Caveats for Cisco IOS Release 15.2(4)M

Caveats

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

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

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

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

This document contains the following sections:

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

Resolved Caveats—Cisco IOS Release 15.2(4)M5

- CSCtd45679

  Symptom: The standby supervisor reloads after removing an IPSLA probe via CLI:

  ```
  R7600(config)#no ip sla 1
  R7600(config)#
  06:53:31: Config Sync: Line-by-Line sync verifying failure on command: no ip sla 1 due
  to parser return error
  06:53:31: rf_reload_peer_stub: RP sending reload request to Standby. User:
  Config-Sync, Reason: Configuration mismatch
  R7600(config)# 06:53:31: %RF-SP-5-RF_RELOAD: Peer reload. Reason: Proxy request to
  reload peer
  R7600(config)# 06:53:31: %OIR-SP-3-PWRCYCLE: Card in module 6, is being power-cycled
  (RF request)
  R7600(config)# 06:53:32: %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded,
  changing to Simplex mode
  R7600(config)#
  ```

  Conditions: This issue only occurs if the probe is configured via SNMP.

  Workaround: Remove the probe via SNMP.

  More Info: This issue is applicable to a Cisco Catalyst 6500 platform running Cisco IOS 12.2SX releases. It may also affect other high availability (HA) platforms running Cisco IOS 12.2 or 15.X releases.

- CSCtq02528

  Symptom: Router crashes when executing **show ip ips session**.

  Conditions: This symptom is observed when you have the IPS configured and applied to at least one interface.

  Workaround: Disable IPS configuration.

- CSCts11166

  Symptoms: A router crashes at cce_dp_ipc_save_feature_objects.

  Conditions: This symptom occurs on a Cisco 2951 router running Cisco IOS Release 15.1(2)T1 and Cisco IOS Release 15.1(4)M1.

  Workaround: There is no workaround as the trigger of the issue is unknown.

- 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.

- CSCtz54775

  Symptom: Traffic sourced from a 2901 through a EHWIC-4ESG module resumes forwarding within a maximum of 5 minutes (ARP expiry) instead of 30 seconds (STP convergence time).

  Conditions: This symptom is observed after an STP failover occurs.

  Workaround: Clear the ARP table of the affected interface (after the VLAN is in a forwarding state).

- CSCtz98228

  Symptom: On the Cisco 3900e platform, a crash and router reload occurs without generating any crashinfo and traceback.

  Conditions: This symptom could be seen with HTTP traffic intercepted by the content-scan feature. It is mostly seen during the content-scan session creation.

  Workaround: Disable the content-scan feature.

- CSCua35161

  Symptom: On the DMVPN HUB, some crypto maps still exist after removing Tunnel protection from the Tunnel interface.

  Conditions: This symptom occurs with scaling test.

  Workaround: There is no workaround.

- CSCub04965

  Symptom: Multiple symptoms may occur including:

  - Multiple sessions established to TACACS+ server which never clear are seen in the output of **show tcp brief**.
  - Pings to the loopback address from directly connected equipment suffers packet loss.
  - Traffic and pings through the switch suffers packet loss.
  - CPU utilization remained stable and below 10% when the issue was occurring, the interface counters were not reporting any errors or drops.
  - TACACS+ authentication errors, authorization errors, or accounting errors.
  - SSH/TELNET via VTY not accessible.
  - If condition exists for a period of time the switch may stop passing traffic.

  Conditions: The symptom is observed when the device is configured with TACACS+. It is seen mostly on Cisco 3750/3760 switches, but has been observed on Cisco 6500 switches.

  Workaround:

  1. Remove the AAA and TACACS+ server configuration.
  2. Clear the existing TCP connections with **clear tcp tcb**.
  3. Reconfigure the TACACS+ server configuration to use “single-connection” mode.
  4. Reconfigure the AAA configuration.

  Mitigation using EEM: A Cisco IOS Embedded Event Manager (EEM) policy that is based on Tool Command Language (Tcl) can be used on vulnerable Cisco IOS devices to identify and detect a hung, extended, or indefinite TCP connection that causes the symptoms to be observed. The policy allows administrators to monitor TCP connections on a Cisco IOS device. When Cisco IOS EEM detects hung or stale TCP connections, the policy can trigger a response by sending a syslog message or a Simple Network Management Protocol (SNMP) trap to clear the TCP connection. The example policy provided in this document is based on a Tcl script that monitors and parses the output from two commands at defined intervals, produces a syslog message when the monitor threshold reaches its configured value, and can reset the TCP connection. The EEM script is available at:

https://supportforums.cisco.com/docs/DOC-19344

- CSCub52278

  Symptom: The DVTI Virtual Access interface may flap during rekey with a large number of IKEv2/IPSec tunnels.

  Conditions: This symptom occurs when IKEv2 is used in large scale deployment.

  Workaround: There is no workaround.

- CSCub83800

  Symptom: The Copperopolis interface configuration gets rejected.

  Conditions: This symptom occurs due to the following NBAR configurations:

  ```
  flow record type mace sfr-avcrec
  collect application http host
  flow exporter LO-exp
  destination 10.88.128.253
  source GigabitEthernet0/1
  ```

  Workaround: Move NBAR related configurations after shdsl controller configurations.

- CSCuc11958

  Symptom: 7600-SIP-400 linecard crash seen with SPA reload.

  Conditions: The symptom is observed with a SPA reload.

  Workaround: There is no workaround.

- CSCuc88175

  Symptoms: When a dynamic cryptomap is used on the Virtual Template interface, SAs do not created and thus the testscripts fail. This issue occurs because the crypto map configurations are not added to the NVGEN, and hence there is no security policy applied on the Virtual Template interface.

  Conditions: This symptom occurs only when a dynamic map is used on the Virtual Template interface. However, this issue is not seen when tunnel protection is used on the Virtual Template interface or when a dynamic map is used on the typical physical interface.

  Workaround: There is no workaround apart from using tunnel protection on the Virtual Template interface.

- CSCuc95160

  Symptoms: After receiving the CRCX message, the Cisco AS5400 does not send 200 ok to SSW. SSW sends the CRCX message to the Cisco AS5400 again. Between these messages, debug outputs are displayed. It seems that the call is not disconnected completely for the end point by the previous disconnect request (the DLCX is received after the CRCX message from SSW). The end point may be stuck in call_disconnecting state.

  Conditions: This symptom is observed with MGCP. This issue occurs when the Cisco AS5400 receives DLCX before sending 200 ok for the first CRCX message.

  Workaround: There is no workaround.

- CSCud13768

  Symptom: RP crashes while trying to verify UDP-JITTER in IP SLAs VRF-lite.

Conditions: This symptom occurs while trying to verify IP SLAs UDP Jitter operation.

Workaround: There is no workaround.

- CSCud24601

  Symptoms: After performing an SSO on a Quad-SUP setup, the previous standby displays the following error message on the console:

  ```
  *Nov 16 15:50:28.455: SW1-7_STBY: ics_cs_nego_open_active_port: ERROR: (no such port):
  Failed to locate active port *Nov 16 15:50:29.591: SW1-7_STBY: Bring up standby
  supervisor as a DFC *Nov 16 15:50:32.331: %PFREDUN-SW1-7_STBY-6-STANDBY: Initializing
  for SSO mode in In-chassis Domain
  ```

  Conditions: This symptom occurs occasionally after performing an SSO on a Quad- SUP setup. This error message is harmless. The system will still reach SSO successfully.

  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 occurs after a reload. The GM fails to install policies from the key server.

  Workaround: Remove the crypto map configuration on the interface and reapply.

- CSCud70577

  Symptoms: RTSP traffic is being dropped with NAT (PAT) and NBAR.

  Conditions: The issue is seen when protocol-disc (cisco-ip-camera or realmedia) and NAT is enabled on the same interface.

  Workaround: Disable NBAR feature.

- CSCud94248

  Symptom: The IOS Gateway reloads when it gets a 400 error response during protocol based fax up-speed.

  Conditions: A fax tone detected on the gateway causes it to send a T.38 Fax offer on the SIP leg. However, the remote SIP device is not configured for fax and hence the gateway receives a 400 Bad Request response for the T.38 Fax offer. When responding with an ACK for the 400 Bad Request response, the gateway reloads.

  Workaround: Remove the fax configuration at both global and dial-peer level.

  ```
  Global: voice service voip no fax protocol t38
  Dial-peer : dial-peer voice <tag> voip no fax protocol t38
  ```

- CSCue08667

  Symptom: When an SMS is received on a system that does not have any pending SMS stored, the new incoming SMS cannot be read with “cellular 0 gsm sms view all”.

  Conditions: This symptom occurs when no pending SMS on the router is stored before this event.

  Workaround: Reload the router. After the reload, all existing and new messages will be visible with the show command.

- CSCue18443

  Symptom: Command authorization is denied while entering an access list that includes a host address and a subnet mask.

  Conditions: This symptom occurs in Cisco IOS Release 15.1(4)M2.

Workaround: There is no workaround.

- CSCue32707

  Symptom: crypto pki export <> causes crash.

  Conditions: This symptom is observed in when a SUB CA trustpoint is configured and a trustpoint is configured and enrolled to that SUB CA.

  Workaround: If possible, have the trustpoint on a separate box.

- CSCue45822

  Symptom: A Cisco 7200 router with a C7200-VSA VPN service module may reload due to memory corruption on boot up.

  Conditions: This symptom is only seen in releases based on Cisco IOS Release 15.2(4)M3. It was introduced via CSCud54133.

  Workaround: There is no workaround.

- CSCue48419

  Symptoms: The Cisco AS5350 stops processing calls on PRI with a signaling backhaul from PGW. In the packet trace, there is no q931message from PGW. Further analysis shows that as5350 sends a q_hold (0x5)message in BSM, causing peer (PGW) to stop sending signaling traffic. However, there is no BSM_resume message or BSM_reset sent after it. Hence, PGW is stuck in this condition. There was earlier defect for CSCts75818 with similar symptoms in U-state.

  Conditions: This symptom is observed due to some RUDP timing issues that cause BSM session switchover.

  Workaround: Reload the Cisco AS5350 (but only when CU notices the outage). Also, shutting both Ethernet interfaces may help, but this workaround has not been tested.

- CSCue68318

  Symptoms: The ATM interface and subinterface are up/up but are unable to access the Internet.

  Conditions: This symptom occurs only when the IP address of that ATM interface is configured under the EIGRP process.

  Workaround: Downgrade to Cisco IOS Release 15.0(1)M8.

- CSCue69214

  Symptom: Memory leaks are seen in the metadata after removing a virtual interface.

  Conditions: This symptom occurs after removing a virtual interface, if metadata is enabled.

  Workaround: There is no workaround.

- CSCue74612

  Symptom: FTP download fails in FTS client.

  Conditions: The symptom is observed with FTS transfer over FTP via VRF.

  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.

- CSCue93416

  Symptom: The startup configuration is not present in ICS after a reload.

  Conditions: This symptom occurs when the startup configuration is modified and the router is reloaded without saving it.

  Workaround: Once the router is up, enter the **wr mem** command which will update the startup configuration to ICS and standby.

- CSCuf48207

  Symptom: Controller SHDSL Group (0) info is in DSL DOWN state:

  ```
  Type: 2-wire g.shdsl, status: Configure Firmware SHDSL wire-pair (0)
  ```

  Conditions: This symptom occurs when the SHDSL line is noisy and the SHDSL controller is struck in GHS_STARTUP state.

  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.

- CSCuf78524

  Symptom: Pings done with size near to the “ppp multilink fragment size” fails when performed from a device connected to the Cisco 2901 router. However, the ping is a success when performed directly from the router.

  Conditions: This symptom is observed when the pings are performed from a device connected to the Cisco 2901 router.

  Workaround: There is no workaround.

- CSCug17808

  Symptom:In Certain Scenarios, EIGRP Routes are advertised only to Stub Peers, not advertised to Non-Stub Peers.

  EIGRP Routes - Routes in EIGRP Topo table. It can be Routes learnt by EIGRP Peer OR Redistributed also.

  Conditions:This symptom is observed when Cisco ASR router is rebooted or the route is cleared via the **clear ip route** command, the route disappears form the spokes. This bug is not restricted to ASR. It can happen with any kind of router when all of the following conditions are met.

  1. Peers to be mixture of Stubs and Non Stubs.
  2. When Route is Lost, We send QUERY to non-stubs and waiting for REPLY from Non Stubs about QUERY.
  3. A new update needs to be sent to all Peers.

  Workaround: Advised to upgrade to an image with a fix. Clearing the EIGRP Neighborship restores the route on the spokes.

More Info: In an ideal scenario, the following is the sequence is:

1. When Route is Lost, Send QUERY to Non-Stubs
2. After Receiving REPLY from Non-Stubs, Send Infinite Metric to Stub Peers
3. Route Learnt Again
4. Route advertised to both Stub and Non Stub Peers properly.

In a defective scenario, (for example clear route), as the new route is learnt before getting a reply from Non Stubs especially when NonStub Neighbors/ Networks beyond Non Stubs are more, step 3 of the sequence comes before step 2. In such cases Routes were sent only to Stub.

- CSCug24114

  Symptom: CTS environment-data download fails from ISE.

  Conditions: The symptom is observed if there is less PAC and environment-data refresh timer is configured in ISE. After multiple refreshes of PAC and environment data and the switch is reloaded, sometimes a CTS environment-data download fails from ISE on the switch.

  Workaround: Unconfigure **pac key CLI** and configure it again as below:

  ```
  no pac key pac key <key-id>
  ```

- CSCug27021

  Symptom:

  - The following message is seen in the log:

  ```
  SYS-2-BADSHARE Bad refcount in retparticle, ptr=xxx, count=0
  ```

  - Interface is up but does not work.

  Conditions: This symptom occurs in a router with an EHWIC-VA-DSL-B card, crypto traffic through a tunnel on the ATM and “qos pre-classify” under the tunnel interface on the ATM.

  Workaround: Remove “qos pre-classify” under the tunnel interface.

- CSCug31938

  Symptom: A device will crash leaving a 0 byte crashinfo file. The console will display some crash data but once its displayed, the device will hang until a power cycle is done. The crash data on the console looks like this:

  ```
  *Apr 12 02:53:46.387: %LINK-3-UPDOWN: Interface ATM1/0, changed state to up *Apr 12
  02:53:46.395: %SYS-2-INTSCHED: ’may_suspend’ at level 3 -Process= "Net Background",
  ipl= 3, pid= 48 -Traceback= 43F07688z 4370C8D4z 436F7C98z 4384F788z 43784928z
  4377FB48z 4377FD4Cz 43781550z 438A6220z 41E64B80z 40B79A44z 40B97724z 40B74B44z
  414F25A4z 414853F4z 414E3660z *Apr 12 02:53:46.399: %SYS-2-INTSCHED: ’may_suspend’ at
  level 3 -Process= "Net Background", ipl= 3, pid= 48 -Traceback= 43F07688z 4370C8D4z
  436F7C98z 4384F788z 43784928z 4377FDB8z 43781550z 438A6220z 41E64B80z 40B79A44z
  40B97724z 40B74B44z 414F25A4z 414853F4z 414E3660z 414F1F1Cz *Apr 12 02:53:46.415:
  %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 485BDEF0. -Process= "Net
  Background", ipl= 4, pid= 48 -Traceback= 43F032E4z 403BD15Cz 43E99DB4z 43E99D98z
  02:53:47 UTC Fri Apr 12 2013: Breakpoint exception, CPU signal 23, PC = 0x40078394
  ```

  Conditions: This issue occurs after applying a QOS policy to an ATM interface that utilizes the rs8234 driver. The NM-1A-OC3, NM-1A-T3, and NM-1A-E3 modules use the driver. The QOS policy also invokes a classmap that uses NBAR.

  Workaround: Remove QOS from the interface or remove NBAR from the classmap.

- CSCug34404

  Symptom: RP crash seen at be_interface_action_remove_old_sadb.

Conditions: The symptom is observed while unconfiguring the 4K SVTI sessions after an HA test.

Workaround: There is no workaround.

- CSCug34877

  Symptom: Switch crashes with the following message:

  ```
  %SYS-2-LINKED: Bad enqueue of 901E0D40 in queue 1AABE690 -Process= "SSH Process", ipl=
  0, pid= 392
  ```

  Conditions: This symptom occurs during an SSH connection to a remote device from the switch while having multiple SSH connections to the same switch.

  Workaround: There is no workaround.

- CSCug38011

  Symptom: Device crashes with CPU hog messages.

  Conditions: The symptom is observed when the device is reloaded after configuring NTP peer:

  ```
  ntp server pool.ntp.org source cell0
  ```

  Workaround: There is no workaround.

- 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.

- CSCug62154

  Symptom: CPU shoots to 100% with TACACS configuration. VTY to the device does not work due to this.

  Conditions: This symptom is observed when the router or switch is booted up with TACACS configurations and the CPU shoots up to 100%. Telnet to the router is not possible. Any command issued on the console would take lot of time.

  Workaround: Remove the TACACS configurations and then reboot the router.

- CSCug63013

  Symptom: A DMVPN spoke router running Cisco IOS Release 15.2(4)M3 and configured with “if-state nhrp” might not reform eigrp neighbourship if the line protocol on the interface goes down and comes back automatically.

  Conditions: This symptom occurs in a DMVPN spoke router running 15.2(4)M3 with “if-state nhrp” configured and interface line protocol going down. It must also be using the new multicast code (15.1(4)M onwards).

  Workaround:

  – Removing “ip nhrp map multicast x.x.x.x y.y.y.y” and readding it resolves the problem.

  – Shut/no shut on the tunnel interface

  More Info: This issue does not exist in Cisco IOS Release 15.2(4)M1.

- CSCug63839

  Symptom: The Cisco 7301 router running c7301-advipservicesk9-mz.152-4.M3 experiences a memory leak in the Crypto IKMP process particularly on the crypto_ikmp_config_send_ack_addr function.

  Conditions: This symptom occurs when running the Cisco 7301 router and connecting EasyVPN through it.

  Workaround: Reload the router over a period of time.

- CSCug72891

  Symptom: EIGRP neighbor flaps due to EIGRP SIA. Troubleshooting shows that a race condition causes EIGRP successor loop first and it leads to EIGRP QUERY loop resulting in the neighbor flaps.

