memory leak for voiprtp-GCFM-CONTEXT.

  Conditions: This symptom is observed when call filter debug is enabled

  Workaround: Do not enable call filter debug

- CSCue93140

  Symptom: Session not coming up

  Conditions: This symptom is observed when invalid ke payload or cookie is received

  Workaround: There is no workaround.

- CSCue93355

  Symptom: GM fails to register with keyserver.

  Conditions: The symptom is observed when SGT tagging is enabled.

  Workaround: There is no workaround.

- CSCue94610

  Symptoms: DSP crash with the following console error:

  ```
  %SPA_DSPRM-3-DSPALARMINFO: Checksum Failure:80000000,0000000e,d0156a80,d0156000 *Mar
  14 17:56:05.851: %SPA_DSPRM-3-DSPALARM: Received alarm indication from dsp (1/3/6).
  %SPA_DSPRM-3-DSPALARMINFO: 0042 0000 0080 0000 0000 0000 4368 6563 6B73 756D 2046 6169
  6C75 7265 3A38 3030 3030 3030 302C 3030 3030 3030 3065 2C64 3031 3536 6138 302C 6430
  3135 3630 3030 0000 0000 0000 0000 0000
  ```

  Conditions: This symptom is observed when an RP switchover process. The standby RP presents DSPs failing to come up.

  Workaround: This command may clear up the DSPs:

```
Router# hw-module subslot x/y reload... Symptom:  DSP crash with the following console
error

*Mar 14 17:56:05.851: %SPA_DSPRM-3-DSPALARMINFO: Checksum
Failure:80000000,0000000e,d0156a80,d0156000

*Mar 14 17:56:05.851: %SPA_DSPRM-3-DSPALARM: Received alarm indication from dsp
(1/3/6).

*Mar 14 17:56:05.851: %SPA_DSPRM-3-DSPALARMINFO: 0042 0000 0080 0000 0000 0000 4368
6563 6B73 756D 2046 6169 6C75 7265 3A38 3030 3030 3030 302C 3030 3030 3030 3065 2C64
3031 3536 6138 302C 6430 3135 3630 3030 0000 0000 0000 0000 0000
```

- CSCue95176

  Symptom: SIP KPML DTMF not recognized after call transfer from Unity to UCCX. CUBE rejects the subscription with a "SIP/2.0 500 Internal Server Error"

  Conditions: This symptom is observed when SIP-SIP CUBE running IOS 15.2.4M2. Call is sent to Unity, caller presses a digit and gets transfer to UCCX, while caller is in queue, they press digit '1' and it should be transferred back to Unity but digit is not recognized and caller remains in queue. Issue was also observed with IOS 15.1(4)M4.

  Workaround: Change DTMF relay method to rtp-nte in the dial-peers and set the RFC2833 DTMF Method in CUCM SIP Trunk Configuration page.

- CSCue95276

  Symptom: Customer reports unstable behavior observed from "show ephone-hunt 1 statistics" command output.

  There are following behaviors:

  Some CME routers used to collect statistics and display them in the show command, but suddenly stops displaying even if router is rebooted

  Some CME routers never were able to display statistics but suddenly start working

  One CME router wasn't able to display statistics but a few days after a reboot, starts working

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCue97986

  Symptom: Calls hang at SIP, CCAPI and VOIP RTP components (but are cleared in the dataplane of the Cisco ASR 1000 series platform).

  Conditions: This symptom occurs when a video call is setup as an audio call. The call then gets transferred with REFER but the caller hangs up the call before the call gets transferred. This is an intermittent problem.

  Workaround: If there is an SIP call dangling (sh sip call sum), then use the clear cal voice cause code 16 command to clear the dangling call.

- CSCuf01088

  Symptoms: Memory leaks are observed with a Cisco ASR router with CVP call flows.

  Conditions: The symptom is observed under load conditions. Memory leaks are seen in Cisco IOS XE 3.8.

  Workaround: There is no workaround.

- CSCuf04726

  Symptom: IPsec(crypto-map mode) configured, manually disable VFR, after reload, the "no ip virtual-reassembly-out" CLI is lost, VFR is re-enabled.

Conditions: The symptom is observed under the following conditions:

1)apply crypto map on the interface

2)manually disable vfr "no ip virual-reassembly-out"

3)save config

4)reload after reload The "no ip virual-reassembly-out" is lost, VFR is re-enabled

Workaround: After reload, manually disable vfr "no ip virual-reassembly-out"

- CSCuf09938

  Symptom: LSC installation fails if the RSA Key pair size associated with CAPF server is larger than 512 Bytes.

  Conditions: The symptom is observed in secure CME implementation. Sample config:

  ```
  ! crypto pki trustpoint capf  enrollment url http://<ip-addr>:<port-num>
  serial-number  revocation-check none  rsakeypair capf 1024 1024  ! capf-server
  auth-mode null-string  cert-enroll-trustpoint <trust-point>  trustpoint-label capf
  source-addr <ip-addr> !
  ```

  Workaround: Use 512 Bytes RSA key size crypto pki trustpoint capf enrollment url http://<ip-addr>:<port-num> serial-number revocation-check none rsakeypair capf 512 512

- CSCuf15260

  Symptoms: A Cisco ASR router crashes while sending notify with KPML digit.

  Conditions: The symptom is observed on a Cisco ASR router. It is seen when the DTMF type is changing to SIP-KPML midcall.

  Workaround: Do not change DTMF type mid-call.

- CSCuf20108

  Symptom: Using MRCPv2 on VXML GW for CVP calls to 3rd party ASR, we have found the MRCP Client process is disappearing after a few hundred calls. This causes all future calls to fail until the VXML GW is rebooted. A traceback is thrown in the logs at this time, indicating a memory problem.

  ```
  Feb 28 00:23:23.949 JST: %SYS-2-FREEBAD: Attempted to free memory at B0D0B0D, not part
  of buffer pool -Traceback= 18B57F4z 2C60B0Cz 5B120B3z 4BCA9F6z 2BCCA09z 4C7692Ez
  4BCAA8Bz 4C8D03Fz 4C8EE4Bz 4C85EF2z 4C85D2Fz 4C75A21z
  ```

  Running 'show process' after this traceback shows the MRCP Client process is no longer running.

  Conditions: The symptom is observed when a Nuance server abnormally tears down MRCPv2 session in the middle of the call. MRCPv2 is needed to trigger the crash. MRCPv1 does not cause a crash.

  Workaround:

  1) Set all sessionTimeout configurations to -1 on the Nuance server (In the NSSserver.cfg file).

  2) Use MRCPv1 instead of MRCPv2

- CSCuf20409

  Symptom: Netsync:Customer seeing clock in ql-failed state on one ASR-2ru

  Conditions: The symptom is observed when distributing stratum 1 clock source through its network.

  Workaround: There is no workaround.

- CSCuf21465

Symptom: GETVPN Group Members (GM) registration window starts at 3%-5% of the remaining TEK lifetime, rather than at 5%-7%, as documented. This can lead to TEK expiry on some GMs in situations when the registration process is slow.

Conditions: The symptom is observed on Cisco ASR running IOS XE 3.7, IOS 15.2S

Workaround: Extend TEK lifetime (and accordingly the corresponding registration window) to avoid traffic drops due to TEK expiration.

- CSCuf21611

  Symptom: TDM voice call gets terminated due to voice-port shutdown when T1/E1 module on other NIM slot is reloaded (OIR).

  Conditions: The symptom is observed when an OIR of T1/E1 module in any NIM slot shuts down the voice-ports (if any) on all other T1/E1 NIM slots.

  Workaround: There is no workaround.

- CSCuf35314

  Symptom: Operation relying on PKI may start failing when enrolling a new trustpoint to same CA as already existing trustpoint.

  Conditions: The symptom is observed with Cisco IOS 15.2(4)M1.

  Workaround: Run the crypto key zeroize pubkey-chain command.

- CSCuf39344

  Symptom: In SBC-B2B, after "no attach/attach" an adjacency, calls rejected with 503 Service Unavailable.