  Conditions: The issue is observed when a worse metric update is received from the successor, once the route is already in active state, in a partially peered multiaccess network.

  Workaround: There is no workaround.

- CSCug78098

  Symptom: Supervisor engine crashes and the Cisco IOS software is forced to reload due to PIM process.

  Conditions: This symptom is observed when using the command, **show ip pim rp-hash** right after the BSR RP times out, causes the crash.

  Workaround: Perform these steps in the following order:

  1. Wait for a minute after BSR RP times out before using this command.
  2. Configuring **no ip domain lookup** will make the time taken to execute **show ip pim rp-hash** to a few milliseconds. This will prevent the crash from being reproduced manually.

- CSCuh23940

  Symptom: The line status of the 9th port is up/down for HWIC-D-9ESW in the Cisco 3945 Integrated Services Router. The port status displays down/down in Cisco IOS Release 15.3(1)T1 and Cisco IOS Release 15.1(4)M5.

  Conditions: This symptom occurs when the Cisco 3945 Integrated Services Router is used.

  Workaround: There is no workaround.

- CSCuh29716

  Symptom: When a call is transferred from IVR to PSTN, the codec negotiation with Verizon fails only if the original invite received includes fax capabilities, dropping the call with reason code 47 and hanging the UDP port used.

  Call flow:

  Verizon -- CUBE -- CUSP -- Genesys/IVR, transferred with SIP Refer back to PSTN hair-pinning the call on CUBE.

  All subsequent calls that try to re-use the same UDP port for RTP stream are dropped with reason code 47 and provisn RSP fail is logged on **show voip fpi stats**.

  Conditions: This symptom occurs in hair-pinned calls that receive FAX capabilities on the original SIP invite from Verizon.

  Workaround: There is no workaround. Reload the router to clear UDP ports.

- CSCuh30421

  Symptom: Memory leak issue could be seen in X.25 Background XOT SVC/tcp_allocatetcb.

  Conditions: Cisco IOS Release 15.1(4)M6 acting as XOT GW-: X.25 Over TCP.

  Workaround: Reload the router.

- 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”.

- 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
  ```

- 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.

- CSCuh43252

  Symptom: After upgrading to Cisco IOS Release 15.0(2)SE3, you can no longer authenticate using TACACS. The TPLUS process on the switch will be pushing the CPU up to 99%.

  Conditions: The symptom is observed when you use TACACS for authentication.

  Workaround: Downgrade the switch to a version prior to 15.0(2)SE3.

- CSCuh46031

  Symptom: The Cisco ASR 1000 router sends a different Acct-Session-Id in the Access-Request and Accounting-Request for the same user.

  Conditions: This symptom occurs when Flex VPN IPsec remote access is configured.

Workaround: There is no workaround.

- CSCuh54504

  Symptom: Drops on Ge interface when QOS policy map applied on Serial interface. For test ping directly connected IP on Ge interface without service policy. If policy is applied on Se interface there is a ping drops on Ge. If policy is not applied on Se interface, then there is no drop.

  Conditions: This symptom is observed on Cisco 2911 router with few VWIC2-2MFT-T1/E1, all Cisco IOS Release 15.x versions. Problems acquired when you apply policy map on serial interface.

  Workaround 1: Remove the policy map.

  Workaround 2: Use the Cisco 2800 platform.

- 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.

- 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.

  More Info: This crash occurred in a customer environment and device with a particular version of the software (Cisco IOS Release 15.1(2)S2). No other similar issue has been identified so far.

- 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.

  More Info: When sending the Accounting Start/Stop msgs the Calling-Station-ID #31 attribute is not added. It is only included in the case of Auth Requests.

- CSCuh98328

  Symptom: Cisco router software restarts.

Conditions: This symptom is observed when Cisco router is configured for waas-express. It is possible that trigger is one of following:

1. WAAS Express was disabled and re-enabled.
2. CIFS-Express Accelerator was disabled and re-enabled.
3. **clear waas cache cifs-express** command was executed.

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. At this point, responder does not have control over selecting the right certificate.

- 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.

- 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.

- CSCui21061

  Symptom: Multicast stops working when CDP is disabled on a physical interface that is part of a port-channel.

  Conditions: This issue is seen when "no cdp enable" is issued on the physical interface. It is not seen if CDP is disabled globally, or if there is no port-channel configured.

  Workaround: Disable CDP globally or use a configuration that does not involve a port-channel.

- CSCui36394

  Symptom: Lots of misalignment errors in show alignment output.

  Conditions: This symptom is observed during normal operation with mlppp or ISM installed.

  Workaround 1: Stop using mlppp until the code fix available.

  Workaround 2: Stop using the ISM and switch to the onboard encryption module until we get a fix.

Resolved Caveats—Cisco IOS Release 15.2(4)M4

- CSCsr06399

  Symptom: A Cisco 5400XM may reload unexpectedly.

  Conditions: This symptom is intermittent and is seen only when the DSPs available are insufficient to support the number of calls.

  Workaround: Ensure that sufficient DSPs are available for transcoding.

- CSCta80024

  Symptom: The router crashes while using the **string repeat** command with the biggest number in the TCL shell.

  Conditions: This symptom occurs when the **string repeat** command is used with the biggest number. This issue also depends on the string being used. For example, the below commands in the TCL shell will lead to crashing of the router.

  ```
  proc demo foo "set bar [string repeat {$foo} 255]"
  demo [string repeat a 16843010]; concat
  ```

  Workaround: There is no workaround.

- CSCtl55445

  Symptom: CUBE logs 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.

- CSCtq12007

  Symptom: Using a c7200 VSA in a 15.0M image, when there are multiple shared IPsec tunnels using the same IPsec protection policy, removing the policy from one tunnel could cause other tunnels to stop working until the next rekey or tunnel reset.

  Using a c7200 VSA in a 15.1T or 15.2T image, you can also see a similar problem but one that is less sever; you may see one every other packet drop, until the next rekey or tunnel reset.

  Conditions: In a 15.0M, 15.1T, and 15.2T image, VSA is used as the crypto engine.

  Workaround: Force a rekey after removing the shared policy from any shared tunnels by using the **clear crypto session** command or resetting all the tunnels.

- CSCtr88785

  Symptom: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.

Conditions: This symptom is observed on a Cisco 3845 running the c3845-advipservicesk9-mz.151-4.M1 image with a PKI certificate server configuration.

Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCts60458

  Symptom: There is a memory leak in PfR MIB.

  Conditions: This symptom occurs when PfR is configured.

  Workaround: There is no workaround.

- CSCtt96462

  Symptom: Traffic gets dropped across the tunnel interface when you have the following features enabled:

  - NAT
  - VRF
  - IPsec

  Conditions: The symptom is observed when crypto map and VRF are applied under physical interface.

  Workaround: Disable CEF.

- CSCtx56183

  Symptom: Router crashes due to block overrun:

  ```
  %SYS-3-OVERRUN: Block overrun at 49156754 (red zone 66616365) -Traceback= 42806C04z
  42809B20z 42809D14z 427AD988z 427AD96Cz . . %SYS-6-BLKINFO: Corrupted redzone blk
  49156754.... . %SYS-6-MEMDUMP: 0x49156754: 0xAB1234CD 0x12A0000 0x12C 0x44395148
  %SYS-6-MEMDUMP: 0x49156764: 0x419B243C 0x49157154 0x49156658 0x800004E8
  %SYS-6-MEMDUMP: 0x49156774: 0x1 0x0 0x1000133 0x47D7699C
  ```

  Conditions: This issue is seen when Websense URL filtering enabled and long URLs have been accessed.

  Workaround: Disable URL filtering.

  Workaround 2: Do not invoke long URLs.

- CSCtx99353

  Symptom: %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level.

  Conditions: The symptom is observed when music on hold (MOH) is enabled.

  Workaround: 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).

- CSCty26035

  Symptom:

  1. There is a discrepancy in the inbound and the outbound SA lifetime in the standby router.
  2. The KB lifetime in a standby router is greater than that of the active router, when a KB lifetime rekey occurs.
  3. The ping will not go through after applying a dynamic crypto map.

  Conditions: The issues are seen after establishing the session between the HA routers and various test conditions.

  Workaround: There is no workaround.

- CSCty57970

  Symptom: A crash occurs when “content-scan out” is unconfigured from the egress interface.

  Conditions: This symptom occurs when “content-scan out” is unconfigured after router runs continuously for around two days.

  Workaround: There is no workaround.

- CSCty59104

  Symptom: For the following objects the ASCII characters that can not be configured from CLI can be configured from SNMP:

  ```
  sysStreetAddress
  callHomeCustomerId
  callHomeContractId
  callHomeSiteId
  callHomeDestProfileName
  ccmDiagSignatureProfile
  ccmAaaAuthUserName
  ```

  Conditions: No special conditions are needed.

  Workaround: There is no workaround.

  More Info: The issue has been fixed in Cisco IOS software releases 15.1(1)SY and later releases.

- CSCty59423

  Symptom: 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

  Symptom: Potential memory leak is seen when handling DNS lookup response.

  Conditions: This symptom occurs when handling DNS lookup response.

  Workaround: There is no workaround.

- CSCtz07902

  Symptom: Standby RP crashes.

  Conditions: The symptom is observed in a scaled setup with redundant RP, and with a BFD configuration on the interfaces.

  Workaround: There is no workaround.

- CSCtz53214

  Symptom: The “clear counter pseudowire <#>” commands do not clear the pseudowire specific counters.

  Conditions: This symptom is reported to be present in all Cisco IOS Release 15.X(S) versions.

  Workaround: Issuing global clear count (“clear counters”) will clear counters including pseudowire specific counters.

- CSCtz90697

  Symptom: EIGRP authentication is not working.

  Conditions: The symptom is observed when authentication is configured with key-id 0.

Workaround: Use any other key-id for authentication.

- CSCua05196

  Symptom: After the reload command is entered, the router gets crashed.

  Conditions: This symptom occurs when SSH traffic is sent.

  Workaround: Enable the warm reboot command.

- CSCua21049

  Symptom: The recursive IPv6 route is not installed in the multicast RPF table.

  Conditions: This symptom occurs in the multicast RPF table.

  Workaround: There is no workaround.

- CSCua50247

  Symptom: Dropped ping packets on an NM-16ESW module.

  Conditions: The symptom is observed with ping packets with a size between 1501-1524 and between NM-16-ESW modules.

  Workaround: There is no workaround.

- CSCua73191

  Symptom: Anyconnect fails to work with IOS SSL VPN and reports the following message:

  ```
  The AnyConnect package on the secure gateway could not be located. You may be
  experiencing connectivity issues. Please try connecting again
  ```

  Conditions: The issue was seen after upgrading to Cisco IOS Release 15.2(3)T.

  Workaround: Connecting via the portal might help.

- CSCua75781

  Symptom: CME reloads for E911 call ELIN translation for incoming FXS/FXO trunk.

  Conditions: The symptom is observed from Cisco IOS interim Release 15.3(0.2)T.

  Workaround: There is no workaround.

- CSCub10950

  Symptom: The router crashes when an MR-APS switch is made. The crashes occur randomly.

  Conditions: This symptom occurs when the MLP is configured with 12 links.

  Workaround: There is no workaround.

- CSCub12694

  Symptom: Interrupt scheduler tracebacks seen.

  Conditions: Examples of log messages seen:

  Example 1:

  ```
  %SYS-2-INTSCHED: 'may_suspend' at level 4  -Process= "IP SNMP", ipl= 4, pid= 429
  -Traceback= <traceback information>
  %SYS-2-INTSCHED: 'may_suspend' at level 4  -Process= "IP SNMP", ipl= 4, pid= 429
  -Traceback= <traceback information>
  ```

  Example 2:

  ```
  %SYS-2-INTSCHED: 'may_suspend' at level 2 , all interrupts disabled -Process= "IP
  SNMP", ipl= 2, pid= 338
  -Traceback= <traceback information>
  %SYS-2-INTSCHED: 'may_suspend' at level 2 , all interrupts disabled -Process= "IP
  SNMP", ipl= 2, pid= 338
  ```

```
-Traceback= <traceback information>
%SYS-2-INTSCHED: 'may_suspend' at level 2 , all interrupts disabled -Process= "IP
SNMP", ipl= 2, pid= 338
-Traceback= <traceback information>
%SYS-2-INTSCHED: 'may_suspend' at level 2 , all interrupts disabled -Process= "IP
SNMP", ipl= 2, pid= 338
-Traceback= <traceback information>
%SYS-3-MGDTIMER: Timer has parent, timer link, timer = 16482930. -Process= "IP SNMP",
ipl= 2, pid= 338
-Traceback= <traceback information>
```

In some cases the tracebacks MAY lead to a software forced reload.

Workaround: There is no workaround.

- CSCub18622

  Symptom: 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 occurs when auth proxy is configured on a tunnel interface.

  Workaround: Move the auth-proxy rules onto a physical interface.

- CSCub28997

  Symptom: Cisco 4400 crashes with 2000 crypto sessions (4000 IPsec SAs) upon repeatedly clearing and reestablishing the SAs.

  Condition: This symptom is observed when the router is configured with 1K VRFs and 1K virtual templates, and the crypto sessions are repeatedly cleared or reestablished.

  Workaround: There is no workaround.

- CSCub34534

  Symptom: A basic call between two SIP phones over SIP trunk (KPML-enabled) fails.

  Conditions: This symptom is observed with Cisco ISR G2 platforms.

  Workaround: There is no workaround

- CSCub46423

  Symptom: Connecting from Windows 7 L2TP/IPSec client to the VPN fails when using HSRP virtual IP as a gateway IP and Error 788 is displayed.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T or later releases, and the Windows 7 L2TP/IPsec VPN client.

  Workaround: Downgrade to Cisco IOS Release 15.1(3)T.

- CSCub53380

  Symptom: Legitimate PPP frames are dropped on an async interface, incrementing both “runts” and “unknown protocol drops” in the **show interfaces** command.

  Conditions: This issue is observed with Cisco ISR G1/G2 platforms running Cisco IOS Release 15.x with the following modules.

  - HWIC-4A/S
  - HWIC-8A/S-232
  - HWIC-8A
  - HWIC-16A

  Workaround: There is no workaround.

- CSCub56064

  Symptom: Ping fails after doing EZVPN client connect if CEF is enabled.

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(0.8)T image. This issue is seen only for a specific topology, where the in/out interface is the same.

  Workaround: There is no workaround.

- CSCub56842

  Symptom: 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, do as follows:

```
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 <<<
```

- CSCub59447

  Symptom: A packet can loop forever in the code due to wrong switching vector overwritten by ISM VPN.

  Conditions: The symptom is observed with ISM VPN + VTI configuration, and when you apply and remove a crypto map from the physical interface which sources the VTI.

  Workaround: Disable ISM VPN or remove the crypto map from the physical interface and reload the router.

- CSCub71162

  Symptom: The VLAN interface is not working.

  Conditions: This symptom occurs because of a change in the netmask.

  Workaround: Shut/no shut resolves the interface.

- CSCub76103

  Symptom: When callback tries to send message there is traceback.

  Conditions: The symptom is observed when you set the call-home profile's transport to HTTP and but you do not set the HTTP address.

  Workaround: When you set the call-home profile's transport to HTTP, ensure the HTTP address value is also set correctly. For example, in call-home profile mode:

```
destination address http https://example.xxx.xxx
```

- CSCub93442

  Symptom: FlexVPN client does not get assigned with IPv6 address when IPv6 address is assigned using radius attribute "addrv6".

  Conditions: This symptom is observed on assigning IPv6 using the radius attribute "addrv6".

  Workaround: Assign IPv6 address statically or use radius IPv6 pool attribute "ipv6-addr-pool".

  More Info:

  1. Radius Server is used for assigning IPv6 address to the FlexVPN clients.

2. Using radius attribute “ipv6-addr-pool” for assigning IPv6 address from a IPv6 pool defined works fine.
3. If Radius attribute “addrv6” is used to assign IPv6 address then the IPv6 address assignment fails and client sends notification with internal address failure.

- CSCub93641

  Symptom: The load balancing feature of the flex-vpn solution of Cisco IOS does not provide authentication facilities to avoid non authorized members to join the load balancing cluster. Thus, an attacker may impact the integrity of the flex-vpn system by inserting a rogue cluster member and having the load balance master to forward VPN session to it. A number of secondary effects, including black-holing of some of the VPN traffic may be triggered by this issue.

  Conditions: Flex-VPN with Load Balancing feature active

  Workaround: Using CoPP and interface access-list may be used to allow only trusted router to join the load balancer cluster

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.9:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:W/RC:C CVE ID CVE-2012-5032 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

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

- CSCub94825

  Symptom: After Cisco IOS XE bootup, there are no static reverse routes inserted as a result of applying/installing and HA crypto map. The same issue is present on the HSRP standby device, namely, the static RRI routes will not get installed in case a failover occurs. The **show cry map** command can be used to verify that RRI is enabled. The **show cry route** command can be used to determine if RRI has happened and if it has been done correctly.

  Conditions: This symptom is observed with the following conditions:

  - Cisco IOS XE Release 3.5 up to Cisco IOS XE Release 3.7
  - VRF-aware IPSec with stateless HA and static RRI
  - IPv4

  Workaround: Removing and reentering the **reverse-route static** command into the the configuration will actually trigger the route insertion.

- CSCub95261

  Symptom: The device crashes due to a bad reference count:

```
%SYS-2-CHUNKBADREFCOUNT: Bad chunk reference count, chunk 40A82BB4 data 313E2F40
refcount FFFFFFFF alloc pc 2341E7F4. -Process= "CSDB Timer process", ipl= 3, pid= 274
-Traceback= <HEX TRACEBACK HERE>
chunk_diagnose, code = 3 chunk name is CSDB 14 structu
current chunk header = 0x313E2F30 data check, ptr = 0x313E2F40
next chunk header = 0x313E2F90 data check, ptr = 0x313E2FA0
previous chunk header = 0x313E2ED0 data check, ptr = 0x313E2EE0
```

  Conditions: This symptom occurs only when IPS is enabled on the router. The likelihood of the defect increases when there is a sudden surge of concurrent short-lived flows, for example, SYN floods.

  Workaround: Disable IPS.

- CSCub95285

  Symptom: No logging messages are seen when configuring the syslog server in CLI mode until configuration mode is exited. However when unconfiguring the syslog server, syslog messages will appear within configuration mode.

  Conditions: The symptom is observed when, in CLI configuration mode, you enter the following command:

  ```
  Router(config)#logging host 1.2.3.4 transport tcp
  ```
  Workaround: There is no workaround.

- CSCub98623

  Symptom: The **show int** command output displays the input queue size as bigger the 0, and never goes down. Shut/no shut does not help as well.

  Conditions: This symptom is observed with the following conditions:

  - A Cisco IOS router actions as XOT.
  - The XOT Server becomes not reachable for sometime while the x25 client is attempting to send traffic.
  - Cisco IOS Release 12.4(24)T7, Cisco IOS Release 15.1M ,or later releases.

  Workaround: Increase the input hold queue size from default 75 to max. Monitor it periodically manually or by script and perform a planed reload when the queue size is close to max.

- CSCuc02262

  Symptom: A crash is seen at tcp_prepare_for_retransmit with the combination of IPv6 and IPv4 traffic.

  Conditions: This symptom is observed in a DMVPN setup with the Cisco 2921 acting as the spoke and the Cisco 3945e as the hub. After passing HTTP traffic using IPv4 as well as IPv6, a crash is seen on the spoke.

  Workaround: There is no workaround.

- CSCuc06307

  Symptom: When an L2TPv3 xconnect with IP interworking is configured on a Switched Virtual Interface (**interface vlan**), it may fail to pass traffic. With **debug subscriber packet error** enabled, debug messages like the following are output:

  ```
  AC Switching[Vl10]: Invalid packet rcvd in process path, dropping packet
  ```
  Conditions: This symptom has been observed in Cisco IOS Release 15.2(3)T4 and earlier.

  Workaround: There is no workaround.

- CSCuc09483

  Symptom: Under certain conditions, running a TCL script on the box, may cause software traceback and reload of the affected device.

  Conditions: Privilege 15 user may run TCL commands that may lead to an affected device reloading

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.8/3.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

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

- CSCuc10588

  Symptom: The router crashes.

  Conditions: This symptom occurs when the normalizer engine is running with the traffic being sent.

  Workaround: There is no workaround.

- CSCuc13992

  Symptom: The Cisco IOSd process crashes due to a segmentation fault in the PPP process:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = PPP Events
  ```

  The root cause for the PPP process crash is wrong IPCP option processing inside PPP control packets.