  Conditions: The symptom is observed when:

  1. config vrf001 on BOX1(ACTIVE) then on BOX2(STANDBY)

  2. config adjacency's vrf&signaling-address and "media-address ... vrf ..." both refer to vrf001

  3. switch-over

  4. no attach/attach adjacency on BOX2(ACTIVE)

  5. later calls rejected with 503 Service Unavailable

  Workaround: Always add or change vrf related SBC config on the same box.

- CSCuf43548

  Symptoms: When the POS Rx fiber at the tail end of the MPLS TE FRR is pulled, the FRR takes longer than 200ms to cut over to the other tunnel.

  Conditions: This symptom occurs with POS MPLS TE FRR when the head end receives a remote defect due to the Rx fiber pull at the tail end. Remote defects do not trigger FRR quickly.

  Workaround: There is no workaround.

- CSCuf45420

  Symptom: CPA not detected for outbound call flow

  Conditions: The symptom is observed with Pi22 image

  Workaround: There is no workaround.

- CSCuf49959

  Symptom: A router may crash when the tunnel interface is flapped or while booting the router with VPN configs

Conditions: The crash occurs in a VPN enabled scenario with either sessions being active and a shut/no shut is issued on the interface or the sessions coming up on the box after a reload.

Workaround: There is no workaround.

- CSCuf51515

  Symptom: Memory leaks are seen in ASR1k 1RU Platforms after booting up with the test image with default configurations on the router. Refer steps to reproduce

  Conditions: Config and swversion are attached.

  Workaround: No functionality is affected.

- CSCuf51539

  Symptom: In some rare situations, EzVPN client routers are seen to have an IKEv1 SA lifetime beyond 24 hours - up to "3 weeks, 3 days". This can lead to unpredictable behavior during IKEv1 phase1 renegotiation, notably this can cause the server to initiate a negotiation which would result in errors and interruptions of service over the VPN.

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuf51801

  Symptom: show crypto session xxx command results in memory leaks.

  Conditions: This symptom is observed when the **show crypto** command is run that causes168-byte memory leak for the following commands:

  - **show crypto session brief - show crypto session local <IP> brief**
  - **show crypto session local <Mac> brief**
  - **show crypto session remote <Mac> brief**
  - **show crypto session remote <Mac> brief**
  - **show crypto session username <any> brief**
  - **show crypto tech-support peer <IP>**
  - **show crypto tech-support**

  Workaround: There is no workaround.

- CSCuf61640

  Symptom: Tracebacks as follows seen during router bootup:

  ```
  %SYS-2-INTSCHED: 'suspend' at level 2 -Process= "Init",  ipl= 2, pid= 3  -Traceback=
  4F6966C 6A708EC 890127C 6B4F924 6B4F7F8 6B4EAAC 6B4F43C 6B4F514  6DD6D4C 6DDB3A8
  6A23E50 6A23F18 6A24100 57D3F94 57D42D8 4F701E4  0x4F6966C  --->
  process_ok_to_reschedule 288 0x6A708EC  ---> process_suspend 4C 0x890127C  --->
  random_fill 248 0x6B4F924  ---> default_entropy_routine 9C 0x6B4F7F8  --->
  hardware_entropy_source CC 0x6B4EAAC  ---> nist_instantiate 78 0x6B4F43C  --->
  try_create_rng 1B4 0x6B4F514  ---> nist_rng 34 0x6DD6D4C  ---> cts_sap_get_key_counter
  54 0x6DDB3A8  ---> cts_sap_init C4 0x6A23E50  ---> subsys_init_routine 60 0x6A23F18
  ---> subsys_init_class_internal A8 0x6A24100  ---> subsys_init_class 8C 0x57D3F94
  ---> system_init 250 0x57D42D8  ---> init_process 94 0x4F701E4  --->
  ppc_process_dispatch
  ```

  Conditions: The symptom is observed during router bootup.

  Workaround: There is no workaround.

- CSCuf65404

  Symptom: Call is failing if transcoder is needed for DTMF interworking and offer-all is configured.

  Conditions: The symptom is observed when CUBE reserves transcoder for codec mismatch and release the transcoder since codec are same, but DTMF still requires transcoder for interworking.

  Workaround: There is no workaround.

- CSCuf65502

  Symptom: Sessions are not cleared.

  Conditions: When there is no media, and a media inactivity timeout is received, sessions are not cleared.

  Workaround: There is no workaround.

- CSCuf65843

  Symptom: On code analysis it was found that the code in crypto_cef.c:crypto_tun_post_decrypt_switch() calls oce_les_inline() in an unsafe manner.

  Conditions: On code analysis it was found that the code in crypto_cef.c:crypto_tun_post_decrypt_switch() calls oce_les_inline() in an unsafe manner which could lead to potential issues

  Workaround: There is no workaround.

- CSCuf82550

  Symptom: Router displays malloc failure error message.

  Conditions: The symptom is observed when the router is running IPsec.

  Workaround: There is no workaround.

- CSCuf85449

  Symptom: Crash @ be_ewag_gtp_path_pdp_remove_one during session churns.

  Conditions: 48K EoGRE sessions of mix GTP (18K) PMIP (18K) and SIP (12K). During session churning, GTP crash is observed.

  Workaround: There is no workaround.

- CSCuf89642

  Symptom: Crash is seen for H.323-SIP transcoding calls.

  Conditions: This symptom is observed when transcoder is invoked.

  Workaround: There is no workaround.

- CSCuf93376

  Symptom: CUBE reloads while testing SDP passthrough with v6.

  Conditions: The symptom is observed while testing SDP passthrough with v6.

  Workaround: There is no workaround.

- CSCuf93395

  Symptom: Traceback observed in HUB on fp reload

  Conditions: QoS does not get applied in hardware when traceback occurs. This occurs when QoS is applied to a spoke's tunnel on the DMVPN hub following the flapping of a spoke's tunnel.

  Workaround: Reload the ESP.

- CSCuf93460

Symptom: Certain PKI CLIs may show wrong values.

Conditions: First found on IOS 15.1(4)M6 but not exclusive to it.

Workaround: There is no workaround.

- CSCuf96673

  Symptom: Memory leaks seen with Smap-Dmap scale scenario. 4K sessions

  Conditions: Leaks seen after stress testing : rekey , dpd, clear commands.

  Workaround: There is no workaround to prevent memory leaks.

- CSCug09761

  Symptom: Handshake fails when we select Diffie Hellman cipher suite from sslvpn configuration.

  Conditions: There is no known condition.

  Workaround: Select other than Diffie Hellman cipher suite at sslvpn.

- CSCug11220

  Symptom: GETVPN IPv6 packets get dropped.

  Conditions: The symptom is observed whenever an IPv6 GETVPN group is configured.

  Workaround: There is no workaround.

- CSCug11577

  Symptom: Traceback is found during HW crypto engine using Dummy packet.

  Conditions: The symptom is observed when Hardware crypto is used.

  Workaround: Use software crypto.

- CSCug12136

  Symptom: On an ASR1K the "clock timezone" command is meant to be used as follows: clock timezone zone hours-offset [minutes-offset] where "zone" is a text field e.g. "EDT", "PST", and hours-offset and minutes-offset are integers. If the hours-offset field is set to 0 (which can occur either intentionally or in some cases due to a typo) some of the ASR1K internal timers may be misconfigured which could lead to incorrect operations related to system time.

  Conditions: One way to cause this to happen (essentially a typo) is to configure clock timezone EST-5 0 0 where one really meant to type clock timezone EST -5 0

  Workaround: If 0 is the intended offset it's probably best to simply remove the config line entirely. If 0 is not intended then correcting the typo will correct the issue.

- CSCug14423

  Symptom: A packet gets dropped when a spoke-spoke session is triggered in Dynamic Multipoint VPN (DMVPN).

  Conditions: This symptom occurs when a ping is sent using a tunnel interface as the source or the destination.

  Workaround: Send traffic from host-host.

- CSCug17289

  Symptom: DMVPN hub crashed.

  Conditions: The symptom is observed when reset to the crypto session.

  Workaround: There is no workaround.

- CSCug18233

Symptom: Using local ikev2 authorisation policy, it is not possible to push prefix along with the ip address to the client. the prefix always gets pushed as 128

Conditions: The symptom is observed when ikev2 local authorisation is used.

Workaround: Use radius server to push the prefix to the client

- CSCug18326

  Symptom: A router reload is observed .

  Conditions: This symptom is observed when acknowledge for initial invite is not seen .

  Workaround: There is no workaround.

- CSCug18685

  Symptom: An NHRP resolution request is forwarded to the first NHS on the tunnel interface instead of being forwarded along the routed path

  Conditions: The symptom is observed during DMVPN phase 3 implementation

  Workaround: There is no workaround.

- CSCug22238

  Symptom: Fields from a refer are not sent out on the corresponding INVITE when this is a SIP GW

  Conditions: The symptom is observed on 15.1.4M6

  Workaround: There is no workaround.

- CSCug28904

  Symptoms: Router drops ESP packets with CRYPTO-4-RECVD_PKT_MAC_ERR.

  Conditions: The symptom is observed when the peer router sends nonce with length 256 bytes.

  Workaround: There is no workaround.

- CSCug30286

  Symptom Memory leak may occur when "Hold" is pressed on a registered SCCP phone in a call with a PSTN/TDM peer.

  Condition A registered SCCP phone puts a PSTN/TDM leg on hold.

  Workaround There is no known workaround.

- CSCug34404

  Symptom: RP_Crash seen @ __be_interface_action_remove_old_sadb

  Conditions: While unconfiguring the 4K svti sessions after the HA-test

  Workaround: There is no workaround.

- CSCug34677

  Symptom: Upon failing link asr1k-D1 (laser shut on Agilent, equivalent to pulling fiber), FRR is not triggered and traffic flow is restored when ISIS reconverges.

  Conditions: The symptom is observed in IP network and when FRR is enabled and when ethernet interface is one of the primary path and protected path and when plugging out ethernet wire or remote shutdown.

  Workaround: There is no workaround.

- CSCug37242

  Symptoms: Router crash due to memory leak.

Conditions: The symptom is observed with a CME shared line feature configuration.

Workaround: Disabling shared line feature will avoid memory leak.

- CSCug38641

  Symptom: Ingress IPSec data packets are process switched on an EzVPN server

  Conditions: cTCP encapsulation is configured

  Workaround: Use UDP encapsulation

- CSCug44197

  Symptom: Only a subset of voice-port commands are supported for bulk config. Command help '?' incorrectly shows "vmwi" as a supported argument: Voice-port configuration commands:

```
vg350#<i>conf t</i>
Enter configuration commands, one per line.  End with CNTL/Z.
vg350(config)#<i>voice-port 2/0/0-71</i>
vg350(config-voiceport)#<i>?</i>
  battery-reversal  Enable FXS battery-reversal generation
  busyout           Configure busyout trigger event & procedure
  cable-detect      enable cable detection
  caller-id         Configure port caller id parameters
  default           Set a command to its defaults
  description       Description of what this port is connected to
  disconnect-ack    FXS sending disconnect acknowledge
  exit              Exit from voice-port configuration mode
  loop-length       Configure loop length on this FXS port
  mwi               Enable MWI on this port
  no                Negate a command or set its defaults
  ren               Ringer Equivalence Number
  ring              Ring frequency Parameters
  shutdown          Take voice-port offline
  signal            The signaling type for the interface FXS or FXO
  snmp              Modify SNMP voice port parameters
  station-id        Configure station ID
  vmwi              Enable VMWI on this FXS port
```

  Conditions: Configuring voice-port in bulk mode

  Workaround: none

- CSCug44667

  Symptom: SG3 fax call failures observed for STCAPP audio calls.

  Conditions: Fax CM tone detection is turned ON even when all fax and modem related configurations have been disabled on the STCAPP gateway.

  Workaround: STCAPP modem pass-through feature can be enabled, but you may run into issues with some answering SG3 fax machines which have stringent requirements for fax CM signal.

- CSCug44692

  Symptom: Audio is skipped when short timeout is configured in Form Element in CVP Studio application

  Conditions: This symptom is observed during short timeout

Workaround: Inserting short silence at the first audio

- CSCug48145

  Symptom: ASR DTMF interworking failed after reinvite with block configured.

  Conditions: Dtmf with different preference configured will result in issue.

  Workaround: There is no workaround.

- CSCug53415

  Symptom: %SMC-2-BAD_ID_HW: is output, and SPA is not disabled. SPA should be disabled if authentication fail.

  Conditions: This symptom is observed on ASR1001 Built-in SPA

  Workaround: There is no workaround.

- CSCug56942

  Symptom: CUOM could not process MOSCQEReachedMajorThreshold clear trap from CUBE SP. For MOSCqe alert clear trap, CUBE should not sent CurrentLevel Varbind but should send csbQOSAlertCurrentValue Varbind.

  Conditions: When CUBE SP generates clear trap for voice quality alerts.

  Workaround: Manually clean the alarm at CUOM after root cause is rectified if earlier CUBE version is used.

- CSCug58617

  Symptom: Usernames do not show up in CCP Express. Username shows up on a router with default configuration.

  Conditions: The symptom is observed on routers with configurations that break show runn | format.

  Workaround: Use default configuration.

- CSCug60584

  Symptom: No audio coming from DSP during transcoding mode and then DSP is unresponsive

  Conditions: When doing transcoding and there is a simultaneous jump in both the sequence number and timestamp.

  Workaround: There is no workaround.

- CSCug63013

  Symptom: A DMVPN spoke router running 15.2(4)M3 and configured for Dual Hub - Dual DMVPN failover will fail to forward multicast traffic for EIGRP neighbor forming after failing from primary to backup and back to the primary. EIGRP neighbrship will fail to complete and flap on the spoke. The hub will never show any EIGRP neighborship.

  Conditions: DMVPN spoke router running 15.2(4)M3 in Dual Hub - Dual DMVPN scenario and running dynamic routing protocol must failover and failback to the primary tunnel for this to occur.

  Workaround: Removing "ip nhrp map multicast x.x.x.x y.y.y.y" and readding it resolves the problem. The issue is not observed in 15.2(4)M1.

- CSCug65706

  Symptom: Attaching performance monitor to OTV interface should be blocked. <conf t> interface Overlay1 otv control-group 239.1.1.1 service-policy type performance-monitor output new-policy ==> this configuration line should be blocked.

  Conditions: FAll tools avc config

Workaround: There is no workaround.

- CSCug66784

  Symptom: DSP fails to recover using "Test DSP Device 0 All Reset".

  Conditions: This symptom is observed when a crashed DSP (LSI PVDM3) fails to recover via the CLI command test voice dsp device 0 all reset.

  Workaround: A complete reload of the router is required to recover the DSP.