  Conditions: This symptom occurs when the BRAS functionality is configured, which includes ISG and PPPoE session termination.

  Workaround: There is no workaround.

- CSCuc25995

  Symptom: 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 occurs when IPsec is used. More precise conditions are not known at this time.

  Workaround: There is no workaround.

- CSCuc31761

  Symptom: The router crashes when GDOI groups are removed.

  Conditions: This symptom occurs when the "crypto isakmp diagnose error <no>" CLI is enabled. This CLI is now enabled by default.

  Workaround: Remove or disable the "crypto isakmp diagnose error" command.

- CSCuc41596

  Symptom: Connection to the remote server fails with "domain name" when port-forward is configured with a VRF.

  Conditions: This symptom occurs when the VRF is configured on the router and the backend server is opened over HTTP using port-forward. The link opens when accessing directly using IP, but fails when a domain name is used after configuring a domain server.

  Workaround: Configure the IP address instead of the domain name.

- CSCuc45796

  Symptom: ISM crypto engine crashes when sending a packet bigger than 16K.

  Conditions: The symptom is observed with a Cisco 1900, Cisco 2900, and Cisco 3900 with ISM crypto engine and an IPsec packet size bigger than 16k.

  Workaround: Use a packet size less than 16K.

- CSCuc47356

  Symptom: Static routes are not getting removed.

  Conditions: This symptom is observed with Smap - Smap. Removal of CLI does not remove the static route.

  Workaround: Remove the ACL before removing the SA.

- CSCuc54300

  Symptom: During an SSO or an initial bootup, standby fails and reboots again.

  Conditions: This symptom occurs when a reload or SSO is performed.

  Workaround: There is no workaround.

- CSCuc59858

  Symptom: Valid dynamic authorization requests which are not retransmissions are marked as retransmission.

  Conditions: This may occur when valid dynamic authorization requests with the same RADIUS packet identifier is sent from different source ports.

  Workaround: There is no workaround.

- CSCuc66518

  Symptom: The ISM-VPN: tlb load/fetch exception is seen on the ISM.

  Conditions: This symptom is observed with site-to-site FlexVPN traffic.

  Workaround: Use the onboard crypto or software crypto engine instead of Reventon.

- CSCuc70472

  Symptom: Compression (V.42bis, V.44) is disabled by “modemcap” for PVDM2-DM. After some time, certain modems start to negotiate V.44/V.42bis and drop those calls before PPP. The number of modems negotiating compression is growing over time, leading to an increase in the drop call rate.

  Conditions: This symptom occurs when the following modemcap is applied:

  ```
  “modemcap entry V32bis_noComp1:MSC=&F0+DCS=0,0;+MS=10,0,4800,14400”
  ```
  or

  ```
  “modemcap entry V32bis_noComp2:MSC=+MS=10,0,4800,14400;%C0”
  ```
  Breakdown:

  - “+DCS=0,0=0,0”—V.44 OFF, V.42bis OFF
  - “+MS=10,0,4800,14400”—V.32bis,No V8.bis, min 4800, max 14400
  - “%C0”—No compression

  After reload:

  ```
  Router#sh modem log 0/463 | i compression
   Data compression                69    None
   Data compression                69    None
   Data compression                69    None
   Data compression                69    None  << No compression
  Router#sh modem configuration 0/463 | i S41|S82
      S41 = 137     Compression selection is MNP 5 Retrain and fallback/fall
  forward disabled
      S82 = 128     Break Handling Options/LAPM Break Control = 0x80
      S82 = 21
  ```
  A few hours/days after reload:

  ```
  Router#sh modem log 0/463 | i compression
   Data compression                68    None
   Data compression                68    V44 << Starts to negotiate V.44, even
  while disabled by modemcap
   Data compression                68    V44
   Data compression                68    V44
  Router#sh modem configuration 0/463 | i S41|S82
      S41 = 139     Compression selection is MNP 5 and V.42 bis
      S82 = 128     Break Handling Options/LAPM Break Control = 0x80
  ```

```
S82 = 25
```

Workaround: Reload.

- CSCuc73473

  Symptom: The IPv6 default route is not redistributed in BGP (VRF).

  Conditions: This symptom occurs when the OSPFv3 “default-information originate always” is configured in the same VRF.

  Workaround: To clear the issue, enter “cle ip bg *”. To avoid the issue, remove “default-information originate always” from OSPFv3 in the respective VRF.

- CSCuc85321

  Symptom: Cisco IOS may crash when AnyConnect is used.

  Conditions: This symptom is observed with the following conditions:

  – The router is configured as the SSL VPN gateway.

  – AnyConnect users make VPN connections to this router.

  Workaround: There is no workaround.

- CSCud02391

  Symptom: The EIGRP routes are not coming up after removing and reenabling the tunnel interface.

  Conditions: This symptom is observed when EIGRP routes do not populate properly.

  Workaround: There is no workaround.

- CSCud05497

  Symptom: Rarely, the WCM fails to send the configuration to a WaasExpress device.

  Conditions: This symptom occurs when CM tries to send the configuration to a WaasExpress device. Rarely, the “SSL peer shutdown incorrectly” error is seen, leading to failure to send the configuration.

  Workaround: Go to any WAAS-EXP configuration page and click submit.

- CSCud05636

  Symptom: The MAC-address gets corrupted when user sends the multicast traffic.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M3 image, where as the same multicast traffic works as expected with Cisco IOS Release 12.4T image.

  Workaround: A possible work around is to enable the **ip pim nbma- mode** command at the CPE end.

- CSCud11078

  Symptom: Removal of the service instance on the target device causes a crash.

  Conditions: Not consistently reproducible on all configurations as the underlying cause is a race condition.

  Workaround: De-schedule the probe before removing the service instance.

- CSCud25043

  Symptom: A WebVPN-enabled gateway crashes on Cisco IOS Release 15.1(4)M5 due to SSLVPN_PROCESS.

  Conditions: This symptom is observed under the following conditions:

  – Cisco IOS Release 15.1(4)M5.

  – SSL VPN (WebVPN enabled).

Workaround: There is no workaround.

- CSCud26339

  Symptom: Changing policy-map parameters triggers a Cisco IOSd crash.

  Conditions: This symptom is observed when the policy-map is attached to a service instance on the Cisco ASR 903.

  Workaround: Remove the policy-map from the target and then make the changes.

- CSCud36208

  Symptom: The multilink ID range has to be increased from the existing 65535.

  Conditions: This symptom is observed specifically with the Cisco MWR1.

  Workaround: There is no workaround. The range is now made configurable based on PD.

- CSCud41058

  Symptom: There is a route-map which matches tags and set a new value. This route-map is used in an EIGRP outbound distribute list. One in 10 times based on the received route tag, the correct route tag value is not set while advertising out.

  Conditions: The symptom is observed when you use a route map which matches tags and sets a new tag. Used in **distribute-list route-map** *name* **out**.

  Workaround: Clear the EIGRP process or re-advertise the route.

- CSCud51791

  Symptom: 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. You may try to remove Presence from running-configuration.

- CSCud54365

  Symptom: The scansafe socket is not closed by reset from the client

  Conditions: This symptom occurs when sending a connection request from the client (SYN packet). This issue is seen when ack is sent instead of syn+ack for a syn request from the server. The client will send a Reset (RST) signal for ack received instead of syn+ack. The L4F/scansafe box displays that the flow is not closed.

  Workaround: Make sure that the server does not have a stale TCP tuple flow entry before trying for a connection from the client.

- CSCud55286

  Symptom: Traffic drops for sometime after doing a switchover.

  Conditions: The symptom is observed when a switchover is performed on a Cisco ASR 903.

  Workaround: Put a neighbor command where the neighbor has no meaning and will never be up. This will solve the timing issue.

- CSCud56450

  Symptom: PPP drops 20-40 percent of incoming frames.

  Conditions: This symptom is observed when using WIC-1B-S/T-V3 or VWIC2-xMFT-T1/E1 in PPP mode on a Cisco c1900/c2900/c3900/c3900e (or ISR G2) router.

  Workaround: Use HWIC-4B-S/T (for BRI) or the VWIC3 card (for T1/E1).

- CSCud63381

  Symptom: Switching from periodic to on-demand DPDs may cause the DPDs to fail intermittently and thus IPsec failover may not work correctly.

  Conditions: This symptom is observed under the following conditions:

  1. If you are using Cisco 7200-VSA.
  2. For Cisco IOS Release 15.1(4)M2.
  3. When on-demand DPDs are configured for IPsec failover.

  Workaround: Disable the SCTP session:

  ```
  ipc zone default
  association 1
  shutdown
  ```

- CSCud64506

  Symptom: HQF does not clear up when the bandwidth remaining ratio is misconfigured on the child policy.

  Conditions: This symptom is observed when an incorrect configuration triggers the policy rejection and fails on the cleanup with the nondefault queue-limit setting in the class-default class.

  Workaround: Apply the configuration with the correct setting.

- CSCud64870

  Symptom: DMVPN hub ASR 1004 may crash after the fetching CRL from MS CRL server.

  Conditions: The crash occurs when there are five 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.

- CSCud65150

  Symptom: The device might crash randomly due to an address error, as follows:

  ```
  16:14:04 CST Fri Nov 30 2012: Address Error (load or instruction fetch) exception, CPU
  signal 10, PC = 0x22895480
  ```

  Conditions: This symptom was first seen on a Cisco 2911 router. The crash is triggered randomly some time after a Kron Policy runs a TCL script:

  ```
  kron occurrence ipchange in 5 recurring system-startup
         policy-list tcl_script

       kron policy-list ipchange
         cli tclsh flash:/SCRIPT.tcl
  ```

  The exact conditions are still being investigated. The exact trigger is not yet known.

  Workaround: Remove the Kron configurations from the system.

- CSCud66669

  Symptom: On the Cisco 7200, the tunnel is established correctly and encryption and decryption occur correctly. However, after decryption, the packet is not punted to the iVRF in which the tunnel interface resides, leading to a broken IPsec-DataPath.

  Conditions: This symptom is observed with the Cisco 7200 with VSA under the following conditions:

  - Tunnel (GRE/mGRE) in an iVRF with Tunnel protection configuration.
  - iVRF not equal to fVRF.

Workaround: This issue has been observed with Cisco IOS Release 15.0(1)M9 and Cisco IOS Release 12.4(24)T8, so downgrade might be an option. There is no known configuration-related workaround yet, although software crypto will work just fine.

- CSCud67105

  Symptom: 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 seen only when CSCuc45115 is already in image.

  Workaround: There is no workaround.

- CSCud67796

  Symptom: No audio and/or no ringback with SIP calls through ZBFW when relying on SIP ALG to open pinholes/pregenerate sessions for RTP.

  Conditions: The symptom is observed with the following conditions:

  1. ZBFW configured to inspect SIP.
  2. No other means to permit RTP traffic in other ZBFW classes/policies.
  3. RTP is opened/negotiated/established by SDP in 180 Ringing and SDP in PRACK.

  Workaround: Modify ZBFW policy to allow RTP port range through. Either inspect all UDP or write more specific classes to allow RTP between only necessary endpoints.

- CSCud68178

  Symptom: The Cisco ASR 1000 series router and Cisco ISR 4400 series hubs crash.

  Conditions: This symptom occurs when the physical and tunnel interface are flapping.

  Workaround: There is no workaround.

- CSCud70577

  Symptom: RTSP traffic is being dropped with NAT (PAT) and NBAR.

  Conditions: The issue is seen when protocol-disc (cisco-ip-camera or realmedia) and NAT is enabled on the same interface.

  Workaround: Disable NBAR feature.

- CSCud72625

  Symptom: Router experiences high CPU due to interruptions and queues when the VSA starts to fill.

  Conditions: The symptom is observed with the following conditions:

  - Cisco 7200 NPE-G2 with VSA module for encryption.
  - Crypto map or tunnel protection mode applied to an interface to send traffic to VSA.

  Workaround: Disable the VSA module. The **test pas vsa reset 0 2000** command resets the VSA module.

- CSCud78362

  Symptom: GW starts to drop calls randomly if you increase simultaneous calls beyond 350.

  Conditions: This symptom occurs 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. A patch was provided which fixed the issue.

- CSCud79067

  Symptom: The BGP MIB reply to a getmany query is not lexicographically sorted.

  Conditions: This symptom is observed when IPv4 and IPv6 neighbor IP addresses are lexicographically intermingled, for example, 1.1.1.1, 0202::02, 3.3.3.3.

  Workaround: There is no workaround.

- CSCud83835

  Symptom: 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 occurs when all of the following conditions are met:

  1. The crypto map is configured on a Virtual-Template interface.
  2. This Virtual-Template interface is configured with “ip address negotiated”.
  3. 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.

- CSCud86856

  Symptom: The router crashes soon after executing “clear policy-firewall sessions”.

  Conditions: This symptom is observed with ZBF, and only with a large number of sessions.

  Workaround:

  1. Do not use the **clear firewall-policy sessions** command.
  2. Increase the IO memory size using “memory-size iomem 25” (use the right percentage depending on your free processor memory) and reload. However, you may still notice CPU hogs when executing “clear policy-firewall sessions”.

- CSCud86954

  Symptom: Some flows are not added to the Flexible Netflow cache, as indicated by the “Flows not added” counter increasing in the **show flow monitor statistics** command output. “Debug flow monitor packets” shows “FNF_BUILD: Lost cache entry” messages, and after some time, all cache entries are lost. At that moment, debug starts showing “FLOW MON: ip input feature builder failed on interface couldn’t get free cache entry”, and no new entries are created and exported (“Current entries” counter remains at 0).

  The following is sample output when all cache entries are lost:

```
Router#sh flow monitor FNF-MON stat
  Cache type:                               Normal
  Cache size:                                 4096
  Current entries:                               0
  High Watermark:                              882

  Flows added:                               15969
  Flows not added:                           32668
  Flows aged:                                15969
    - Active timeout      (  1800 secs)          0
    - Inactive timeout    (    15 secs)      15969
    - Event aged                                 0
    - Watermark aged                             0
    - Emergency aged                             0
```

  Conditions: This symptom occurs when all of the following are true:

  - Flexible Netflow is enabled on a DMVPN tunnel interface.

  - Local policy-based routing is also enabled on the router.
  - Local PBR references an ACL that does not exist or an ACL that matches IPsec packets.

  Workarounds:

  1. Make sure that the ACL used in the local PBR route-map exists and does not match IPsec packets sent over the DMVPN tunnel interface.
  2. Disabling encryption on the tunnel interface, or changing tunnel mode from mGRE to GRE also removes this bug.
  3. The issue will not be seen if FNF is not configured, or if FNF is configured but is not monitoring VPN traffic.

- 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**.

- CSCud90568

  Symptom: The Input queue of an interface shows 76/75. In “show buffers input-interface interface packet”, you will find UDP packets with the port used by DTLS.

  Conditions: This symptom is observed with SSLVPN with DTLS enabled (it could be enabled by default, depending on the platform).

  Workaround: Disable DTLS. Reload.

- CSCud95940

  Symptom: A Cisco 3900 running with CME and Skinny phones could experience CPU hogs and a watchdog, resulting in a crash.

  ```
  %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  (630/222),process = Skinny Msg Server. -Traceback= 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX
  0xXXXXXXXX %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Skinny Msg
  Server. -Traceback= 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX
  ```

  Conditions: This symptom is observed with Cisco 3900 running with CME and Skinny phones.

  Workaround: There is no workaround.

- CSCud96075

  Symptom: A router running Cisco IOS Release 15.2(4)M2 will reload with a bus error soon after the DSP reloads when there is a live transcoding session.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(4)M2.

  Workaround: There is no workaround.

- CSCue01721

  Symptom: The ISM-VPN stops with clear session of DMVPN tunnels.

  Conditions: This symptom is observed with site-to-site DMVPN is enabled.

  Workaround: Use the onboard crypto or software crypto engine instead of Reventon.

- CSCue03316

  Symptom: The box crashed during scale testing.

Conditions: During scale testing, the box runs out of memory resulting in MALLOCFAIL. Memory malled is not checked for failure resulting in crash.