- CSCug68282

  Symptom: ASR1000 RP crash after software upgrade

  ```
  Apr 20 09:53:01.396: %SYS-3-BADBLOCK: Bad block pointer 3AFDF4B0 -Traceback=
  1#b3d795682537523829953c9aa18e3e0  :10000000 6FCCF4 :10000000 6FD0A0 :10000000
  1F2279C :10000000 1F1C1B0 :10000000 1F3F750 Apr 20 09:53:01.399: %SYS-6-MTRACE:
  mallocfree: addr, pc  33A1E15C,1011798C 33A1E15C,101178CC 33A1E15C,30000060
  4C3A105C,600003E4  4C3A0834,1049C71C 4C3A0834,1049C5FC 4C3A0834,400003FC
  412703FC,125DFF80 Apr 20 09:53:01.399: %SYS-6-MTRACE: mallocfree: addr, pc
  412703FC,300000F6 4C29B4E0,125DFF80 4C29B47C,20005F00 33A1E15C,1011798C
  33A1E15C,101178CC 33A1E15C,30000060 3AAFFF14,154DA6C4 4C1403F4,60000012 Apr 20
  09:53:01.399: %SYS-6-BLKINFO: Corrupted magic value in in-use block blk 3AFDF4B0,
  words 60, alloc 8, InUse, dealloc 0, rfcnt 1 -Traceback=
  1#b3d795682537523829953c9aa18e3e0  :10000000 6FCCF4 :10000000 6FD0A0 :10000000
  1F1D9C4 :10000000 1F227B4 :10000000 1F1C1B0 :10000000 1F3F750 Apr 20 09:53:01.402:
  %SYS-6-MEMDUMP: 0x3AFDF4B0: 0xF8 0x24 0x3C 0x1653EC7C Apr 20 09:53:01.402:
  %SYS-6-MEMDUMP: 0x3AFDF4C0: 0x8 0x8 0x3AFDF38C 0x8000003C Apr 20 09:53:01.402:
  %SYS-6-MEMDUMP: 0x3AFDF4D0: 0x1 0x0 0x1000001 0x3058827C  %Software-forced reload
  Exception to IOS Thread: Frame pointer 0x30742CC8, PC = 0x87308B4  UNIX-EXT-SIGNAL:
  Aborted(6), Process = Check heaps -Traceback= 1#b3d795682537523829953c9aa18e3e0
  c:86FA000 368B4 c:86FA000 368B4 c:86FA000 384C8 :10000000 32FD91C :10000000 1F227BC
  :10000000 1F1C1B0 :10000000 1F3F750   Fastpath Thread backtrace:  -Traceback=
  1#b3d795682537523829953c9aa18e3e0  c:86FA000 D9F08 c:86FA000 D9EE8 iosd_unix:887E000
  1580C pthread:7DB2000 5A4C   Auxiliary Thread backtrace:  -Traceback=
  1#b3d795682537523829953c9aa18e3e0  pthread:7DB2000 B598 pthread:7DB2000 B578
  c:86FA000 EF9C4 iosd_unix:887E000 212F4 pthread:7DB2000 5A4C   PC  = 0x087308B4  LR
  = 0x08732384  MSR = 0x0002D000 CTR = 0x07DC0D60  XER = 0x20000000 R0  = 0x000000FA
  R1  = 0x30742CC8  R2  = 0x30085C70  R3  = 0x00000000 R4  = 0x00006908  R5  = 0x00000006
  R6  = 0x00000000  R7  = 0x08730B5C R8  = 0x0002D000  R9  = 0x3007E7F0  R10 = 0x3007E7F0
  R11 = 0x30742CA0 R12 = 0x08732384  R13 = 0x18456078  R14 = 0x11F3F604  R15 = 0x00000000
  R16 = 0x00000000  R17 = 0x00000000  R18 = 0x00000000  R19 = 0x00000000 R20 = 0x00000000
  R21 = 0x1630C7D8  R22 = 0x18BDAA28  R23 = 0x18BDAC70 R24 = 0x18BDB3B8  R25 = 0xAB1234AB
  R26 = 0xAB1234CD  R27 = 0x30742E58 R28 = 0x3AFDF4E0  R29 = 0x30742CE0  R30 = 0x0886A7AC
  R31 = 0x00000006   ========= Start of Crashinfo Collection (09:53:01 UTC Sat Apr 20
  2013) =========  For image: Cisco IOS Software, IOS-XE Software
  (PPC_LINUX_IOSD-ADVIPSERVICESK9-M), Version 15.2(4)S1, RELEASE SOFTWARE (fc3)
  Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by Cisco
  Systems, Inc. Compiled Sat 06-Oct-12 11:55 by mcpre   Uptime = 00:02:51
  ```

  Conditions: Device configured with SBC with interchassis redundancy mode none application redundancy group 1 name ECS preempt priority 150 failover threshold 100 timers delay 100 control Port-channel30.8 protocol 1 data Port-channel30.9 track 1 decrement 200 track 2 decrement 200 protocol 1 name BFD timers hellotime msec 250 holdtime msec 1000

  Workaround: do not setup B2B redundancy between XE36(or older) and XE37(or later)

- CSCug72547

  Symptom: Static DMVPN spoke-spoke tunnel initially comes up when tunnel comes up, but if IPsec SAs go down (cleared or are not rekeyed) then the IPsec SAs will not come backup. Data traffic that is supposed to got directly over the spoke-spoke tunnel is forwarded over the spoke-hub-spoke path.

Conditions: Running DMVPN Phase 3 on an ASR1k as spoke routers, on both ends of the spoke-spoke tunnel. If the IPsec SAs for the spoke-spoke tunnel are cleared either because there was no spoke-spoke traffic for long enough for the IPsec SAs to not be rekeyed or or the idle-timer to expire or the IPsec SAs are cleared manually.

Workaround: Have a process (like IP SLA) ping the remote spokes tunnel IP address to keep the IPsec SAs up or to bring them back up if they happen to go down. Probably ping about every 60-120 seconds.

- CSCug77212

  Symptom: ASR1K CUBE RP may crash with Segmentation fault(11), Process = CCSIP_SPI_CONTROL when sip headers are manipulated using a sip profile for 200 response messages for KPML notify.

  Conditions: Crash seems to be happening due to SIP profiles configs being wrongly applied to Notify response (this profile was meant for 200 OK Invite response).

  Workaround: Do not configure sip profiles to manipulate the headers for 200 responses.

- CSCug83538

  Symptoms: Static routes injected through RRI (reverse-route static) are not getting removed.

  Conditions: This symptom is observed when a static crypto map that has "reverse-route static" enabled is applied on two different interfaces with a local-address.

  Workaround: Reload the Router.

- CSCug84396

  Symptom: May 3 12:46:21.835: %SYS-2-FREEFREE: Attempted to free unassigned memory at 3EC4FF9C, alloc 350B5A70, dealloc 350B5608 -Traceback= 35D9BEC4z 350C158Cz 350AEED8z 350B081Cz 32C23084z 32C23068z May 3 12:46:21.839: %SYS-6-MEMDUMP: 0x3EC4FF7C: 0x350B5A70 0x3EC50C58 0x3EC4FDF0 0x65E May 3 12:46:21.839: %SYS-6-MEMDUMP: 0x3EC4FF8C: 0x0 0x350B5608 0x1000133 0x3CDD2E48 %Software-forced reload -Traceback= 0x30DF22BCz 0x30DF05F0z 0x32C3278Cz 0x35D9BEC4z 0x350C158Cz 0x350AEED8z 0x350B081Cz 0x32C23084z 0x32C23068z

  Conditions: May be with Presence or Shared line feature.

  Workaround: There is no workaround.

- CSCug86432

  Symptom: Incorrect statistic from SNMP OID "1.3.6.1.4.1.9.9.171.1.3.1.1", related to a number of IPSec tunnels after running "clear crypto sa / session" command

  Conditions: Configured DMVPN, running "clear crypto sa / session" command

  Workaround: reloading of router helps to solve the issue

- CSCug88270

  Symptom: E1 R2 channels randomly get stuck in S_WAIT_RELEASE

  Conditions: Outgoing calls that get RNA might get stuck when the SP clears the channel

  Workaround: shut, no shut the controller

- CSCug93301

  Symptom:NGVM will fail to boot, causing DSP to be in downloading state

  Conditions:This condition may occur on the first attempt to boot a new NGVM module

  Workaround:Use the NGVM boot loader to set the PID environment variable to match the PID as shown in the "show diag subslot x/x eeprom" command.

- CSCug98723

  Symptom: The TCP RST packets generated by ZBFW are dropped by ZBFW on ASR box

  Conditions: TCP flow specific TCP RST packets generated by ASR to rset the connection to the client and server when "TCP packet inspection" is on.

  Workaround: There is no workaround.

- CSCug98820

  Symptom: multicast RP-Announcement/RP-Advertisement packet is replicated more than one copy per incoming packet. The number of copies is equal to the number of interfaces/ioitems with IC flag enabled (show ip mfib to get the number of IC interfaces)

  Conditions: AUTO-RP filter is configured on PIM interfaces

  Workaround: There is no workaround.

- CSCuh01007

  Symptom: After ESP 100 reload, "show policy-map interface" counters does not populate results

  Conditions: With an egress service policy on SPA gige interface and sending high/low priority traffic.

  Workaround: Reload the SPA after FP reload.

- CSCuh03859

  Symptom: If customer configured "snmp server enable traps sbc sla-violation-rev1", csbSLAViolationRev1 trap is not sent.

  Conditions: Normal operation.

  Workaround: There is no workaround.

- CSCuh09403

  Symptom: ESP may reload in B2B NAT ZBFW setup

  Conditions: B2B NAT ZBFW setup with stateful traffic

  Workaround: There is no workaround.

- CSCuh09451

  Symptom: Exception to IOS Thread:UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SBC main process

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuh12779

  Symptom: IPv6 ping packets fail

  Conditions: only with ICMPv6 echo reply RP generated packets.

  Workaround: There is no workaround.

- CSCuh13527

  Symptom: Create 2000 GRE IPSEC tunnels (sample config shown below, repeated 2000 times) causes RP crash interface tunnel10001 bandwidth 1000 ipv6 address 1003:0:0:1::1/64 ipv6 enable tunnel source Loopback10001 tunnel dest 1004:0:1:1::1 tunnel mode gre ipv6 tunnel protection ipsec profile hub10001

Conditions: On ASR1K: We have tested it to work fine when scaled up to 2500 sessions. At 4K, we have observed the crash. The in between numbers are not available.

Workaround: Do not configure beyond the scale of 2500 on ASR1K.

- CSCuh14012

  Symptom: The crypto session remains UP-ACTIVE after tunnels are brought down administratively.

  Conditions: This symptom occurs in tunnels with the same IPsec profile with a shared keyword.

  Workaround: There is no workaround.

- CSCuh27137

  Symptom: phone-proxy failed to attach to the second dial-peer

  Conditions: configure two phone proxy

  Workaround: Using one phone proxy Symptom: 2 phone-proxy added, one attach to dial-peer, the other phone-proxy failed to attach to the other dial-peer.

- CSCuh36750

  Symptom: ESP crashes

  Conditions: Subscriber session w/QoS over tunnel or shaped vlan.

  Workaround: There is no workaround.

- CSCuh38488

  Symptom: An ASR with zone-based firewall enabled may drop SIP INVITE packets with the following drop reason:

```
Router#show plat hardware qfp active feature firewall drop
-------------------------------------------------------------------------------
Drop Reason                                                            Packets
-------------------------------------------------------------------------------- L7
inspection returns drop                                                    1
Router#
```

  Conditions: Application (L7) inspection for SIP must be enabled for the flow.

  Workaround: Any of the following workarounds are applicable:

  1) Disable the port-to-application mapping for SIP with the 'no ip port-map sip port udp 5060' command. This prevents ZBF from treating UDP/5060 as SIP. Instead, it is treated as simple UDP.

  2) Use the 'pass' action in both directions instead of 'inspect'. This disables all inspection (even L4) for the traffic.

- CSCuh42885

  Symptom: changing modes in cgn and sending traffic results in ucode crash

  Conditions: unconfiguring one mode and switching to another mode and sending traffic

  Workaround: There is no workaround.

- CSCuh48747

  Symptom: Multiple NAT entries are created

  Conditions: UUT Configured with PAT with route-map

  Workaround: There is no workaround.

- CSCuh50125

  Symptom: ESP crashes

Conditions: On ASR1002-X, ESP100 or ESP200 based platforms, ESP can crash when you have interfaces where the bandwidth can change dynamically and you have a hierarchical QoS policy-map applied.

Workaround: When applying a hierarchical QoS policy-map to ain interface that supports dynamic bandwidth changes, be sure to apply the QoS policy while there are no bandwidth changes to the interface as the same time.

- CSCuh62307

  Symptom: ASR1000 router may crash when users run the **call-policy-set copy source XXX destination YYY** command to create a new call-policy-set.

  Conditions: This symptom is observed when you enter the na-src-address-table that is configured within the call-policy-set with na-src-address-table XXX after it the table is created by the **call-policy-set copy** command.

  Workaround: Instead of using **call-policy-set copy source XXX destination YYY** command, copy and paste the text into config terminal to create a new call-policy-set.

- CSCuh63682

  Symptom: Router crash in automatic test. The trigger to the crash is the following show command: **show flow monitor <name> cache format csv**

  Conditions: no delay between "configuration" phase and "show" command execution.

  Workaround: Maintain a delay of 10 seconds between "configuration" phase and "show" command execution.

- CSCuh66763

  Symptom: Following phrases are dispalyed in English irrespective of locale configured on CME. "Next" "Previous" "Please modify number" ""Invalid speed dial number" "Invalid personal speed dial number" "Invalid blf speed dial number" "Personal speed dial number can not exceed 32 digits" "Personal speed dial label can not exceed 30 characters" Speed dial number can not exceed 24 digits" "The record is full" "Please delete unuse entry" "Logging Out" "CME hardware conference" "CME software conference" "add party allowed" "add party not allowed" "Whisper" "CME group pickup" "CME pickup" "Access Mailbox (trnsfVM)" "Failed to send call to Mobile Phone" "Live Record is not enable" "Live Record already in progress" "Not conference creator." "Live Record has stopped", "Live Record timeout"]

  Conditions: This symptom is observed when non-English user-locale is configured.

  Workaround: There is no workaround.

- CSCuh74069

  Symptom: Super-package MDR ISSU fails with the following message:

  ```
  MDR:FAILED: Insufficient memory available on harddisk: to support MDR
  ```

  Conditions: Super-package MDR ISSU operation is issued.

  Workaround: Issue sub-package MDR ISSU.

- CSCuh75480

  Symptom: QFP reload may occur

  Conditions: When running NAT in CGN mode and doing a removal of a mapping

  Workaround: Switch to classic mode, to mapping removal, switch back to CGN mode.

Open Caveats—Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.0S

This section documents the open issues in Cisco ASR 1000 Series Aggregation Services Routers Release 3.10.0S.

- CSCuc33131

  Symptom: In some scenarios, retransmitted packets are not accounted against the retransmitted packet count metric.

  Conditions: If retransmitted packets have the same sequence numbers and same IP IDs, they are NOT treated as retransmitted packets. This can sometimes cause the retransmission packet count to be zero (0), incorrectly, even when there are retransmitted packets.

  Workaround: There is no workaround.

- CSCue39501

  Symptom: Rise in number of flows and memory utilization was observed when protocol pack 4.1 was integrated into XE3.10.

  Conditions: This may occur when using XE3.10

  Workaround: There is no workaround.

- CSCue60469

  Symptom: ASR1001 Series router throws error messages when a RP (IOS) switch over is done

  Conditions: ASR1001 Series router throws error messages when a RP (IOS) switch over is done along with traffic

  Workaround: There is no workaround.

- CSCue78691

  Symptom: The ESP may crash during ISSU (in-service software upgrade) downgrade from IOS XE 3.10 to IOS XE 3.8 or IOS XE 3.9, at the stage of route processor (RP) switchover.

- Conditions: The problem may occur when using one of the incorrectly defined "derived" records described for the CSCue53207 caveat. (Calculating derived fields is dependent on the values of other fields. CSCue53207 describes several fields incorrectly defined as derived.)

  Workaround: Configure the incorrectly defined records explicitly.

- CSCue86166

  Symptom: The interrupt infrastructure is in place; the userspace handling of interrupt delivery to HKP userspace driver code is not being done correctly.

  Conditions: This fixes the userspace handling of interrupt delivery to HKP userspace driver code

  Workaround: There is no workaround.

- CSCue86848

  Symptom: The output for the policy detailed view may not include information for some classes. Functionality is not affected. The following command provides the policy detailed view:

  show platform hardware qfp active feature mma client <policy-map_name> <policy_name> detail

  Workaround: There is no workaround.

- CSCue89240

Symptom: In presence of http subclassification, traffic goes to http tunneled protocol (behavior is broken, previously if http subclassification configured ,traffic never classifiy as http tunneled protocol, instead if subclassification does not match , it classify as "http")

Conditions: This symptom is observed when http subclassification is present.

Workaround: Remove http subclassification.

- CSCue91053

  Symptom:Full line rate HP traffic will have jitter between Max and Avg latency is 50 - 60 usec in Ethernet linecard for traffic lessthan 128byte frame size

  Conditions:When Full line rate HP traffic over ethernet linecard with frame size less than 128byte will experience Max Latency of 200 - 250 usec and with Avg Latency of 64-80 usec. And Jitter Between Max Latency is 50-60 usec

  Workaround: There is no workaround.