Workaround: There is no workaround.

- CSCue06309

  Symptom: A Cisco 2900 series router running Cisco IOS Release 15.2(4)M1 may generate the following error message:

  ```
  SYS-2-BADPOOL Attempt to use buffer with corrupt pool pointer, ptr= xxxxxxxx, pool=
  D0D0D0D -Process= "IGMP Snooping Receiving Process", ipl= x, pid= xxx"
  ```

  This results in memory fragmentation and a low memory condition in the IO pool.

  Conditions: This symptom occurs when IGMP is enabled on the router.

  Workaround: There is no workaround. The router needs to be proactively reloaded to reclaim the memory.

- CSCue13902

  Symptom: When using OTP challenge authentication the OTP password challenge is never displayed to the client.

  Conditions: The symptom is observed with the following conditions:

  - IOS SSLVPN.
  - Cisco IOS Release 15.2.x.

  Workaround: There is no workaround.

- CSCue18133

  Symptom: The Cisco 7600 Router crashes at show_li_users.

  Conditions: This symptom is observed under the following conditions: In li-view, create an username: lawful-intercept and li_user password: lab1. Then, attempt its delete by “no username li_user”. Later, show users of LI.

  Workaround: There is no workaround.

- CSCue25575

  Symptoms : The crash is observed for SDP pass through or call forward or antitrombone cases.

  Conditions: The crash is observed for a basic call involving SDP pass through or call forward or antitrombone cases.

  Workaround: There no workaround.

- CSCue26213

  Symptom: The connected interface that is enabled for EIGRP will not be redistributed into BGP.

  Conditions: This symptom occurs when the prefix of the connected interface is in the EIGRP topology table with “redistribute eigrp” under BGP address-family IPv4.

  Workaround: Redistribute the connected interface and EIGRP.

- CSCue28318

  Symptom: A Cisco router doing authentication proxy may unexpectedly reload when running the **test aaa command** command.

  Conditions: This symptom occurs when the router is using LDAP authentication and has a misconfigured LDAP authentication configuration.

  Workaround: Correct the misconfiguration.

- CSCue31321

  Symptom: A Cisco router or switch may unexpectedly reload due to bus error or SegV when running the **how ip cef ... detail** command.

  Conditions: This symptom is observed when the output becomes paginated (---More---) and the state of the CEF adjacency changes while the prompt is waiting on the more prompt.

  Workaround: Set "term len 0" before running the **how ip cef ... detail** command.

- CSCue32350

  Symptom: Crash after removing the Kron occurrence.

  Conditions: The symptom is observed when multiple Kron occurrences are configured to be triggered at the same time.

  Workaround: There is no workaround.

- CSCue33313

  Symptom: A Cisco ASR repeatedly produces a "no-input" event despite inputs provided by caller.

  Conditions: The symptom is observed with the following conditions:

  - 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.

- CSCue36197

  Symptom: The Cisco 7600 router may crash while performing the NSF IETF helper function for a neighbor over a sham-link undergoing NSF restart.

  Conditions: This symptom occurs when a router is configured as an MPLS VPN PE router with OSPF as PE-CE protocol. OSPF in VRF is configured with a sham-link and a neighbor router over a sham-link is capable of performing an NSF IETF restart on sham-links.

  Note: This problem cannot be seen if both routers on sham-link ends are Cisco IOS routers.

  Workaround: Disable the IETF Helper Mode protocol by entering the following commands:

```
enable
  configure terminal
  router ospf process-id [vrf vpn-name]
  nsf ietf helper disable
```

```
end
```

Note: Disabling Helper Mode will result in an OSPF peer dropping adjacency if the peer is reloaded.

- CSCue36321

  Symptom: A crash occurs when MLP is configured.

  Conditions: This symptom is observed with an MLP configuration.

  Workaround: There is no workaround.

- CSCue39206

  Symptom: ES crashes after the second 401 challenge.

  Conditions: This symptom occurs 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.

- CSCue39518

  Symptom: A Cisco 7200 with VSA fails to encrypt traffic under specific conditions.

  Conditions: The symptom is observed under the following conditions:

  - Cisco 7200 has IPsec SSO configured with HSRP. Dynamic crypto map is configured. Remote sides have static crypto map to this device.
  - All the 15.x codes to the latest Cisco IOS 15.2(4)M2 are affected.
  - Issue is not seen in the Cisco IOS 12.4 codes.
  - Issue not seen when IPsec SSO and HSRP are removed.

  Workaround: There is no workaround.

- CSCue40304

  Symptom: Some senders could not be found in the **show ip rsvp sender vrf** <*vrf_name*> command output.

  Conditions: This symptom is observed on configuring senders on spokes when using Refresh Reduction.

  Workaround: Turn off refresh reduction and **clear ip rsvp sender ***

- CSCue45934

  Symptom: This problem is specific to the Catalyst 6000 platform. With IPv4 crypto map, ICMP echo reply is not triggered from the remote end.

  Conditions: This symptom is observed in IPv4 crypto map configuration and Catalyst 6000 platform.

  Workaround: There is no workaround.

- CSCue48254

  Symptom: After an upgrade from Cisco IOS Release 15.0M to Cisco IOS Release 15.2M, the CPU usage with the same traffic load is increased.

  Conditions: This symptom is observed with the Cisco ISR-G2 platform.

  Workaround: There is no workaround.

- CSCue49424

  Symptom: The device crashes repeatedly on bootup.

Conditions: This symptom occurs due to a Kron job that runs on bootup. The Kron job invokes a chat-script that unlocks a cellular card.

Workaround: Use EEM instead of Kron.

- CSCue49632

  Symptom: TCP closes connection for DLSw peer without calling dlsw_tcpd_fini.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(4)M4, dlsw_tcpd_fini is not called and DLSw times out. When you close the remaining TCP connections and the DLSw peer FSM cycles back to disconnected. This issue is seen only when TCP FIN is received.

  Workaround: Set the higher IP address on 7206 VXR router.

- CSCue52864

  Symptom: When the Output Service policy is applied to the serial links of the HWIC-xCE1T1-PRI card, the serial links bounce.

  Conditions: This symptom is observed with the following conditions:

  1. When more than two channel groups are applied to the same controller port.
  2. When the serial links are congested.
  3. When the Output Service policy is applied to more than two serial links of the same controller port.

  Workaround: Do not apply the Output Service policy.

- CSCue53686

  Symptom: The ISM Encryption module consumes fragmented packets that need further fragmentation prior to encryption when using a crypto map.

  Conditions: This symptom is observed with a LAN-to-LAN crypto map-based IPsec tunnel. A large IP fragment traverses the IPsec tunnel but it needs to be fragmented prior to encryption.

  Workaround: Disable the ISM module and use the onboard crypto engine.

- CSCue54104

  Symptom: A crash is seen intermittently.

  Conditions: This symptom occurs after 60+ PRI calls take place. The exact conditions are still being investigated.

  Workaround: There is no known workaround. Downgrade to Cisco IOS Release 15.1(4)M3 or earlier releases.

- CSCue55739

  Symptom: PfR MC/BR session may be flapped, if PfR learn is configured with scale configuration.

  Conditions: This symptom may be observed, if PfR traffic-classes are learned by PfR global **learn** configuration.

  Workaround: Disable PfR global **learn** by configuring **traffic-class filter access-list** pointing to the **deny ip ip any** ACL, and configure PfR learn “list”.

- CSCue59775

  Symptom: The device crashes.

  Conditions: This symptom is observed when the service-policy is removed.

  Workaround: There is no workaround.

- CSCue61691

  Symptom: In a dual-homing topology, switching from the backup mode to the nominal mode ends up with the active “source” router sending a data MDT but transmitting on the default MDT.

  Conditions: The symptom is observed on a dual-homing topology with CORE GRE tunnel.

  Workaround: Use the following command:

  ```
  clear ip mroute vrf <>
  ```
- CSCue62292

  Symptom: The router crashes with an address error with the following messages before the crash:

  ```
  Di0 DDR: dialer shutdown complete
  %DIALER-6-BIND: Interface Vi3 bound to profile Di0
  %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
  %LINK-3-UPDOWN: Interface Virtual-Access3, changed state to up
  %DIALER-6-UNBIND: Interface Vi3 unbound from profile Di0

  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x22473FA0
  ```
  Conditions: This symptom is observed when a dialer interface is unbound.

  Workaround: There is no workaround.
- CSCue65130

  Symptom: cmCallerID in CISCO-MODEM-MGMT-MIB is not updated when there is no CallerID.

  Conditions: This symptom is observed where incoming calls with no CID (Caller-ID) do not update the cmCallerID entry in the CISCO-MODEM-MGMT-MIB. When a call with no CID arrives, the CID from the previous caller stays in the MIB, which leads to an authentication bypass and produces billing errors.

  Workaround: There is no workaround.
- 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.
- CSCue65498

  Symptom: Wrong CIR is getting cloned to the VA interface.

  ```
  Dialer1
     Service-policy output: OPT3-DIALER-4b-TR25
       Class-map: CRI-OUT (match-any)
         police:
             cir 8 %
             cir 819000 bps, bc 25593 bytes           <<<<<

    Virtual-Access3
     Service-policy output: OPT3-DIALER-4b-TR25
       Class-map: CRI-OUT (match-any)
         police:
             cir 8 %
             cir 8000000 bps, bc 250000 bytes         <<<<<
  ```
  Conditions: This symptom is observed with the PPPoE dialer/client configuration.

  Workaround: Remove and reapply the service-policy under the dialer interface.
- CSCue68127

  Symptom: A Cisco 3845 router will crash due to IO memory corruption.

Conditions: This symptom occurs when WebVPN is enabled and the router receives a TLS hello packet from the server.

Workaround: There is no workaround.

- CSCue68761

  Symptom: A leak in small buffer is seen at ip_mforward in Cisco IOS Release 15.1(4)M3. Device: Cisco 2911 Cisco IOS: c2900-universalk9-mz .SPA.151-4.M3.bin

  Conditions: This symptom is observed with the Cisco 2911 running Cisco IOS Release 15.1(4)M3.

```
------------------ show buffers ------------------


Buffer elements:
     156 in free list (500 max allowed)
     11839912 hits, 0 misses, 617 created

Public buffer pools:
Small buffers, 104 bytes (total 45187, permanent 50, peak 45187 @ 10:04:00):
     0 in free list (20 min, 150 max allowed)
     7968057 hits, 202704 misses, 2128 trims, 47265 created
     71869 failures (680277 no memory)

------------------ show buffers usage ------------------


Statistics for the Small pool
Input IDB    :        Mu1 count:    45180
Caller pc    : 0x22CF95C4 count:    45180
Resource User:   IP Input count:    45180
Caller pc    : 0x22381654 count:        2
Resource User:       Init count:        2
Output IDB   :        Mu1 count:        4
Caller pc    : 0x2380114C count:        4
Resource User: PIM regist count:        4
Number of Buffers used by packets generated by system: 45187
Number of Buffers used by incoming packets:

++++++++++++++++++++++++++++small buffer
packet++++++++++++++++++++++++++++++++

<snip>

Buffer information for Small buffer at 0x2A815220
  data_area 0xD9DEB04, refcount 1, next 0x0, flags 0x2080
  linktype 7 (IP), enctype 16 (PPP), encsize 2, rxtype 1
  if_input 0x30F21520 (Multilink1), if_output 0x0 (None)
  inputtime 00:02:46.212 (elapsed 05:55:11.464)
  outputtime 00:01:22.632 (elapsed 05:56:35.044), oqnumber 65535
  datagramstart 0xD9DEB56, datagramsize 38, maximum size 260
  mac_start 0xD9DEB56, addr_start 0x0, info_start 0xD9DEB58
  network_start 0xD9DEB58, transport_start 0xD9DEB6C, caller_pc 0x22CF0044

  source: 10.131.124.33, destination: 224.0.1.40, id: 0x55F0, ttl: 11,
  TOS: 192 prot: 17, source port 496, destination port 496

0D9DEB56:                    002145C0 002455F0          .!E@.$Up
0D9DEB5E: 00000B11 F14C0A83 7C21E000 012801F0  ....qL..|!`..(.p
0D9DEB6E: 01F00010  82211200  00000000 000000    .p...!.........

Workaround: There is no known workaround. Reboot frees up memory.
CSCue69527
```

```
Symptom: More than 95 SCCP controlled FXS ports cannot be configured on the Cisco
VG350.
The debug output for "debug ccm-manager config-download errors" is as follows:
cmapp_sccp_gw_start_element_handler: warning - max number of interfaces reached.
Conditions: This symptom occurs when configuring more than 95 SCCP FXS ports on the
Cisco VG350 using CUCM.
```

Workaround: There is no workaround.

- CSCue71921

  Symptom: A crash is seen when WAAS Express is enabled and the **show waas auto-discovery list** command is issued.

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 13:37:19 CST Wed Feb 13 2013 addr=0x0,
  pc=0x23E18C9Cz , ra=0x23E18C90z , sp=0xC1C5E9D8
  %ALIGN-1-FATAL: Illegal access to a low address 13:37:19 CST Wed Feb 13 2013 addr=0x0,
  pc=0x23E18C9Cz , ra=0x23E18C90z , sp=0xC1C5E9D8
  TLB (store) exception, CPU signal 10, PC = 0x23E26A9C
  ```

  Conditions: This issue occurs after entering the **show waas auto-discovery list** command with connections being optimized by CIFS Express Accelerator or WAAS Express.

  Workaround: There is no workaround.

- CSCue75404

  Symptom: Files beyond a certain size with certain websites such as yahoo.com cannot be attached.

  Conditions: This symptom is observed with files beyond a certain size.

  Workaround: There is no workaround.

- CSCue76102

  Symptom: 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.

- CSCue77265

  Symptom: Increment memory leaks are seen at IPSec background proc.

  Conditions: This symptom occurs when “clear cry session” is issued multiple times when bringing up the tunnel.

  Workaround: There is no workaround.

- CSCue81327

  Symptom: Standby RP crashes during bulk sync with:

  ```
  Unexpected exception to CPU: vector 1400
  ```

  Conditions: The crash occurs while syncing a shutdown TE tunnel interface configuration.

  Workaround: Delete the shutdown TE tunnel configuration, if not required.

- CSCue85737

  Symptom: 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.

- CSCue88659

  Symptom: When installing a new signature file, a router reports traceback or crash with Cisco IOS-IPS.

  Conditions: This symptom occurs when installing a new signature file.

  Workaround: There is no workaround.

- CSCue89019

  Symptom: Datapath is broken since the traffic exit via a wrong VRF.

  Conditions: This symptom is observed with the following conditions:

  - VRF-aware IPsec.
  - ISM module enabled.
  - Hub or Spoke is located behind NAT

  Workaround: If there is nat between the client and the hub, you must disable ISM and use the onboard crypto engine instead.

  Make sure there is no nat between the client and the hub

- CSCue92705

  Symptom: The “DHCPD Receive”, “CDP Protocol”, and “Net Background” processes leaks could be seen after disabling “macro auto monitor”.

  Conditions: This symptom is observed in Cisco IOS 15.0(2)SE1 Release, 2960S, dhcp, cdp traffic, and link flapping.

  Workaround: Configure “no service dhcp” if the switch is not a DHCP server. Configure:

  ```
  device-sensor filter-spec cdp exclude all
  device-sensor filter-spec dhcp exclude all
  device-sensor filter-spec lldp exclude all
  ```

- CSCue94880

  Symptom: RTP traffic fails in reverse direction when an outside source list is configured and RTP SA IP matches against this list.

  Conditions: The symptom is observed with a Cisco IOS version above 12.4(9) mainline.

  Workaround: Use Cisco IOS Release 12.4(9).

- 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 causecode 16** command to clear the dangling call. More Info:

- CSCue98812

  Symptom: No syslog message when you exit a TTY session.

  Conditions: The symptom is observed when you exit a TTY session (from telnet or SSH, etc).

  Workaround: There is no workaround.

- CSCuf09006

  Symptom: Upon doing a **clear ip bgp * soft out** or **graceful shutdown** on a PE, all VPNv4/v6 routes on an RR from this PE are purged at the expiry of enhanced refresh stale-path timer.

  Conditions: The symptom is observed with the following conditions:

  1. PE must have BGP peering with at least one CE (VRF neighbor) and at least one RR (VPN neighbor).
  2. PE must have a rtfilter unicast BGP peering with the RR.
  3. IOS version must have “Enhanced Refresh” feature enabled.
  4. A **clear ip bgp * soft out** or **graceful shutdown** is executed on the PE.

  Workaround: Instead of doing **clear ip bgp * soft out**, do a route refresh individually towards all neighbors.

- CSCuf36446

  Symptom: Router crashes during processing of the following CLI:

  ```
  (conf) no metadata flow
  ```

  Conditions: The symptom is observed with a moderate scale of metadata flows, using several different interfaces.

  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.

- CSCuf62756

  Symptom: If **bandwidth qos-reference** *value* is configured on an interface which bandwidth can change, then the actual interface bandwidth will be used for QoS service-policy validation when the interface bandwidth changes. This can result in a service-policy being removed if the interface bandwidth is insufficient to meet the requirements of the service-policy, such as bandwidth guarantees.

  Conditions: Affects variable-bandwidth interfaces such as EFM interfaces or PPP multilink bundles.

Workaround: Use proportional actions in the QoS service-policy, such as “police rate percent....”, “bandwidth remaining ratio...”, “bandwidth remaining percent...”, and “priority percent”.

Workaround 2: You can configure **bandwidth qos-reference** with maximum bandwidth of the interface:

```
interface Ethernet0
 bandwidth qos-reference <max bandwidth of interface>
```

This can prevent policy-map detached due to interface bandwidth change.

- 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. More Info:

- CSCuf93606

  Symptom: A Cisco 3945E router crashes.

  Conditions: The symptom is observed with the following conditions:

  - Extension mobility is configured for the phone. The logout profile should not be configured with any number.
  - In the logged out state, user has to press the “NewCall” softkey followed by dialing any digit between 1-9 (excluding 0).
  - Instead of pressing “dial” softkey, press “AbbrDial” softkey.

  Workaround: Have a proper number configured under the logout profile.

- CSCuf93964

  Symptom: The fix for CSCty56830 has introduced a buffer overrun error and is breaking static analysis for a number of SNMP clients in t_base_3. Potentially, it could cause a crash. Specifically, in the definition of the SnmpTrapParm_ structure the fix changed the definition of enterprise from:

  ```
  const OID* enterprise;
  ```

  to:

  ```
  OID enterprise[SNMP_TRAPSTRING_SIZE];
  ```

  In other words instead of being a pointer to an OID structure it is now an _array_ of 120 OID structures. Also, in SnmpSendTrapInternal() it changed the initialization of the enterprise OID field in the trapbuffer from:

  ```
  trapBuffer->enterprise = enterprise;
  ```

  Conditions: The symptom is observed while sending custom traps.

  Workaround: memcpy(trapBuffer->enterprise, enterprise, SNMP_TRAPSTRING_SIZE).

- CSCug00841

  Symptom: When a Cisco router is running with Cisco IOS Release 15.2(4)M3 software for L2VPN pseudowire redundancy on the frame relay, if the primary pseudowire goes down, and backup pseudowire is activated, the connection remains in OPER DOWN state and traffic is not able to go through.

  Conditions: This issue occurs with frame relay to pseudowire local connect with backup pseudowire.

  Workaround: There is no workaround.

- CSCug04187

  Symptom: Build breakage.

  Conditions: Due to CSCuf62756.

Workaround: There is no workaround.

- CSCug17820

  Symptom: Random crashes are seen pointing to managed timer in L4F component.

  Conditions: The symptom is observed during scansafe traffic.

  Workaround: Disable the scansafe feature.

- CSCug28904

  Symptom: 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.

- CSCug34507

  Symptom: Traffic decrypted on a Cisco ISR G2 series is process switched instead of staying in the CEF path.

  Conditions: The symptom is observed when the hub and/or the spoke are located behind NAT or PAT.

  Workaround: Disable NAT/PAT.

- CSCug37242

  Symptom: 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.

- CSCug43453

  Symptom: Cellular interface not able to establish a call.

  Conditions: The symptom is observed after router bootup or reload, with an EHWIC-4G-LTE-G card and 03.05.19.04 modem firmware.

  Workaround: Power-cycle or reset the modem.

- 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.

- CSCug52119

  Symptom: A RIB route is present for a prefix, but the router continues to LISP encapsulate.

  Conditions: The symptom is observed when a LISP map-cache existed for a prefix and then the RIB route was added later.

  Workaround: Use the following command:

  ```
  clear ip/ipv6 lisp map-cache <prefix>
  ```

- 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.

- CSCug92144

  Symptom: ISAKMP SA negotiation is not successful on the UUTs.

  Conditions: The symptom is observed when **show crypto isakmp sa** is given while checking for the state as OM_IDLE, the state is actually MM_NO_STATE.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(4)M3

- CSCug55040

  Symptoms: The cellular interface stops sending or receiving traffic due to modem crash.

  Conditions: This symptom is observed when bi-directional iMIX traffic is sent from test center with 5 Mbps Uplink and 12 Mbps Downlink. Traffic is sent normally for about an hour, then the modem/IOS get heart beat timeout and traffic stop sending.

  Workaround: The modem recovers automatically if the link recovery is turned ON.

- CSCug22606

  Symptoms: The cellular interface become non-responsive due to the Software Development Kit crash.

  Conditions: This symptom is observed when the network connection (data bearer) to the SP is reset multiple times in very short duration (multiple resets per minute), the Cisco router cellular interface becomes unresponsive and hangs causing the Software Development Kit driving the modem to crash. A router reload is required to recover from it.

  Workaround: Reload the Cisco router. Optionally,

  - Modify the “embedded link recovery monitor-time” parameter from 20 seconds to 60 seconds.
  - Modify the cellular controller “lte modem link-recovery monitor-timer” from 20 to 60 seconds.
  - For C819G-4G-V-K9, modify the cellular interface “dialer enable-timeout” from 15 to 60 seconds.

Resolved Caveats—Cisco IOS Release 15.2(4)M3

- 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 message:

  ```
   ...  cnonce="305EE7FF",qop="auth",algorithm=MD5,nc=0000000A
  ```

  Workaround: There is no workaround.

- CSCtg82170

  Symptoms: The IP SLA destination IP/port configuration changes over a random period of time. This issue is hard to reproduce but has been reported after upgrading to Cisco IOS Release 15.1(1).

  So far, it only seems to have affected the destination IP and port. The destination IP may be changed to an existing destination IP that has already been used by another probe. The destination port is sometimes changed to 1967 which is reserved for IP SLA control packets. Other random destination ports have also been observed to replace the configured port for some of the IP SLA probes.Each time when the change happens, many of the IP SLA probes will stop running.

  Conditions: This symptom is observed in Cisco IOS Release 15.1(1)XB and Cisco IOS Release 15.1(1)T. Other Cisco IOS versions may also be affected.

  Workaround: A possible workaround is to downgrade to any Cisco IOS versions older than Cisco IOS Release 15.1.x.

- CSCtn15610

  Symptoms: Cisco IOS may crash with a bus error accessing addr=0x0 after DSP reset.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T13a engineering special and 12.4(24)T4 version.

  Workaround: There is no workaround at this time.

- CSCtn16281

  Symptoms: Mesh AP crashes on BVI restart by DHCP.

  ```
  *Feb 9 04:00:45.911: %MESH-6-ADJ_VIDB_LINK: Mesh neighbor 0021.1bc0.XXXX VIDB
  Virtual-Dot11Radio2 dot1x control *Feb 9 04:01:03.199: %DHCP-5-RESTART: Interface BVI1
  is being restarted by DHCP
  *Feb 9 04:01:06.023: %MESH-6-CAPWAP_RESTART: Mesh Capwap re-started
  === Start of Crashinfo Collection (04:01:06 UTC Wed Feb 9 2011) ===
  ```

  Conditions: This symptom is a corner case and is a low probability crash.

  Workaround: There is no workaround. AP will reload and rejoin the controller.

- CSCto87436

  Symptoms: In certain conditions, IOS device can crash, with the following error message printed on the console: “%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SSH Proc”

  Conditions: In certain conditions, if an SSH connection to the IOS device is slow or idle, it may cause a box to crash with the error message printed on the console.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.5:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C CVE ID CVE-2012-5014 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

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

- CSCtq23960

  Symptoms: A Cisco ISRG2 3900 series platform using PPC architecture crashes and generates empty crashinfo files:

  show flash: all

  ```
  -#- length-- -----date/time------ path
  <<snip>>
  ```

```
2   0       Mar 13 2011 09:40:36 crashinfo_<date>
3   0       Mar 13 2011 12:35:56 crashinfo_<date>
4   0       Mar 17 2011 16:14:04 crashinfo_<date>
5   0       Mar 21 2011 05:50:58 crashinfo_<date>
```

Conditions: The symptom is observed with a Cisco ISRG2 3900 series platform using PPC architecture.

Workaround: There is no workaround.

- CSCtq41512

  Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/no shut brings the PRI layer 1 to Active and layer 2 to Multi-frame established.

  Conditions: This symptom occurs when “voice-class busyout” is configured and the controller TEI comes up before the monitored interface.

  Workaround: Remove the “voice-class busyout” configuration from the voice-port.

- CSCtr47084

  Symptoms: Changing zone from multilink interface and replacing the entire configuration by doing a **config replace flash:***config-file-name* crashes the router.

  Conditions: The symptom is observed when traffic is running.

  Workaround: There is no workaround.

- CSCts75737

  Symptoms: Tracebacks are seen at swidb_if_index_link_identity on the standby RP.

  Conditions: This symptom is observed when unconfiguring and reconfiguring “ipv4 proxy-etr” under the router LISP.

  Workaround: There is no workaround.

- CSCtt40285

  Symptoms: The router crashes. The following message is displayed:

```
System returned to ROM by bus error at PC 0x629D2EBC, address 0xB0D0B11 at
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x629D2EBC
```

  Conditions: The symptom is observed across multiple Cisco IOS Releases such as Cisco IOS Release 15.1(4)M2 and Cisco IOS Release 15.2(4)M1. This issue occurs only if NAT SIP ALG processing is enabled on the router.

  Workaround: This crash can be prevented by disabling NAT SIP ALG processing on the router by issuing the **no ip nat service sip** command.

- CSCtu02543

  Symptoms: The assigned address for an EzVPN client is not freed up after a disconnect.

  Conditions: This is seen if there is another L2L tunnel terminating on the same interface of the EzVPN server.

  Workaround: There is no workaround.

- CSCtu28696

  Symptoms: A Cisco ASR 1000 crashes with **clear ip route ***.

  Conditions: The symptom is observed when you configure 500 6RD tunnels and RIP, start traffic and then stop, then clear the configuration.

  Workaround: There is no workaround.

- CSCtu54300

Symptoms: Router crashes when you try to unconfigure the crypto.

Conditions: The symptom is observed when you clear the crypto and VRF configuration using automated scripts. The crash seen after the test is repeated three or four times. Before the crash the VRF and crypto features/functions are working fine.

Workaround: There is no workaround.

- CSCtw65575

  Symptoms: The router may unexpectedly reload when OSPFv3 MIB is polled via SNMP.

  Conditions: This symptom occurs when OSPFv3 is configured with area ranges whose prefix length is /128. A router with no area ranges is not vulnerable.

  Workaround: Configure area ranges to have a smaller prefix length (that is, in the range of /0 to /127).

- CSCtw78539

  Symptoms: A Cisco ISR router running Cisco IOS Release 15.2(2)T may lose the ability to forward traffic via its Gigabit Ethernet interface due to a stuck Tx ring.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T1, 15.2(2)T, and 15.2(4)M. This is a regression issue that does not affect 15.0(1)M3 nor 15.1(4)M2 based on anecdotal accounts.

  During the event the following logs can be seen which indicate a spurious memory access has occurred:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0xXXXXXXXX reading 0x0
  %ALIGN-3-TRACE: -Traceback= 0xXXXXXXXX ...
  ```

  At this time, the Tx ring of the interface becomes hung, causing packet drops to accumulate at the output queue (as seen via “show interface”), effectively preventing traffic flow. E.g.:

  ```
  Total output drops: 25185 Output queue: 331/1000/25184 (size/max total/drops)
  ```

  Workaround: Reload the router or bounce the interface via “shut”/”no shut”.

- CSCtw89123

  Symptoms: A router may crash after configuring “ppp fragment delay”.

  Conditions: The symptom is observed when “ppp fragment delay” + policy-map is configured on a multilink interface and traffic crosses the device.

  Workaround: Increase “ppp multilink fragment delay” under multilink interface and crash will not be seen.

- CSCtw98200

  Symptoms: Sessions do not come up while configuring RIP commands that affect the virtual-template interface.

  Conditions: This symptom is observed if a Cisco ASR1000 series router is configured as LNS.

  RIP is configured with the **timers basic** *5 20 20 25* command. Also, every interface matching the network statements is automatically configured using the **ip rip advertise** *5* command. These interfaces include the loopback and virtual-template interfaces too.

  On a Cisco ASR1000 series router, this configuration causes the creation of full VAIs which are not supported. Hence, the sessions do not come up. On Cisco ISR 7200 routers, VA sub-interfaces can be created.

  Workaround: Unconfigure the **timers rip** command.

- CSCtx31177

  Symptoms: RP crash is observed on avl_search in a high scaled scenario.

Conditions: This symptom is observed in a high scaled scenario with continuous traffic flow.

Workaround: There is no workaround.

- CSCtx34823

  Symptoms: OSPF keeps on bringing up the dialer interface after idle-timeout expiry.

  Conditions: This symptom occurs when OSPF on-demand is configured under the dialer interface.

  Workaround: There is no workaround.

- CSCtx36095

  Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.

  Conditions: This symptom occurs during a line card reload.

  Workaround: There is no workaround.

- CSCty61216

  Symptoms: CCSIP_SPI_Control causes leak with a Cisco AS5350.

  Conditions: The symptom is observed with the following IOS image:
  c5350-jk9su2_ivs-mz.151-4.M2.bin.

  It is seen with an outgoing SIP call from gateway (ISDN PRI --> AS5350 --> SIP --> Provider SIP gateway).

  Workaround: There is no workaround.

- CSCty82414

  Symptoms: A crash is seen.

  Conditions: The symptom is observed when all of ZBFW, SGFW, IPS and Scansafe are configured on the router and traffic as in the traffic profile is sent (http- [tcp], dhcp -[udp] traffic).

  Workaround: Unconfigure IPS.

- CSCtz15274

  Symptoms: When attempting a T.38 fax call on gateway, you may see the following in the logs:

  ```
  006902: %FLEXDSPRM-3-UNSUPPORTED_CODEC: codec cisco is not supported on dsp 0/0
  006903: %FLEXDSPRM-5-OUT_OF_RESOURCES: No dsps found either locally or globally.
  ```

  Conditions: The symptom is observed with a T.38 fax call.

  Workaround: There is no workaround.

- CSCtz21456

  Symptoms: A router has an unexpected reload due to CCSIP_SPI_CONTROL process.

  Conditions: This issue has been seen in Cisco IOS Release 15.2(3)T.

  Workaround: There is no workaround.

- CSCtz35999

  The Cisco IOS Software Protocol Translation (PT) feature contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-pt

Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtz78943

  Symptoms: A Cisco router experiences a spurious access or a crash. Cisco ISR-G1 routers such as a 1800/2800/3800 experience a spurious access. ISR-G2 routers such as the Cisco 2900/3900 routers that use a Power PC processor crash because they do not handle spurious accesses.

  Conditions: This symptom occurs after enabling a crypto map on an HSRP-enabled interface. The exact conditions are being investigated.

  Workaround: There is no workaround.

  Further Problem Description: The CSCtx90408 DDTS was originally filed to fix this issue. Unfortunately, this caused another issue, which was addressed by backing out of the changes. The fix was backed out in the CSCty83376 DDTS, so this DDTS (CSCtz78943) will address both issues.

- CSCtz83221

  Symptoms: Active or standby route processor crashes.

  Conditions: This symptom can be seen during the configuration or removal of ATM virtual circuits.

  Workaround: There is no workaround.

- CSCtz94286

  Symptoms: A router with an enabled ISM-VPN-29 module does not process ESP traffic when GRE packets are denied on the outside ACL.

  Conditions: There are two conditions that must both be met to experience this issue:

  1. The router uses an ISM-VPN module, and the module is installed and enabled.
  2. There is an ACL on the “outside” interface of the router that does not permit GRE traffic from the remote IPsec peer.

  Workaround 1: Permit GRE traffic from the remote IPsec peer.

  Workaround 2: Disable the ISM-VPN module.

- CSCtz94902

  Symptoms: Memory allocation failure occurs when attaching to SIP-40 using a web browser.

  Conditions: This symptom occurs on the line card.

  Workaround: Reset the line card.

- CSCua04049

  Symptoms: If a capture is stopped because of the limits reached and the capture is started immediately, the capture fails to stop.

  Conditions: This symptom occurs after immediate activation of a capture.

  Workaround: Clear buffer before activating the capture or wait for a minimum of 5 seconds before reactivation of a capture point.

- CSCua12317

Symptoms: The Cisco 3900 router resets when configuring Object Group/ACL when there is traffic on the interface where an ACL match is needed.

Conditions: This symptom is observed with the following conditions:

1. The ACL definition should have service OG ACE.
2. Reconfigure the service OG ACE or delete it.
3. Traffic should be passing on the interface where the OG is applied when the above operation is performed.

Workaround:

1. Configure a new ACL with the changes needed and apply it to the interface of interest, instead of modifying the already applied one. This is recommended when configuration change is needed.
2. Remove ACL checks on the interface when changing the configuration ("no ip access-group..").

- CSCua12396

  Symptoms: IPv6 multicast routing is broken when we have master switchover scenarios with a large number of members in stack. Issue is seen on platforms like Cisco 3750E and Cisco 3750X where IPV6 multicast routing is supported.

  Conditions: This symptom is observed when IPV6 multicast routing is configured, mcast routes are populated and traffic is being forwarded. Now, in case of master switchover, synchronization between master and members is disrupted. This is seen only for IPv6 multicast routing. Observed the issue with 9-member stack and either during first or second master switchover. No issues are seen for IPv4 multicast routing.

  Workaround: Tested with 5-member stack, and no issues are seen. It is recommended to enable IPv6 multicast routing when there is deployment with low members in stack.

- CSCua12945

  Symptoms: Applying QoS under the serial interface is causing the interface to flap and most of the time causes line protocol to be DOWN.

  Conditions: Issue happens during both congestion and non-congestion on the link.

  Workaround: Doing a shut/no shut on the interface makes the interface come UP and running.

- CSCua13848

  Symptoms: The Cisco ASR 1000 crashes.

  Conditions: This symptom is more likely to occur when a large number of VRFs are repeatedly configured and deleted.

  Workaround: There is no workaround.

- CSCua22789

  Symptoms: Router crashes while doing on-demand image download to switch which does not support Smart Install feature.

  Conditions: Router crashes while using CLI to upgrade the images on switch which does not support Smart Install feature.

  Workaround: There is no workaround.

- CSCua29095

  Symptoms: Spurious memory access is seen when booting the image on a Cisco 7600 router.

  Conditions: This symptom occurs while booting the image.

Workaround: There is no workaround.

- CSCua31157

  Symptoms: One way traffic is seen on a DMVPN spoke-to-spoke tunnel one minute after the tunnel is built. Issue is only seen intermittently.

  Logs on the spoke that fails to receive the traffic show “Invalid SPI” error messages exactly one minute after the tunnel between the spokes came up.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T1.

  Workaround: There is no workaround.

- CSCua31934

  Symptoms: Crash seen at __be_address_is_unspecified.

  Conditions: The symptom is observed with the following conditions:

  1. It occurs one out of three times and it is a timing issue.
  2. DMVPN tunnel setup between Cisco 2901 as spoke and Cisco ASR 1000 as hub.
  3. Pass IPv4 and IPv6 traffic between the hub and the spoke for 5-10 minutes.
  4. It can occur with v6 traffic alone.
  5. If you remove the tunnel interface on the ASR and add it again using **conf replace nvram:startup-config** the crash will occur.

  Workaround: Use CLI to change configuration instead of the rollback feature.

- CSCua42104

  Symptoms: CUBE with a transcoder generates malformed RTCP packets.

  Conditions: This symptom is observed with SIP-to-SIP CUBE with a transcoder registered to CUCM.

  ```
  CIPC -- CUCM -- SIP -- CUBE -- SIP -- ITSP
  CIPC -- G.729 -- CUBE (with transcoder) -- G.711 -- ITSP
  ```

  RTCP packets sent from ITSP are sometimes malformed when CUBE them sends to the originating device.

  Workaround: There is no workaround.

- CSCua45206

  Symptoms: The hub router crashes while removing the Stale Cache entry.

  Conditions: This symptom occurs when two spokes are translated to the same NAT address.

  Workaround: Spokes behind the same NAT box must be translated to different post-NAT Addresses.

- CSCua46304

  Symptoms: A crash is seen at __be_nhrp_group_tunnel_qos_apply.

  Conditions: This symptom is observed when flapping a DMVPN tunnel on the hub in a scale scenario.

  Workaround: There is no workaround.

- CSCua50697

  Symptoms: After unplugging and reconnecting a T1 cable, the T1 controller remains down or report continuous errors. After a router reload, the T1 controller remains up until the cable is disconnected again.

Conditions: This symptom affects only the following cards: HWIC-xCE1T1-PRI, NM-8CE1T1-PRI, VWIC3-xMFT-T1/E1, and GRWIC-xCE1T1-PRI. Also, the T1 signal must be somewhat out-of-specification according to T1.403 standards.

Workaround 1: Reload the router with the T1 cable plugged in.

Workaround 2:

1. Upgrade to a fixed-in Cisco IOS version.
2. Issue the following commands (hidden, so tab complete will not work):

```
enable
config t
controller <t1/e1> <slot/subslot/port> ! ( example: controller t1 0/0/0 )
hwic_t1e1 equalize
```

3. Shut/no shut the T1 controller, or reload the router to allow the CLI to take effect.

- CSCua55629

  Symptoms: SIP memory leak seen in the event SIPSPI_EV_CC_MEDIA_EVENT.

  Conditions: The command **show memory debug leaks** shows a CCSIP _SPI_CONTORL leak with size of 6128 and points to the event "SIPSPI_EV_CC_MEDIA_EVENT?:

```
Adding blocks for GD...

                 I/O memory


Address    Size   Alloc_pc  PID  Alloc-Proc       Name

                 Processor memory


Address    Size   Alloc_pc  PID  Alloc-Proc       Name
 286E144     6128  8091528  398  CCSIP_SPI_CONTR CCSIP_SPI_CONTROL
```

  Workaround: There is no workaround.

- CSCua56802

  Symptoms: QoS will not work on one of the subinterfaces/EVC.

  Conditions: This symptom occurs when HQoS policy is configured on more than one subinterface/EVC on ES+ and then add flat SG on them.

  Workaround: Remove and reapply SG.

- CSCua61201

  Symptoms: Unexpected reload with BFD configured.

  Conditions: When a device is configured with BFD it may experience unexpected reloads.

  Workaround: There is no workaround.

- CSCua61330

  Symptoms: Traffic loss is observed during switchover if,

  1. BGP graceful restart is enabled.
  2. The next-hop is learned by BGP.

  Conditions: This symptom occurs on a Cisco router running Cisco IOS XE Release 3.5S.

  Workaround: There is no workaround.

- CSCua64100

Symptoms: SCTP receives message fails.

Conditions: When sock-test testing infrastructure is used for SCTP testing.

Workaround: Use another test tool for SCTP testing. Issue is in sock-test. Not in SCTP.

- CSCua65278

  Symptoms: Modem disappears with the **cellular 0 cdma mode evdo** command.

  Conditions: The symptom is observed with the **cellular 0 cdma mode evdo** command when loaded with Cisco IOS interim Release 15.3(0.4)T.

  Workaround: There is no workaround.

- CSCua75069

  Symptoms: BGP sometimes fails to send an update or a withdraw to an iBGP peer (missing update)

  Conditions: This symptom is observed only when all of the following conditions are met:

  1. BGP advertise-best-external is configured, or diverse-path is configured for at least one neighbor.
  2. The router has one more BGP peers.
  3. The router receives an update from a peer, which changes an attribute on the backup path/repair path in a way which does not cause that path to become the best path.
  4. The best path for the net in step #3 does not get updated.
  5. At least one of the following occurs:

  - A subsequent configuration change would cause the net to be advertised or withdrawn. - Dampening would cause the net to be withdrawn.
  - SOO policy would cause the net to be withdrawn.
  - Split Horizon or Loop Detection would cause the net to be withdrawn.
  - IPv4 AF-based filtering would cause the net to be withdrawn.
  - ORF-based filtering would cause the net to be withdrawn.
  - The net would be withdrawn because it is no longer in the RIB.

  The following Cisco IOS releases are known to be impacted if they do not include this fix:

  - Cisco IOS Release 15.2T and later releases
  - Cisco IOS Release 15.1S and later releases
  - Cisco IOS Release 15.2M and later releases
  - Cisco IOS Release 15.0EX and later releases

  Older releases on these trains are not impacted.

  Workaround: If this issue is triggered by a configuration change, you can subsequently issue the **clear ip bgp** *neighbor* **soft out** command.

- CSCua82425

  Symptoms: A Cisco router may unexpectedly reload when using EMM when choosing a menu option that executes “reload” or “do reload”.

  Conditions: This symptom occurs if there are unchanged configuration changes.

  Workaround: Change the menu option to save the configuration before the reload. If you do not want to save the configuration, then there is no currently known workaround.

Further Description: In the newer code, the crash does not occur with “do reload” (though “reload” still crashes), but it still does not result in the desired behavior or reloading the device.

- CSCua91473

  Symptoms: Memory leak occurs during rekey on the IPsec key engine process.

  Conditions: This symptom occurs after rekey, when the IPsec key engine does not release KMI memory, causing the IPsec key engine holding memory to keep increasing.

  Workaround: Clear crypto session for IPsec key engine to release memory.

- CSCua91698

  Symptoms: ephone-type disappears from the running-configuration.

  Conditions: This symptom occurs in SRST mode and after reload.

  Workaround: Reconfigure the ephone-type commands and again save to startup-configuration.

- CSCua93001

  Symptoms: Auto-RP group is not automatically joined upon bootup.

  Conditions: The symptom is observed when the router reboots and starts from the existing configurations.

  Workaround: Manually re-enable “ip pim autorp” after bootup.

- CSCua99969

  Symptoms: IPv6 PIM null-register is not sent in the VRF context.

  Conditions: This symptom occurs in the VRF context.

  Workaround: There is no workaround.

- CSCub05907

  Symptoms: Reverse routes are not installed for an IPsec session while using dynamic crypto map.

  Conditions: This symptom occurs when the remote peer uses two or more IP addresses to connect and it goes down and comes back at least twice.

  Workaround: Issue “clear crypto session” for that peer.

- CSCub07855

  Symptoms: The VRF error message is displayed in the router.

  Conditions: This symptom occurs upon router bootup.

  Workaround: There is no workaround.

- CSCub14044

  Symptoms: A crash with traceback is seen, and all calls are dropped.

  Conditions: This symptom is observed under all conditions.

  Workaround: There is no known workaround. The gateway crashes, and the soak time appears to be six weeks.

- CSCub14145

  Symptoms: A Cisco ISR-G2 with VPN-ISM logs output similar to:

  ```
  !! Cannot find ISM-VPN counters struct for flowid: 0x44000084
  ```

  Conditions: The symptom is observed when using a VPN-ISM in an IPsec deployment with images from the Cisco IOS 15.2 train.

  Workaround: There is no workaround.

Further Problem Description: The issue is cosmetic in nature while the VPN-ISM is queried for counters (e.g.: show commands).

- CSCub15402

  Symptoms: A VRF cannot be deleted. The following error message is displayed:

  ```
  error message "% Deletion of VRF VPNA in progress; wait for it to complete".
  ```
  Conditions: This symptom occurs after having previously issued “sh ip cef vrf * sum”.

  Workaround: There is no workaround. Reboot is required to remove the VRF.

- CSCub17971

  Symptoms: There is no re-registration after switching from HW to SW crypto engine.

  Conditions: The symptom is observed after switching from HW to SW crypto engine.

  Workaround: There is no workaround.

- CSCub19185

  Symptoms: Path confirmation fails for a SIP-SIP call with IPV6 enabled.

  Conditions: This symptom occurs when UUTs are running Cisco IOS Release 15.2(2)T1.5.

  Workaround: There is no workaround.

- CSCub30381

  Symptoms: Router crashes very frequently.

  Conditions: The symptom is observed with a router configured with X25 and any dynamic routing protocol.

  Workaround: Use static routing instead of dynamic routing.

- CSCub36403

  Symptoms: Standby reloads due to no switchport.

  Conditions: Configure a port as “no switchport”. No IP configuration needed. Set the “tftp source interface <>”. Now defaulting the interface causes this issue.

  Workaround: There is no workaround.

- CSCub39268

  Symptoms: Cisco ASR 1000 devices running an affected version of IOS-XE are vulnerable to a denial of service vulnerability due to the improper handling of malformed IKEv2 packets. An authenticated, remote attacker with a valid VPN connection could trigger this issue resulting in a reload of the device. Devices configured with redundant Route Processors may remain active as long as the attack is not repeated before the affected Route Processor comes back online.

  Conditions: Cisco ASR1000 devices configured to perform IPSec VPN connectivity and running an affected version of Cisco IOS-XE are affected. Only authenticated IKEv2 connection is susceptible to this vulnerability.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-5017 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

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

- CSCub42181

  Symptoms: The router crashes continuously after a normal reboot due to power or some other reason.

```
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M4,
RELEASE SOFTWARE (fc1)
 uptime is 4 days, 11 hours, 38 minutes
System returned to ROM by error - a Software forced crash, PC 0x88D26F0 at
07:42:45 UTC Sat May 5 2012
System restarted at 07:43:55 UTC Sat May 5 2012
System image file is "flash:c3900-universalk9-mz .SPA.150-1.M4.bin" ;
Last reload type: Normal Reload
----------------------------
generated Traceback:

Pre Hardware Replacement Crashinfo:
------------------------------------
#more flash0:crashinfo_20120519-165015-UTC

------------------
Traceback Decode:
------------------

tshakil@last-call-2% rsym c3900-universalk9-mz.150-1.M4.symbols.gz
Uncompressing and reading c3900-universalk9-mz.150-1.M4.symbols.gz via
/router/bin/zcat
c3900-universalk9-mz.150-1.M4.symbols.gz read in
Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c
0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4
Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c

0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4
Enter hex value:


--------------------------------
Crash File Post Installation:
------------------------------

#more flash0:crashinfo_20120519-185725-UTC


------------------
Traceback Decode:
-----------------

Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c
0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4
```

```
Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c
0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4

--------------------------------------------------
```

Conditions: This symptom is observed with the following conditions:

- MGCP gateway.
- Take out all the modules from the router.
- Put the modules one by one.
- Apply the configuration.
- The router is stable.

The lab test recreated as follows:

1. Disable auto-configuration, that is, “no ccm-manager config”.
2. Reload the gateway.
3. Enable the CCM manager configuration and the router does not crash.

Workaround 1: Bypass the start-up configuration and log in via ROMmon without any configuration. Add the configuration one by one. Once the configuration is added, save the configuration and reload the gateway.

Workaround 2: Shut down the router and add the cards one by one in slots 0, 1, 2, 3, and 4. The device is stable until the third slot is inserted and brought up. As soon the router is powered on, after adding the fourth slot, the crash starts. Shut down the router and remove the card in slot 4 (EVM-HD-8FXS/DID). Bring the device up without the card in slot 4 (EVM-HD-8FXS/DID). Remove the “mgcp” and “ccm-manager fallback-mgcp” configuration from the device because the console log is displaying the “Call Manager backhaul registration failed” error message. Shut down the router and add the card which was removed. Bring up the router. Readd the **ccm-manager fallback-mgcp** command and do a “no mgcp/mgcp”. The router becomes stable.

Workaround 3: Remove the **ccm-manager config** command by no ccm-manager config which tears down the connection from the call manager to the MGCP gateway. The gateway will not download the configuration from the call agent at the time of startup. Reload the router. Once the router is back and stable, readd the command.

- CSCub44898

  Symptoms: Stale scansafe sessions are seen on the router. They do not get cleared even with the **clear content-scan sessions *** command.

  Conditions: This issue occurs when one of the end points (client or server) does not properly close the connection. In TCP terms, when one end does not send an ACK to the FIN request sent by the other end in L4F UNPROXIED state.

  Workaround: There is no workaround. The router needs to be rebooted to clear the stale sessions.

- CSCub45054

  Symptoms: OQD drop counters increment on the mGRE tunnel even though there are no drops.

  Conditions: This symptom is observed with an mGRE tunnel when multicast traffic is sent over the tunnel. This issue is seen when EIGRP or OSPF is configured on the tunnel.

  Workaround: There is no workaround.

- CSCub55790

  The Smart Install client feature in Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

  Affected devices that are configured as Smart Install clients are vulnerable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that have the Smart Install client feature enabled.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-smartinstall

- CSCub61009

  Symptom: Spurious errors observer on Cisco AS5400.

  Conditions: None.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/6.5:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C CVE ID CVE-2012-5422 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

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

- CSCub61795

  Symptoms: The log fills with SYS-2-BADSHARE messages, leading to a crash.

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=69AD4440, count=0 -Traceback=
  601E887Cz 601E50B4z 601E56C0z 602D24CCz 60F38F04z 6065B628z Invalid magic number in
  receive buffer (0x0)
  ```

  Conditions: This symptom occurs with a large amount of traffic passing through an ATM interface. This issue might be specific to an ATM interface using the CX27470 ATMOC3 driver as seen in the **show interface** command output. The ATM module that the issue was originally seen on was a NM-1A-OC3-POM. QOS might be needed to trigger the issue.

  Workaround: A possible but unconfirmed workaround is to disable QOS on the interface.

- CSCub69976

  Symptoms: Cisco 1941 in a DMVPN setup crashes with Cisco IOS Release 15.2(2)T2. The Cisco 2911 router and the Cisco 3945 router crash in a FlexVPN setup running Cisco IOS Release 15.3(00.14)T

  Conditions: This symptom occurs in a DMVPN setup and in the FlexVPN setup.

  Workaround: Disable the ISM module and switch to the onboard crypto engine using "no crypto engine slot 0".

- CSCub70336

  Symptoms: The router can crash when "clear ip bgp *" is done in a large-scale scenario.

  Conditions: This symptom is observed only in a large-scale scenario, with ten of thousands of peers and several VPNv4/v6 prefixes.

Workaround: “clear ip bgp *”is not a very common operation. Hence, this issue has not been observed by customers. The crash can only happen when “clear ip bgp *” is done. The workaround is not to execute “clear ip bgp *”.

- CSCub73177

  Symptoms: RP crash occurs.

  Conditions: This symptom occurs upon router reload

  Workaround: There is no workaround.

- CSCub74272

  Symptoms: Intermittently during Phase II rekey, after new SPIs are negotiated and inserted into SPD, old SPIs are removed and then the VTI tunnel line protocol goes down.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T, with VTI over GRE.

  Workaround: There is no workaround.

- CSCub79590

  Symptoms: The **match user-group** commands do not appear in the running configuration after being configured.

  Configure an inspection type class-map:

```
class-map type inspect TEST
    match protocol tcp
    match user-group cisco
```

  Save the configuration. Try to view the configuration in the running configuration:

```
hostname# show run class-map
building configuration...

Current configuration : 66 bytes
!
class-map type inspect match-all TEST
   match protocol tcp
end
```

  But, view the configuration directly in the class-map:

```
hostname# show class-map type inspect
   Class Map type inspect match-all TEST (id 1)
     Match protocol tcp
     Match user-group cisco
```

  The configuration never shows up in the running configuration, but it is in the class-map configuration. As a note, the functionality exists on the ZBFW, but the configuration does not show up in the running configuration.

  Conditions: This symptom is only observed with the **match user-group** commands.

  Workaround: This issue only affects devices after a reload as the router will read the startup configuration, which will not have the **match user-group** command. As a result, the **match user-group** commands need to be reentered after ever reload.

- CSCub80386

  Symptoms: The following interface configuration should be used:

```
interface Ethernet2/1
description lanethernet1
ipv6 enable
ospfv3 100 network manet
ospfv3 100 ipv6 area 0
```

Dead interval is calculated according to network type; in this case, it is 120s. Issue the **no ospfv3 dead-interval** command on dead interval. Dead interval is set to the default of 40s instead of 120s, which is correct for manet or P2MP interface types.

Conditions: This symptom is an OSPFv3-specific issue (see the configuration example).

Workaround: Configure dead interval explicitly or reapply the network command.

- CSCub80710

  Symptoms: SSL handshake between Cisco VCS and the Cisco ASR fails if the Cisco ASR is running Cisco IOS XE Release 3.7S.

  Conditions: This symptom occurs in a working setup, if the Cisco ASR is upgraded to Cisco IOS XE Release 3.7S, then SSL handshake and subsequently SIP-TLS calls start to fail. If in the same setup, the Cisco ASR is downgraded back to Cisco IOS XE Release 3.5S or Cisco IOS XE Release 3.4.4S, then the calls work (without requiring any additional changes).

  Workaround: There is no workaround.

- CSCub82495

  Symptoms: Channel-group goes down with the HWIC-xCE1T1-PRI controller after reloading the router.

  Conditions: This symptom occurs when channel-group goes down after reload.

  Workaround: There is no workaround.

- CSCub84471

  Symptoms: WAAS-optimized traffic is stuck in a loop when ISM VPN is enabled.

  Conditions: This symptom occurs when the ISM-VPN Module is turned on.

  Workaround: There is no workaround.

- CSCub86011

  Symptoms: The embedded event manager (EEM) is not available on the Cisco VG202/204.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T or later releases.

  Workaround: There is no workaround.

- CSCub86319

  Symptoms: Router reloads when you enable **no cdma modem dm-log enable** CLI.

  Conditions: The symptom is observed when you enable **no cdma modem dm-log enable** CLI with Cisco IOS interim Release 15.3(0.12)T.

  Workaround: There is no workaround.

- CSCub86706

  Symptoms: After multiple RP switchover, the router crashes with the “UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP HA SSO” error.

  Conditions: This symptom is observed with MVPN with 500 VRFs, when performing multiple switchovers on PE1.

  Workaround: There is no workaround.

- CSCub89144

  Symptoms: The VTI tunnel is always in up/up state.

Conditions: This symptom is observed when HSRP failover is configured on the HSRP standby router only. This issue was first seen on the Cisco ASR router, but it is platform-independent and is seen on the latest Cisco IOS Release 15M&T and later releases as well.

Workaround: Use GRE or routing protocols for redundancy.

- CSCub90459

  Symptoms: If CUBE has midcall reinvite consumption enabled, it also consumes SIP 4XX responses. This behavior can lead to dropped or hung calls.

  Conditions: This symptom occurs when midcall reinvite consumption is enabled.

  Workaround: There is no workaround.

- CSCub95141

  Symptoms: FP Pending Refs are observed when "cypto map <> local-address loopbackX" is removed from the configuration when the crypto map is applied on a subinterface.

  Conditions: This symptom is observed with the following configuration:

```
crypto map cry local-address Loopback0

interface GigabitEthernet0/0/0.100
  crypto map cry

interface GigabitEthernet0/0/0.200
  crypto map cry
```

  Workaround: Remove "crypto map" from the subinterface first and then remove "crypto map <> local-address loopbackX".

- CSCub96618

  Symptoms: Error message seen on standby.

  Conditions: The symptom is observed with tunnel configurations.

  Workaround: There is no workaround.

- CSCub99756

  Symptoms: The Cisco ASR 1000 router running Cisco IOS Release 15.2(4)S acting as a GM in a Get VPN deployment starts using the most recent IPsec SA upon KS rekey instead of using the old key up to 30 seconds of expiration.

  Conditions: This symptom is observed only in Cisco IOS Release 15.2(4)S.

  Workaround: There is no workaround.

- CSCub99778

  Symptoms: The Cisco ASR 1000 router being GM in a Get VPN deployment fails to start GDOI registration after a reload.

  Conditions: This symptom occurs when running Cisco IOS Release 15.2(4)S. The following error is displayed in the **show crypto gdoi** command output after reload.