- CSCue94537

  Symptom: Tail drops are seen on FP 160 with HP traffic on ASR1000-2T 20X1GE Ethernet Line card.

  Conditions: When ASR1000-2T 20X1GE Ethernet Line card interfaces are configured with Service-policy to classify the egress Traffic and sending 40gbps of bi-directional traffic causes Tail drop on the QFP

  Workaround: Configure the Service-policy with larger q-limits. Policy-map test class prec1 priority level 1 q-limit 5000 packet More Info:

- CSCuf24865

  Symptom: sui_mtp_dp_dump_external_flags function is not registered.

  Conditions: when using show tech support CLI, a message appear that this function is not registered.

  Workaround: ignore the error message, a new function sui_dump_external_flags is replaced with this

- CSCuf30150

  Symptom: CUBE crashed in media flow-around call on overlord platform

  Conditions: This symptom is observed when media flow-around is configured on both inbound and outbound dial-peers

  Workaround: There is no workaround.

- CSCuf52756

  Symptom: %IOSXE_RP_SPA-4-IFCFG_CMD_TIMEOUT: Interface configuration commad

  Conditions: Observed tracebacks and traffic drop during MDR upgrade.

  Workaround: There is no workaround.

- CSCuf57507

  Symptom: EVENTLIB-3-RUNHOG: SIP2: cmcc: undefined: 7179ms

  Conditions: While performing an active RP failure during ASR1006 subpackage MDR upgrade

  Workaround: There is no workaround.

- CSCuf78556

Symptom: UPDATE is not being forwarded to UAC and it is being responded with 200OK to UAS. This issue is seen when UPDATE is received from UAS, when 18X transaction is still pending on UAC side

Conditions: This symptom is observed when 18x response is transmitted reliably on both call-legs.

Workaround: When UPDATE is received from UAS after some delay (i.e after completion of 18X ?PRACK transaction on UAC side), then CUBE is sending the early dialog UPDATE to the UAC side correctly.

- CSCuf80594

  Symptom: ESP Crash is observed after router is booted

  Conditions: This symptom is observed when reature is configured OTV with scale level of 250

  Workaround: There is no workaround.

- CSCuf84655

  Symptom: One-way video is seen while CUBE is trying to negotiate packetization mode=1 for H264 video codec in both the legs and one video endpoint doesn't support packetization mode=1 for H264 video codec.

  Conditions: When there is DO-DO video call from a video endpoint which supports only Packetization Mode=0 for H264 video codec to a video endpoint which supports both packetization modes like 0 & 1.

  Workaround: Make an EO-EO video call from the endpoint which only support packetization mode=0,so that CUBE will negotiate packetization mode=0 for both the legs and two-way video will be seen. More Info:

- CSCug01428

  Symptom: Router is hanged

  Conditions: After coping config with CLI "show platform hardware qfp active tcam resource-manager usage"

  Workaround: There is no workaround.

- CSCug23145

  Symptom: Interface where HSRP is configured , crypto ikev2 clustering feature does not work.

  Conditions: This symptom is observed when master or slave do not sync with each other and the socket error is seen.

  Workaround: Feature works without vrf.

- CSCug38621

  Symptom: Router crashed at ccsip_spi_incoming_reg_contact_change

  Conditions: This symptom is observed when configuring "registrar ipv4:9.60.51.254" under "sip-ua"

  Workaround: There is no workaround.

- CSCug40942

  Symptom: CUBE is modifying the refresher role in mid-dialog after 491 transaction.

  Conditions: This symptom is observed when session refresh is enabled for only one call-leg and not for other.

  Workaround: There is no workaround.

- CSCug47360

Symptom: The order of packets in the packet trace is not stable

Conditions: This symptom is observed when checking the output of packet trace, the order of packets with same flow change every time.

Workaround: check the output of the specific packet before and after the expected with ~2 packets deviation

- CSCug48525

  Symptom: On performing SPA OIR with configuration of Unicast/Multicast/Broadcast storm control on 32k EFPs,fman_fp core was observed

  Conditions: This issue is seen on FP100 card.

  Workaround: Workaround can be stop traffic before doing SPA OIR.

- CSCug50150

  Symptom: During MDR in a APS Setup, under certain conditions, IOSXE_APS-3-CCCONFIGFAILED, mesage is seen.

  Conditions: If the MDR of Protect interface is Started first followed by a MDR of the Working, then the above TB will occur.

  Workaround: Ensure that the working Interface is the first which goes through the MDR. IF the interfaces are on the SAME SIP, the traffic must be flowing through the Working interface, to e

- CSCug55787

  Symptoms: Serial interface protocol status shows down

  Condition: Perform OIR and configure few channel-groups. Then swap original board abck

  Workaround: Reload the router

- CSCug58033

  Symptom: For DNS ALG vtcp resemble size 16k , the default behavior is drop it due to limitation and send tcp reset to both outside and inside . But there was no rst is sent to inside at this moment.

  Conditions: This symptom is observed when dns alg response 16k from outside

  Workaround: There is no workaround.

- CSCug61559

  Symptom: Matching dameware-mrc protocol under it's attributes will not work.

  Conditions: Using the default protocol-pack.

  Workaround: There is no workaround.

- CSCug63839

  Symptom: 7301 router running c7301-advipservicesk9-mz.152-4.M3 is experiencing memory leak in Crypto IKMP process particularly on crypto_ikmp_config_send_ack_addr function

  Conditions: When running 7301 router and connecting EasyVPN through it, causes leak in Crypto IKMP process over time.

  Workaround: Reload the router over a period of time.

- CSCug73829

  Symptom: Data Conversion Errors seen while configuration changes at Remote end device.

  Conditions: Data Conversion Error and traceback can be seen while doing configuration changes on remote end device.

Workaround: There is no workaround.

- CSCug74947

  Symptom: When down physical interfaces on remote site routers, local router physical interface go down down and tunnel interfaces become up down. The ISAKMP for the tunnel that is connected with serial T3 goes down but for Gig link, ISAKMP remain QM_LDLE.

  Conditions: Irrespective of the Serial and Ethernet links, sometimes, multiple IKE SAs (duplicate SAs) get created with the same peer. When the dpd is configured and the interface of the peer is shutdown, the duplicate SA continues to exist

  Workaround: There is no workaround.

- CSCug78025

  Symptom:Multicast packets are dropped when DMVPN HUB is scaled.

  Conditions:This happens to bigger packet size. The problem is seen on ASR1001 and Overlord ISR4451.

  Workaround:There is no known workaround.

- CSCug99389

  Symptom: tracebacks when moving from the getvpn multicast rekey configs to getvpn unicast configurations with config-replace command

  Conditions: moving from getvpn mcast keyring to getvpn unicast keyring

  Workaround: without using config-replace command, completely erase the getvpn configuration from GM router and then try to configure the getvpn unicast rekey. On-fly don;t change configuration from getvpn mcast to unicast with help of config-replace command.

- CSCuh09872

  Symptom: Issue seems to happen when we check the bridge-domain related platform command, first on the RP, then on the FP repeatedly.

  Conditions: Usage of the 'show platform software bridge-domain rp active 11 mac-table' followed by 'show platform software bridge-domain fp standby 11 mac-table <>' multiple times results in this RP crash

  Workaround: There is no workaround.

- CSCuh11104

  Symptom: Memory leak is seen for SDP Passthrough scenario.

  Conditions: This memory leak occurs when the wsapp is not registered .

  Workaround: There is no workaround.

- CSCuh14758

  Symptom: Basic SIP calls fail with Redundancy Group enabled for Box to Box HA case

  Conditions: Redundancy Group enabled with dual attach for SP & ENT networks

  Workaround: Yes, remove and add the sip bindings (control/media) at the outgoing voip dial-peer after Redundancy Group is added in 'voice service voip'

- CSCuh23859

  Symptom: With Suite-B configured (i.e. esp-gcm / esp-gmac transform) on a GETVPN Key Server (KS), Group Members (GM) will see the following un-gated error message on the console when the KS policy ACL is changed or edited and a rekey is sent from the KS using "crypto gdoi ks rekey"...