```
Registration status : Not initialized
```

  Workaround: Use an EEM script to issue "clear crypto gdoi" some time after boot time or issue this manually.

- CSCuc01575

  Symptoms: The command **no monitor capture** *name* **control-plane** leads to a crash.

  Conditions: The symptom is observed with the command **no monitor capture** *name* **control-plane**.

  Workaround: There is no workaround.

CSCuc05631

Symptoms: Tracebacks are seen in the ISM-VPN background.

Conditions: This symptom is observed when Get VPN and DMVPN are turned by having the ISM-VPN Module.

Workaround: Disable ISM-VPN and use the onboard VPN ACCL.

- CSCuc07984

  Symptoms: The Cisco 819 router serial interface does not interoperate with modems such as Adtran, Aethra, and Pardayn.

  Conditions: This symptom occurs on the serial interface on the Cisco 819 series router while connecting to some specific types of modems.

  Workaround: There is no workaround.

- CSCuc08061

  Symptoms: IPv6 DMVPN spoke fails to rebuild tunnels with hubs.

  Conditions: This symptom occurs when the tunnel interface on the spoke is removed and reapplied again.

  Workaround: Reboot the spoke.

- CSCuc12685

  Symptoms: Address Error exception is observed with ccTDUtilValidateDataInstance.

  Conditions: This symptom is observed with ccTDUtilValidateDataInstance.

  Workaround: There is no workaround.

- CSCuc12907

  Symptoms: The **waas config remove-all** and **waas config restore-default** commands fail.

  Conditions: The **waas config remove-all** and **waas config restore-default** commands fail. WAAS-Express class-maps, policy-maps, and parameter-map fail to be removed when the previous commands are issued. The following error is seen: % Remove All Config failed: Unable to remove WAAS class-map(s).

  Workaround: On Cisco c3900, c2951, c2900, and c1900, install the datak9 package. The CLIs are successful then.

- CSCuc14088

  Symptoms: The default class is not being exported with the class option template.

  Conditions: This symptom occurs when class-default is not exported when typing the option c3pl-class-table under the flow exporter.

  Workaround: There is no workaround.

- CSCuc14674

  Symptoms: In a GetVPN configuration, when utilizing the ISM VPN module, traffic does not pass even though IPsec SAs are up when CEF is enabled, and "ip traffic-export" is configured in the crypto map interface.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T1 or later releases, and when CEF is enabled. This issue is seen when "ip traffic-export" is configured in the crypto map interface, and ISM is the crypto engine.

  Workaround 1: Disable CEF.

Workaround 2: Do not configure “ip traffic-export” in the crypto map interface.

Workaround 3: Disable ISM using “no cry engine slot 0”. Then, the onboard engine will be used.

- CSCuc15695

  Symptoms: The counters are not polling the correct stats.

  Conditions: This symptom was first observed on the ATM interfere, but it is not particular to the ATM as this issue was reproduced on the Gigabit Ethernet interface as well.

  Workaround: There is no workaround.

- CSCuc16172

  Symptoms: When the reset button is pushed on a Cisco C881W-A-K9 router, the start-up configuration is automatically backed up as “startup.backup.xxx” and stored in the flash.

  Conditions: This symptom occurs when a xxx.cfg file is present on the flash and the push button is pressed. The Cisco C881W-A-K9 Router boots up with the xxx.cfg file present on the flash, but also backs up the start-up configuration as “startup.backup.xxx” and stores it on the flash.

  Workaround: There is no workaround.

- CSCuc19046

  Symptoms: Active Cisco IOSd was found to have crashed following the “clear ip mroute *” CLI.

  Conditions: This symptom occurs with 4K mroutes (2k *,G and 2K S,G) running the FFM performance test suite.

  Workaround: There is no workaround.

  Further Problem Description: So far, this issue is only seen in the FFM performance test script.

- CSCuc19862

  Symptoms: Traceback and CPU hog is seen due to spurious memory access when Flexible NetFlow (FNF) is enabled.

  Conditions: This symptom is seen when enabling FNF.

  Workaround: Use classic netflow or configure FNF on the tunnel template interface (preferred).

  Note: the first option of using classic netflow is not available on some platforms which only support FNF. Notably these are Cat 6k, Sup 2T and the Cat 4K K10.

- CSCuc24937

  Symptoms: The voice gateway router is configured as a CME for handling ephone reloads due to spurious memory access.

  Conditions: This symptom occurs as the voice gateway router is capable of handling ephones. Reload is very specific to ephone handling.

  Workaround: There is no workaround.

- CSCuc30630

  Symptoms: An update to the Cisco IOS-IPS signature package may cause the router to crash in some very rare scenarios, when signature scanning and signature build happens simultaneously.

  Conditions: This symptom occurs on a Cisco 2911 ISR G2 router running Cisco IOS Release 15.2(4)M1.

  Workaround: There is no workaround.

- CSCuc36469

Symptoms: Crash is observed when removing the **crypto call admission limit ike in-negotiation-sa** *value* configuration and clear crypto sessions, which triggers a connection from all the clients burdening the server and forcing it to crash within seconds.

Conditions: This symptom happens only when 150 connections simultaneously try to establish connection with the head-end EzVPN server.

Workaround: Configure **crypto call admission limit ike in-negotiation- sa** *20* when scaling to 150 tunnels.

- CSCuc37047

  Symptoms: VSS crashes on reconfiguring "ipv6 unicast-forwarding" multiple times.

  Conditions: This symptom occurs when CTS is configured on an interface and "ipv6 unicast" is toggled multiple times.

  Workaround: There is no workaround.

- CSCuc40448

  Symptoms: No-way audio is observed on hair-pinned calls back from CUBE to SIP Provider.

  The call flow is as follows:

```
PSTN caller --Verizon---(sip)---ASR CUBE---(sip)---CUSP---(sip)---Genesis (SIP Refer
sent to transfer back to Verizon) -- CUSP - CUBE - Verizon -- PSTN
```

  Conditions: This symptom is observed only after upgrading to Cisco IOS Release 15.2(2)S.

  Workaround: Modify the diversion header on the transfer leg invite, so Verizon handles the call differently.

- CSCuc42518

  Symptoms: Cisco IOS Unified Border Element (CUBE) contains a vulnerability that could allow a remote attacker to cause a limited Denial of Service (DoS). Cisco IOS CUBE may be vulnerable to a limited Denial of Service (DoS) from the interface input queue wedge condition, while trying to process certain RTCP packets during media negotiation using SIP.

  Conditions: Cisco IOS CUBE may experience an input queue wedge condition on an interface configured for media negotiation using SIP when certain sequence of RTCP packets is processed. All the calls on the affected interface would be dropped.

  Workaround: Increase the interface input queue size. Disable Video if not necessary.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4/3.1:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:OF/RC:C CVE ID CVE-2012-5427 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

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

- CSCuc44438

  Symptoms: There is a memory corruption issue with loading NBAR protocol pack.

  Conditions: This symptom occurs when an NBAR protocol pack is loaded into the router using the **ip nbar protocol-pack** command.

  Workaround: There is no workaround.

- CSCuc44629

  Symptoms: The switch/router crashes while processing NTP.

Conditions: This symptom occurs if NTP is configured using DNS, along with the source interface. For example:

```
config# ntp server <dns> source <interface>
```

Workaround 1: config# ntp server <dns>

Workaround 2: config# ntp server <ip>

Workaround 3: config# ntp server <ip> source <interface>

For workarounds 1 and 2, the device automatically selects the source interface. For workarounds 2 and 3, resolve the DNS and use the corresponding IP address for that DNS. For example:

```
Router# ping <dns>
```

The above command gives the IP address for DNS. Use that IP address to configure the NTP server.

- CSCuc45115

  Symptoms: EIGRP flapping is seen continuously on the hub. A crash is seen at nhrp_add_static_map.

  Conditions: This symptom is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.

  Workaround: There is no known workaround.

- CSCuc45528

  Symptoms: Incremental leaks are seen at:__be_nhrp_recv_error_indication.

  Conditions: This symptom occurs when the NHRP error indication is received on the box. This issue is seen only if CSCub93048 is already present in the image. CSCub93048 is available from Cisco IOS Release 15.3M&T onwards.

  Workaround: There is no workaround.

- CSCuc46087

  Symptoms: CUBE does not send a response to an early dialog UPDATE in a glare scenario.

  Conditions: This symptom occurs when CUBE receives an early dialog UPDATE when it sends 200OK to INVITE and expects ACK.

  Workaround: There is no workaround.

- CSCuc47399

  Symptoms: IKEv2 STOP Accounting records show wrong counters for packets/octets, when the sessions are locally cleared using “clear crypto sa” or “clear crypto session” on ASR1K.

  Conditions: This symptom is observed with latest Cisco IOS XE Release 3.8S images when IKEV2-Accounting is enabled. This issue is easily reproducible with a single session, and may be service impacting as STOP Accounting records are usually used for billing purposes.

  Workaround: The STOP records reflect the right counters when the disconnect is through the remote-end.

- CSCuc50398

  Symptoms: Client is crashing while doing telnet from host to server.

  Conditions: The symptom is observed with the following set up:

  host <---> client <---> mid-router <---> server

  It is crashing consistently due to memory overrun.

  Workaround: There is no workaround.

- CSCuc55346

  Symptoms: SNMP MIB cbQosCMDropPkt and cbQosCMDropByte report 0.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)S1 and Cisco IOS Release 15.2. This issue is not seen with Cisco IOS Release SRE4.

  Workaround: Use SNMP MIB cbQosPoliceExceededPkt and cbQosPoliceExceededByte.

- CSCuc55634

  Symptoms: IPv6 static route cannot resolve the destination.

  Conditions:

  1. A VRF is configured by the old style CLI (for example “ip vrf RED”).
  2. Configure “ip vrf forwarding RED” under an interface.
  3. Configure IPv6 address under the same interface (for example 2001:192:44:1::2/64).
  4. Configure IPv6 static route via the interface configured in item 3, (for example IPv6 route 2001:192:14:1::/64 2001:192:44:1::1).
  5. Then, we are not able to ping the 2001:192:14:1::2 although we can reach 2001:192:44:1::1.

  Workaround: There is no workaround.

- CSCuc63884

  Symptoms: A router configured with HSRP and RF interdev may experience an NMI watchdog during reload after failover, as it transitions from a standby to an active state.

  ```
  SYS-2-INTSCHED ’sleep for’ at level 6 -Process= "RF Interdev reload process", ipl= 6,
  pid= 316
  NMI Watchdog timeout!!: vector 2, PC = 0x219B3C
  ```

  Conditions: This symptom is observed with HSRP and interdev configured. HSRP failover is triggered by link failure if the configuration is being saved at the same time.

  Workaround: There is no workaround.

- CSCuc67033

  Symptoms: A Cisco IOS router with the ISM VPN encryption module enabled can experiences memory corruption-related crashes.

  Just before the crash, the router may display some syslog error messages related to the ISM VPN module:

  ```
  Aug 21 15:55:22: !!! Cannot find Revt counters struct for flowid: 0x4400012A
  Aug 21 15:55:24: !!! Cannot find Revt counters struct for flowid: 0x4400012A
  Aug 21 15:55:24: !!! Cannot find Revt counters struct for flowid: 0x4400012A
  ```

  Here, the word “Revt” is specific for the ISM VPN module.

  Also, some generic syslog error messages related to memory allocation failures may be displayed the crash:

  ```
  Aug 21 15:55:33: %SYS-3-BADBLOCK: Bad block pointer DD7D7D0
  -Traceback= 23B9EA7Cz 23BA1A44z 23BA1E24z 23B712B8z 23B7129Cz
  Aug 21 15:55:33: %SYS-6-MTRACE: mallocfree: addr, pc
   352791C4,22DB4A50 352791C4,3000006C 38808760,2627EDF0 34C91824,262724A8
   352791C4,22DB6214 352791C4,22DB4A50 352791C4,3000006C 352791C4,22DB6214
  Aug 21 15:55:33: %SYS-6-MTRACE: mallocfree: addr, pc
   352791C4,22DB4A50 352791C4,3000006C 352791C4,22DB6214 3875D9C4,600002CA
   3875D5E0,2627EDF0 35092ACC,262724A8 352791C4,22DB4A50 352791C4,3000006C
  Aug 21 15:55:33: %SYS-6-BLKINFO: Corrupted next pointer blk DD7D7D0, words
  32808, alloc 214E636C, InUse, dealloc 0, rfcnt 1
  ```

  Conditions: This symptom is observed with the following conditions:

  - The ISM VPN crypto acceleration module is installed, enabled, and used for crypto operations (IPsec, etc.).
  - Cisco IOS supports ISM VPN (Cisco IOS Release 15.2(1)T1 or later releases).

  Workaround: Disable the ISM VPN module. The crash is specific to ISM VPN.

- CSCuc69342

  Symptoms: About 10 minutes after CUBE boot, the router crashes with the following traceback:

  ```
  -Traceback= 5B01805 46158ED 45F4F57 45BB19E 45BA1CF 451D6DC 4525549 45252D9 4519C30
  45196A9 4778FFD
  ```

  After the reload from the crash, it may take some time before it crashes again.

  Conditions: This symptom occurs when CUBE receives the SIP REFER message with the Refer-To header having no user part.

  Workaround: There is no workaround.

- CSCuc71493

  Symptoms: Significant transaction time degradation is observed when an e-mail with attachment(s) is sent from the Windows 7 client using Outlook to a server running Outlook 2010 on the Windows 2008 server and the WAN latency is low, that is, ~12ms RTT.

  Conditions: This symptom is observed when the client is Windows 7 and data is being uploaded using the MAPI protocol and the connection is being optimized by WAAS-Express.

  Workaround: Disable WAAS-Express.

- CSCuc71706

  Symptoms: Execution of the **show run** command and other commands such as **copy run start** and **show access-list** cause the router to stop for a few minutes before completing.

  Conditions: This symptom is observed with Cisco ISR G2 routers. This issue is seen only with IPV6 configured and used.

  Workaround: There is no workaround.

- CSCuc72594

  The Cisco IOS Software implementation of the IP Service Level Agreement (IP SLA) feature contains a vulnerability in the validation of IP SLA packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Mitigations for this vulnerability are available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ipsla

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCuc73615

  Symptoms: If you reload CPE with “dsl-group auto”, the ALU-SMLT-C-lines does not train.

Conditions: The symptom is observed with "dsl-group auto" configuration.

Workaround 1: Flap the link on CO side or unplug/plug cable.

Workaround 2: Use manual 4-wire configuration instead of auto. See the configuration below:

```
dsl 0 pair 0-1 m-pair
shdsl 4-wire mode en
hand g.shdsl
```

- CSCuc76298

  Symptoms: In ASR B2B HA setup, the new active router crashes at ccsip_send_ood_options_ping immediately after switchover with OOD OPTIONS enabled.

  Conditions: This crash is seen in the following scenario:

  - Standby router has OOD OPTIONS enabled either because it is present in startup configuration or enabled after boot-up.
  - Next, disable OOD OPTIONS.
  - Switchover happens.

  Workaround: Reload standby router once after OOD OPTIONS configuration changes from enabled to disabled.

- CSCuc77704

  Symptoms: The GETVPN/GDOI Secondary Cooperative Key Server (COOP-KS) does not download the policy (that is, when the **show crypto gdoi ks policy** command is issued on the Secondary COOP-KS and the command output shows that no policy is downloaded) and Group Members (GMs) registering to the Secondary COOP-KS fail to register without any warning/error message.

  Conditions: This symptom is observed when the GETVPN/GDOI group (with COOP configured) has an IPsec profile configured with one of the following transforms in its transform-set:

  - esp-sha256-hmac
  - esp-sha384-hmac
  - esp-sha512-hmac

  Workaround: Use esp-sha-hmac as the authentication transform instead.

- CSCuc79143

  Symptoms: The cellular driver should handle the profile getting inactive and should bring down the cellular interface.

  Conditions: This symptom occurs when the profile is deactivated by the HA.

  Workaround: Doing a "clear line" will bring down the cellular interface and restore the connection.

- CSCuc82551

  Symptoms: A Cisco ASR 1001 running Cisco IOS XE Release 3.6.2S or Cisco IOS XE Release 3.7.1S crashes with SNMP traffic.

  Conditions: This symptom is observed with SNMP polling with an IP SLA configuration.

  The crash signature is as follows:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SNMP ENGINE
  ```

  Workaround: Remove the SNMP configuration from the router or schedule the probe before polling via SNMP.