May 31 09:56:49.906 IST: *** SERIOUS ERROR: OVERLAPPING IV RANGES DETECTED *** When the GM receives the rekey, the policy is installed successfully. However, after this the GM re-registers twice and then these errors are displayed.

Conditions: Suite-B is configured (i.e. esp-gcm / esp-gmac transform) on a GETVPN Key Server (KS), the KS policy ACL is changed or edited and a rekey is sent from the KS using "crypto gdoi ks rekey" This issue was seen with at least 50 Group Member (GM) instances using VRF-Lite on a ASR1K GM box and no more than 30 ACE's in the KS policy ACL, however this issue should also be seen on a ISRG2 GM box with less GM instances and less ACE's as well.

Workaround: If a Key Server (KS) policy ACL must be changed or edited while Group Members (GM) have already registered and downloaded GETVPN Suite-B policy (i.e. esp-gcm / esp-gmac transform), issue "crypto gdoi ks rekey replace-now" instead of "crypto gdoi ks rekey" after changing the KS policy ACL. (NOTE: a very small amount of traffic loss may be expected) If possible, do not change the KS policy ACL after a GETVPN network using Suite-B is up and running.

- CSCuh27266

  Symptom: CPP core not generated when FP crash happen

  Conditions: Perform SPA OIR with Unicast/Multicast/Broadcast storm control on 32k EFPs

  Workaround: There is no workaround.

- CSCuh29125

  Symptom: in meetme confernece calls, the call-id/tag modification for NOTIFY work for pre-INVITE NOTIFY, but it seems does not work pre-BYE NOTIFY

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuh42953

  Symptom: 10G ports on the [ASR1000-2T 20X1GE] Ethernet Line card is not able to handle traffic with IFG<=8

  Conditions: Traffic with IFG<=8

  Workaround: There is no workaround.

- CSCuh43137

  Symptom: With Suite-B configured (i.e. esp-gcm / esp-gmac transform), GETVPN Key Sever (KS) shows TEK SPI's for deny ACE's when "show crypto gdoi ks policy" is issued while a Group Member (GM) does not show TEK SPI's for deny ACE's when "show crypto gdoi" is issued.

  Conditions: The command "show crypto gdoi ks policy" is issued with Suite-B configured (i.e. esp-gcm / esp-gmac transform) deny ACE's in the policy ACL for GETVPN / GDOI.

  Workaround: There is no workaround.

- CSCuh53255

  Symptom: no media issue is encountered.

  Conditions: By default, without "asymmetric payload full" configured, there will be no end-to-end PT negotiated. CUBE should do payload type interworking at RTP level. But right now, CUBE does not behave correctly, no media issue is encountered.

  Workaround: configure "asymmetric payload full" under voice service voip -> sip

- CSCuh54693

  Symptom: Crypto Socket remains CLOSED on DmVPN setup

Conditions: DmVPN with extended CLI to mention IKE profile as the ISAKMP profile

Workaround: Remove the ikev2 profile configuration from the ipsec profile

- CSCuh55668

  Symptom: DSP Alarms observed & Call gets disconnected with VCC configuration on INBOX HA.

  Conditions: Steps to reproduce:

  1. Make call from A to B

  2. Once is call is successful, do HOLD (MOH)

  3. check "show log | inc DSP" to check the dsp alarms. 4. Do SSO, you will see DSP alarms on new active & call gets disconnected.

  ```
  Jun 18 00:02:10.914 IST: %SPA_DSPRM-3-DSPALARM: Received alarm indication from dsp
  (1/1/19).  Jun 18 00:02:10.914 IST: %SPA_DSPRM-3-DSPALARMINFO: 0042 0000 0080 0000
  0000 0000 4368 6563 6B73 756D 2046 6169 6C75 7265 3A63 3030 3030 3030 302C 3030 3030
  3030 3030 2C64 3031 3534 3834 342C 6430 3030 3030 3030 0000 0000 0000 0000 0000  Jun
  18 00:02:10.914 IST: %SPA_DSPRM-3-DSPALARMINFO: Checksum
  Failure:c0000000,00000000,d0154844,d0000000  Jun 18 00:02:10.914 IST: spa dsp alarm
  : dsp 1/1/18)  Jun 18 00:02:10.915 IST: %SPA_DSPRM-3-DSPALARM: Received alarm
  indication from dsp (1/1/20).  Jun 18 00:02:10.915 IST: %SPA_DSPRM-3-DSPALARMINFO:
  0042 0000 0080 0000 0000 0000 4368 6563 6B73 756D 2046 6169 6C75 7265 3A63 3030 3030
  3030 302C 3030 3030 3030 3030 2C64 3031 3534 3834 342C 6430 3030 3030 3030 0000 0000
  0038 0000 0000  Jun 18 00:02:10.915 IST: %SPA_DSPRM-3-DSPALARMINFO: Checksum
  Failure:c0000000,00000000,d0154844,d0000000  Jun 18 00:02:10.915 IST: spa dsp alarm
  : dsp 1/1/19)  Jun 18 00:02:10.917 IST: %SPA_DSPRM-3-DSPALARM: Received alarm
  indication from dsp (1/1/21).  Jun 18 00:02:10.917 IST: %SPA_DSPRM-3-DSPALARMINFO:
  0042 0000 0080 0000 0000 0000 4368 6563 6B73 756D 2046 6169 6C75 7265 3A63 3030 3030
  3030 302C 3030 3030 3030 3030 2C64 3031 3534 3834 342C 6430 3030 3030 3030 000A 7789
  0300 0000 0000  Jun 18 00:02:10.917 IST: %SPA_DSPRM-3-DSPALARMINFO: Checksum
  Failure:c0000000,00000000,d0154844,d0000000  Jun 18 00:02:10.917 IST: spa dsp alarm
  : dsp 1/1/20)
  ```

  Workaround: There is no workaround.

- CSCuh62529

  Symptom: ASR router crashes for media forking HA feature

  Conditions: media forking feature crashed in B2BHA standby router

  Workaround: There is no workaround.

- CSCuh62579

  Symptom: CUBE send 403 response for untrusted Requests by default. This request to make the TDOS feature enabled by default came from marketing for Ease-of-use to the customer.

  Conditions: Request should come from untrusted host.

  Workaround: enable silent-discard explicitly.

- CSCuh62628

  Symptom: ASR Router crashed for hydrogen serviceability feature

  Conditions: This symptom was observed under the following scenarios:

  1. enabled following event trace commands at common_setup section,

  ```
  monitor event-trace voip ccsip fsm
  monitor event-trace voip ccsip msg
  monitor event-trace voip ccsip misc
  monitor event-trace voip ccsip api
  monitor event-trace voip ccsip global
  ```

```
monitor event-trace voip ccsip limit connections 1000
monitor event-trace voip ccsip stacktrace 8
monitor event-trace voip ccsip history enable"
monitor event-trace voip ccsip history clear"
monitor event-trace voip ccsip all enable"
```

2. By default all feature codes and log level are enabled at particular TC setup section

3. Single audio call is established, after 4 to 5 sec. crash occurred.

Workaround: There is no workaround.

- CSCuh63727

  Symptom: Router may crash when unconfiguring large (8k) redirect ACL list in MASK config

  Conditions: There is no known condition.

  Workaround: There is no workaround.

- CSCuh66373

  Symptom: KS not sending rekey to the registered GM

  Conditions: KS not sending rekey to the registered GM

  Workaround: If we enable retransmission on KS , rekey are received by the GMs

- CSCuh66745

  Symptom: Error Message seen on ASR1K while reloading router

  Conditions: While reloading the asr1k box error message is coming

  Workaround: There is no workaround.

- CSCuh70934

  Symptom: Condition debug messages are showing for portchannel EVC even when the debug is not turned on

  Conditions: This symptom is observed when unconfig/config portchannel EVC, shut/not shut portchannel interface

  Workaround: There is no workaround.

- CSCuh70997

  Symptom: Memory leak observed in l2fib_nhop, l2fib_nhop_key,l2fib_nhop_update

  Conditions: This symptom is observed when clear xconnect all - during longevity

  Workaround: There is no workaround.

- CSCuh72004

  Symptom: FPD upgrade causes line protocol to stay down on ASR1000 Fixed Ethernet Line Card Interfaces, RP goes out of sync.

  Conditions: FPD upgrade on Ethernet Line Card causes this issue.

  Workaround: Reload of Line Card slot resolves the issue.

- CSCuh72756

  Symptom: When loading protocol-pack 6.0 or 6.1 a traceback might occur. There is no functionality impact.

  Conditions: When loading protocol-pack 6.0 or 6.1 on top of version 15.3(3)S with RP1 platform.

  Workaround: Currently there is no workaround.

- CSCuh74635

  Symptom:Syslog not seen for ICMP connection denied

  Conditions:Have a deny any any policy and send icmp traffic

  Workaround: There is no workaround.

- CSCuh75393

  Symptom: When subject name is used as secondary under truspoint for authorization without primary configured, it doesnt pick the correct value.

  Conditions: only subject name is configured as secondary without primary.

  Workaround: configure subject name as primary

- CSCuh77629

  Symptom: Alert-Info header is not passed through when given in any SIP message except initial INVITE.

  Conditions: Alert-Info header is not passed through when given in any SIP message except initial INVITE.

  Tested with 180,200 OK, re-invite and BYE messages.

  Alert-Info header is not passed through in any of the above messages.

  Workaround: There is no workaround.

- CSCuh81638

  Symptom: RP crashes at boot and continuously reloads.

  Conditions: %SCOOBY-3-SERIAL_BRIDGE_CRITICAL_ERROR_RATE: R1/0: cmand: Reloading R1:0 due to critically high serial bridge error rate. *Jun 28 19:26:55.074: %PMAN-3-PROCHOLDDOWN: R1/0: pman.sh: The process cmand has been helddown (rc 69)Jun 28 19:27:01.578 R1/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit with reload fru code

  Workaround: There is no workaround.

- CSCuh81850

  Symptom: Aux output on management interface.

  ```
  rtp-xdm-100:131> telnet hat-q 31401 Trying 172.18.133.41... Connected to hat-q.
  Escape character is '^]'.  Linux 2.6.32.39 (ASR1013-Q1401_RP_1) (0)  2013/06/28
  17:08:37 : <anon> [ASR1013-Q1401_RP_1:~]$  [ASR1013-Q1401_RP_1:~]$
  [ASR1013-Q1401_RP_1:~]$  [ASR1013-Q1401_RP_1:~]$  [ASR1013-Q1401_RP_1:~]$
  [ASR1013-Q1401_RP_1:~]$  [ASR1013-Q1401_RP_1:~]$  [ASR1013-Q1401_RP_1:~]$
  ```

  Conditions: Loaded latest image.

  Workaround: There is no workaround.

- CSCuh87618

  Symptom: Configured two APS groups (one for OC3/hdlc and other with OC12/PPP) between ASR1013 and ASR1006 using back to back connections. APS group 1 interfaces Inactive after RP-switchover

  Conditions: During ASR1013 Subpackage MDR

  Workaround: There is no workaround.

- CSCuh87919

  Symptom: Seeing PuntPerCausePolicerDrops on sending traffic through LISP router.

Conditions: No traffic drops associated

Workaround: There is no workaround.

- CSCuh91225

  Symptom: Router crashes @ pki_import_trustpool_bundle

  Conditions: While doing "default profile CiscoTAC-1" with call-home v2 feature

  Workaround: There is no workaround.

- CSCuh91563

  Symptom: ucode crash seen on unconifugring nat with nbar

  Conditions: This symptom is observed during a script run

  Workaround: There is no workaround.

- CSCuh95747

  Symptom: Hash table updated incorrectly when more than one interface assigned with ip address on wae

  Conditions: This symptom is observed when you apply ip and configs with uut and wae.

  Workaround: Issue not seen when there is only one interface assigned with ip address on wae.

- CSCuh97072

  Symptom: Under certain rare circumstance, ZBFW will not properly build the connection for the first packet of the flow. This causes subsequent packets to be dropped due to TCP state checking.

  Conditions: This was first observed when NAT, ZBFW and HA were all enabled on the ASR platform. This only affects ASR platforms.

  Workaround: Removing and re-adding the NAT configuration resolves the issue. Sometimes it requires readding the NAT configuration without any redundancy keywords before readding it with the redundancy keywords.

- CSCui00427

  Symptom: With Popinac line card, 40Gbps performance with 68byte frame sized data results in huge packet drops. The drops are reported as ESP tail drops.

  Conditions: Stress the Popinac line card with bi-directional 40Gbps traffic of frames size 68 bytes. Use ESP160 for test.

  Workaround: There is no workaround.

- CSCui01732

  Symptom: UUT is Crashing

  Conditions: UUT is configured in CGN mode

  Workaround: There is no workaround.

- CSCui02617

  Symptom: Hi scale resync on ANCP session can cause a crash on ESP100.

  Conditions: ANCP Resync at scales beyond 200 AN-Subscribers

  Workaround: There is no workaround.

- CSCui05310

  Symptom: CPP crashes when arp packets are received on an interface which has platform conditional debugging with access-list as filter is enabled.

Conditions:

1. platform conditional debugging with access-list as filter is enabled

2. About 50 ARP packets are received on interface what has platform conditional debugging is enabled

Workaround: Do not use access-list as filter for platform conditional debugging

- CSCui05893

  Symptom: UUT is crashing

  Conditions: Sending Traffic from 50 K addresses

  Workaround: There is no workaround.

- CSCui08714

  Symptom: Show vlan counters refreshed after RP switchover on dual RP system

  Conditions: Send traffic through a VLAN on Popinac---SPA back to back connectivity. Check the vlan coutners using "**show vlan dot1q <vlanid>**" show command. Switchover to redundant RP. Now check the "**show vlan dot1q <vlanid>** " cmd to see if the counters are incremental or starting from 0 after standby RP becomes Active .

  Workaround: There is no workaround.

- CSCui10537

  Symptom: When E1 interface have both channel-group and ds0-group, OIR will have some issues

  Conditions: Some framer bits are not completely cleaned up, causing interface failed to come up.

  Workaround: Sometimes shut/no shut will fix this issue.

- CSCui29433

  Symptom: An ISSU breakage will occur when upgrading from IOS XE 3.9.2 to IOS XE 3.10 if the router configuration includes a flow record with the following fields:

  collect connection client counter bytes network long

  collect connection server counter bytes network long

  Conditions: The router configuration includes a flow record with the following CLI:

  flow record type performance-monitor rec…

  collect connection client counter bytes network long

  collect connection server counter bytes network long...

  Workaround: Remove the field configuration described above before upgrading to IOS XE 3.10, or upgrade directly to 3.10.1 when it becomes available. The following describes how to remove the problematic field configuration:

  flow record type performance-monitor rec

  no collect connection client counter bytes network long

  no collect connection server counter bytes network long

- CSCui40686

  Symptom: **show policy-map target service-context <service-context name> passthru-reason** command does not show the correct PT stats indicated by SN on AppNav-XE.

  All the below mentioned statistics will have incorrect values.

  Indicated by SN:

```
Passthrough Reasons           Packets       Bytes
-------------------           -------      --------
   PT Internal Error                0             0
   PT App Override                  0             0
   PT Server Black List             0             0
   PT AD Version Mismatch           0             0
   PT AD AO Incompatible            0             0
   PT AD AOIM Progress              0             0
   PT DM Version Mismatch           0             0
   PT Peer Override                 0             0
   PT Bad AD Options                0             0
   PT Non-optimizing Peer           0             0
   PT SN Interception ACL           0             0
   PT IP Fragment Unsupport         0             0
```

Conditions: When the AppNav-XE is acting as the controller with 3.9/3.10/3.11 image and Service nodes having WAAS 5.3.1 image (intruder), the PT reasons indicated by the SN is not interpreted correctly on AppNav-XE since the PT reasons are offset by 1. This messes up with the PT reason stats on AppNav-XE.

Workaround: There is no workaround.