- CSCuc91717

Symptoms: Router crashes when making basic x25 configuration change.

Conditions: Remove x25 translation statement from running configuration when traffic is on.

Workaround: Shut the interface before making x25 configuration change.

- CSCuc93739

  Symptoms: Phase 2 for EzVPN client with split network and VTI does not come up if IPsec SA goes down.

  Conditions: The root cause of the issue is that IPsec SA is not being triggered after IPsec SA is down due to no traffic. So in spite of traffic IPsec SA is not coming up leading to packet drops in client network. The same problem is not seen with Cisco IOS Release 15.0(1)M7. This behavior is introduced post-PAL where virtual-interface creates a ruleset where traffic cannot trigger IPsec SA again once IPsec SA is deleted.

  Workaround 1: Configure “ip sla” on EZVPN client for split networks, so IPsec SA will not go down.

  Workaround 2: Remove “virtual-interface” from EZVPN client profile if that is not needed.

  Further Problem Description: The problem is not seen in Cisco IOS Release 15.2(4)M1 without virtual-interface.

- CSCuc94687

  Symptoms: SHA2 processing in software causes low throughput or high CPU.

  Conditions: This symptom is observed with the Cisco 892 with SHA2 configured and the onboard crypto engine enabled running Cisco IOS Release 15.2(4)M and later releases.

  Workaround: There is no workaround.

- CSCuc96631

  Symptoms: Incoming calls through e1 r2 stop working in Cisco IOS Release 15.2(4)M1.

  Conditions: This symptom is observed with incoming calls through e1 r2 in Cisco IOS Release 15.2(4)M1. Outgoing calls work fine.

  Workaround: Use Cisco IOS Release 15.2(2)T.

- CSCud01502

  Symptoms: A crash occurs in CME while accessing a stream in sipSPIDtmfRelaySipNotifyConfigd.

  Conditions: This symptom occurs in CME.

  Workaround: There is no workaround.

- CSCud02361

  Symptoms: Sequence number of spoofed ACK sent to the server has a 0x00 value.

  Conditions: Once the max-incomplete high is reached, when the next SYN packet is sent from the client, the UUT sends a SPOOFED-ACK after getting the SYN-ACK from the server. When this ACK packet is observed at the server pagent with the packets tool, the sequence number is found to be 0x00.

  Workaround: There is no workaround.

- CSCud03273

  Symptoms: All the paths using certain next-hops under the route-map are marked inaccessible.

Conditions: This symptom occurs under the following conditions:

1. Configure peer groups.
2. Apply BGP NHT with route-map (no BGP neighbors are created or added to peer groups).
3. Configure the Prefix-list.
4. Configure the route-map.
5. Configure the BGP neighbor and add them to peer groups.

Workaround: Configure "route-map permit <seq-num> <name>" or activate at least one neighbor in "address-family ipv4".

- CSCud03877

  Symptoms: After volume rekey, the IPsec PD flow sets both the hard and soft limit of the traffic limit to 0.

  Conditions: This symptom is observed when the volume rekey is set to 0.

  Workaround: Clear crypto session to recover the volume rekey value.

- CSCud06180

  Symptoms: When the SDK crash occurs, the cellular interface is not operational.

  Conditions: This symptom occurs when the IPSLA is present on the cellular interface, and you power-cycle the modem 8-10 times, causing the CWAN_SHIM layer to crash.

  Workaround: There is no workaround.

- CSCud06887

  Symptoms: IPsec Stateful failover is configured between two routers.

  router_1 is chosen as Active.

  router_2 is chosen as Standby.

  router_3 acts as the VPN end peer.

  - A VPN tunnel is created between the VIP of routers 1 and 2 and router_3.
  - SPIs are replicated from Active (router_1) to Standby (router_2).
  - After switchover from Active to Standby (done by reload of Active router_1), router_2 becomes Active and takes over the VPN connection.
  - router_1 comes up after manual reload and then reloads again by itself.
  - When router_1 comes up after the second reload, SPIs are not replicated from Active router_2.

  Conditions: This symptom occurs when IPsec Stateful failover is configured on Cisco IOS Release 15.2(4)M1. This issue is seen when the HW crypto engine is enabled.

  Workaround: There is no workaround. When next switchover from Active to Standby will be triggered, then new VPN connection is being created, packet loss occurs.

- CSCud08595

  Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/no shut brings the PRI layer 1 to Active and layer 2 to multiframe established.

  Conditions: This symptom occurs when "voice-class busyout" is configured and the controller TEI comes up before the monitored interface.

  Workaround: Remove the "voice-class busyout" configuration from the voice-port.

- CSCud22222

Symptoms: On a router running two ISIS levels and fast-reroute, the router may crash if “metric-style wide level-x” is configured for only one level.

Conditions: Issue may happen if metric-style wide is configured for only one level on router running both levels, and fast-reroute is configured.

Workaround: Configure metric-style wide for both levels (by default).

- CSCud27379

  Symptoms: WS-SUP720-3B running Cisco IOS Release 12.2(33)SRE4 crashes at get_alt_mod after issuing “sh run int g4/13” with several trailing white spaces until the cursor stops moving.

  Conditions: This symptom occurs when you issue the **show run interface** command with trailing spaces until the cursor stops moving.

  Workaround: Do not specify trailing spaces at the end of the **show run interface** command.

- CSCud31808

  Symptoms: With the two commands configured listed under the conditions of this release note, the Cisco router might start advertising a low TCP receive window size to the TCP peer for a specific TCP transaction. The value of this receive window size becomes equal to the configured MSS value, and it will never exceed this value anymore. This might impact TCP performance.

  Conditions: This symptom happens only if the following two commands are configured on the router:

  ip tcp mss x

  ip tcp path-mtu-discovery

  Workaround: Either change the path-mtu discovery ager timeout to 0, or remove one of the two commands.

- CSCud33159

  Symptoms: Excessive loss of MPLS VPN traffic and high CPU utilization is observed due to the process switching of MPLS traffic over the ATM interface.

  Conditions: This symptom occurs when MPLS is enabled on the ATM interface with aal5snap encapsulation.

  Workaround: There is no workaround.

- CSCud34809

  Symptoms: The ISM module on the cisco 3900 router suddenly fails to encrypt IPsec data on specific tunnels.

  Conditions: This symptom occurs when ISM-VPN-39 is installed and active on the Cisco 3900 router. This issue is seen when the Cisco 3900 router is an IPsec endpoint.

  Workaround: Reloading the router is the only way to resolve this issue. Clearing IPsec SAs and/or crypto configuration will not resolve this issue.

- CSCud38774

  Symptoms: Router is showing CPU utilization at 99%. LDAP seems to be hogging the CPU process.

  Conditions: This issue can occur randomly at any point of time where NTLM authentication is deployed. This issue is observed only when the server is not able to handle the churn of requests and requests are being stuck at Bind On-Going state, which can be verified with **show ldap server** *server-name* **connections**.

  Workaround: Clearing LDAP server connections helps in resolving this issue:

  clear ldap server *server-name*.

- CSCud42529

  Symptoms: Router crashes when receiving IPv6 ICMP packet.

  Conditions: The symptom is observed when ISM-VPN is used as a crypto engine. This does not occur when using an onboard crypto engine.

  Workaround: There is no workaround.

- CSCud42938

  Symptoms: After a **clear crypto session**, sometimes ident SM remains at responder side.

  Conditions: Doing 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 never come up.

  Workaround: Router reboot.

- CSCud46314

  Symptoms: The Cisco router crashes when polling ciscoEnvMonSupplyStatusDescr MIB.

  Conditions: The ciscoEnvMonSupplyStatusDescr MIB is getting polled.

  Workaround: Apply the following to block the view:

  - snmp-server view blockmib iso include
  - snmp-server view blockmib 1.3.6.1.4.1.9.9.13.1.5.1.2 exclude

  Similarly apply the following to the community:

  snmp-server community <community> view blockmib ro

- CSCud46826

  Symptoms: The Cisco 7200 VSA may stop encrypting outbound traffic for some SAs in a dual-Hub Phase 3 DMVPN setup. Inbound traffic is decrypted correctly by the Cisco 7200 Hub. Only outbound traffic is affected. The following error can sometimes be seen:

  ```
  Dec 1 2012 18:24:39.261 MSK: %VPN_HW-1-PACKET_ERROR: slot: 0 Packet
  Encryption/Decryption error, Invalid
  SA:srcadr=192.168.200.5,dstadr=192.168.200.11,size=88
  ```

  This error causes EIGRP flapping on the Hub due to unidirectional connectivity. For example:

  ```
  Dec 1 2012 18:11:43.779 MSK: %DUAL-5-NBRCHANGE: EIGRP-IPv4 77: Neighbor 192.168.20.20
  (Tunnel1) is down: retry limit exceeded Dec 1 2012 18:11:46.107 MSK:
  %DUAL-5-NBRCHANGE: EIGRP-IPv4 77: Neighbor 192.168.20.20 (Tunnel1) is up: new
  adjacency
  ```

  EIGRP may come up on a spoke, but it eventually goes down with:

  ```
  Dec 1 2012 18:10:23.317 MSK: %DUAL-5-NBRCHANGE: EIGRP-IPv4 77: Neighbor 192.168.20.3
  (Tunnel1) is down: holding time expired
  ```

  Conditions: This symptom is observed with Cisco 7200. The issue is not seen with software crypto engine. The issue is not seen on the Cisco ASR 1000 Hub with Cisco IOS Release 15.2(4)S1 and the same configuration. The issue is not seen in a test setup if a single Spoke is connected. The issue with one IPsec SA can be resolved by clearing this SA, but it may affect another SA that was working before. It was noticed that first Phase 2 rekey may resolve the issue completely.

  To diagnose this issue, check if the “pkts encaps” counter is incremented:

  ```
  BSNS-7200-1#show crypto ipsec sa peer 192.168.200.10 | i ident|caps
     local  ident (addr/mask/prot/port): (192.168.200.5/255.255.255.255/47/0)
     remote ident (addr/mask/prot/port): (192.168.200.10/255.255.255.255/47/0)
      #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
      #pkts decaps: 130, #pkts decrypt: 130, #pkts verify: 130
  ```

```
BSNS-7200-1#show crypto ipsec sa peer 192.168.200.10 | i ident|caps
   local  ident (addr/mask/prot/port): (192.168.200.5/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.200.10/255.255.255.255/47/0)
    #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
    #pkts decaps: 132, #pkts decrypt: 132, #pkts verify: 132
```

Workaround: This issue is not seen in Cisco IOS Release 15.1(4)M3a. Cisco IOS Release 15.1(4)M5 is known to be affected.

- CSCud53687

  Symptoms: Packets sourced from a registered application port for which ALG support is present may be incorrectly classified as ALG, and therefore the session is dropped.

  An example is an application that uses TCP source port 1720 to establish a connection with a remote device. The router performing NAT incorrectly marks this packet as needing ALG processing ultimately resulting in the connection failing.

  Conditions: This symptom occurs when you use one of the registered source ports that support ALG processing and NAT.

  Workaround: You can disable the NAT ALG fixup for the particular protocol which port number matches with the non-ALG traffic's source port. But this will restrict the coexistence of ALG as well as non-ALG traffic with the same source port.

- CSCud54133

  Symptoms: During the FIPS code review, a non-conformance was found. Specifically, when the SP 800-90 Deterministic Random Bit Generator (DRBG) calls the ACT chip for a seed, there is no Continuous Random Number Generator Test applied to the value output from the chip.

  Conditions: The symptom is observed when the SP 800-90 DRBG calls the ACT chip for a seed, there is no Continuous Random Number Generator Test applied to the value output from the chip.

  Workaround: There is no workaround.

- CSCud59176

  Symptoms: Backing out the fix CSCub95141.

  Conditions: The symptom is observed with the fix for CSCub95141.

  Workaround: There is no workaround.

- CSCud67779

  Symptoms: One-way audio is observed when a call goes through BACD and comes over SIP trunk.

  Conditions: This symptom occurs 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.

- CSCud67792

  Symptom: Invalid modem detected

  Conditions: during bootup

  Workaround: Use 15.2t based images.

  CSCud69078

  Symptoms: In a GETVPN setup, when using the ISM module, decryption fails and the original (ESP) packet gets forwarded to a destination which eventually will get dropped.

  Conditions: This symptom is observed when the same GETVPN crypto map is applied on two or more different interfaces on the router with ISM.

Workaround:

1. Switch to onboard or sw encryption.
2. To get encryption/decryption working on one interface, remove the crypto map from both interfaces, shut/no shut both interfaces, and then reapply the crypto map on one of the interfaces.

- CSCud74552

  Symptoms: Ping on the EHWIC-1GE-SFP-CU interface fails.

  Conditions: This symptom is observed when ISM-VPN is installed. However, it is not necessarily utilized for encryption/decryption.

  Workaround: There is no workaround.

- CSCud99034

  Symptoms: Data encapsulation fails in the Cisco IOS Release 15.3(1.11)T image.

  Conditions: This symptom occurs when ISM-VPN is enabled as the crypto engine.

  Workaround: Disable ISM-VPN and use either the Onboard crypto engine or the Software crypto engine.

- CSCue05844

  Symptoms: The Cisco 3925 router running Cisco IOS Release 15.0(2)SG reloads when connecting to a call manager.

  Conditions: This symptom is observed with the Cisco 3925 router running Cisco IOS Release 15.0(2)SG.

  Workaround: Remove SNMP.

- CSCue06116

  Symptoms: VG350 gateway crashes when the configuration file is downloaded from CUCM. This occurs when the VG350 has 144 ports configured.

  Conditions: The VG350 supports a maximum of 144 FXS ports. Configure MGCP control and download configuration from CUCM, gateway crashes.

  Workaround: Use **no ccm-manager config** to stop the configuration download from CUCM.

Resolved Caveats—Cisco IOS Release 15.2(4)M2

- CSCsq83006

  Symptoms: When some port-channels go down at the same time on a router, it can cause EIGRP SIA errors.

  Conditions: The symptom occurs with full mesh four routers which are connected via port-channels. Additionally, it occurs with over five routers which are connected via a partial mesh port-channel.

  Workaround: Use the port-channel interface settings below:

  ```
  (config)# interface port-channel <port-channel interface number>
  (config-if)# bandwidth <bandwidth value>
  (config-if)# delay <delay value>
  ```

  Further Problem Description: If a test is done with a physical interface, not a port-channel, this issue is not seen.

- CSCsy93069

Symptoms: After a period of telepresence calls, tracebacks and then a router crash is seen.

Conditions: The symptom is observed only when running Cisco IOS firewall with l7 SIP inspect policies applied. This crash happens at low scale with one CTS 3k call cycling with a hold time of 600 secs.

It occurs intermittently and over time in an environment where there may be some call failures.

Workaround: There is no workaround.

- CSCtj59117

  Symptoms: The following error message is seen and the router freezes and crashes:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle
  ```
  A reload is required to recover.

  Conditions: The symptom is observed on a Cisco 1803 that is running Cisco IOS Release 12.4(15)T12 or Release 12.4(15)T14.

  Workaround: Remove CEF.

- CSCtk15666

  Symptoms: IOS password length is limited to 25 characters.

  Conditions: IOS password length is limited to 25 characters on NG3K products.

  Workaround: There is no workaround.

- CSCto88178

  Symptoms: Packet corruption is observed when NAT processes an H.323 packet that has some trailing data beyond the User-User Information Element.

  Conditions: This symptom occurs when NAT is configured to process H.323 packets, and it encounters an H.323 packet that has some trailing data beyond the User-User Information Element.

  Workaround: Although it is not feasible for most implementations, using the **no ip nat service H225** command prevents the packet corruption. Additionally, this issue is not present in those releases that have NAT TCP ALG support enabled.

- CSCtq91063

  Symptoms: A Cisco router may unexpectedly reload due to bus error or generate a spurious access.

  Conditions: The issue occurs due to the F/S particle pool running out of free particles and the next packet failing to successfully obtain a particle. The F/S pool is used for fragmentation, so this will only occur when there is a large amount of fragmentation occurring. It has only been seen when there is a "ip mtu 1500" configured on a tunnel interface where the physical mtu is 1500 forcing packets to be fragmented on the physical interface rather than on the tunnel interface.

  Workarounds:

  1. Remove "ip mtu 1500" from the tunnel interface; or
  2. Configure "service disable-ip-fast-frag"; or
  3. Reduce hold queue sizes such that the total size of the queues for all active interfaces in the system does not exceed 512.

- CSCts08224

  Symptoms: Expected ACL/sessions not found for most of the protocols.

  Conditions: The symptom is observed with expected ACL/sessions.

  Workaround: There is no workaround.

- CSCts55778

  Symptoms: This is a problem involving two SAF forwarders, where one is running EIGRP rel8/Service-Routing rel1 and the other is running EIGRP dev9/Service-Routing dev2. The capabilities-manager, a client of the service-routing infrastructure, will advertise 2 services. When forwarders are peering with the same release image, the services propagate between the forwarders without any problems. But, when you run rel8/rel1 on one forwarder, and dev9/dev2 on the other forwarder, a third service appears in the topology table and the SR database that was not advertised. Note: The problem cannot be recreated if both forwarders are running an Cisco IOS XE Release 3.4S or and Cisco IOS XE Release 3.5S image.

  Conditions: This symptom occurs if two SAF forwarders peer with each other, where one SAF forwarder is running EIGRP SAF rel9 or above and the other SAF forwarder is running EIGRP SAF rel8 or below.

  Workaround: Make sure each SAF forwarder is running EIGRP rel8 or below, or rel9 or above.

- CSCts87612

  Symptoms: Traffic over L2TPv3 becomes very slow. Ping shows high latency.

  Conditions: This symptom is observed when EHWIC-1GE-SFP-CU is used as the xconnect interface.

  Workaround: Do shut/no shut on the EHWIC-1GE-SFP-CU interface

- CSCtu07968

  Symptoms: A Cisco 890 router may provide incorrect performance monitor statistics and omit some incoming packets from being handled by flexible netflow.

  Conditions: This is observed when performance monitoring or flexible netflow is enabled with IPsec over a tunnel on an input interface.

  Workaround: There is no workaround.

- CSCtu08373

  Symptoms: Router crashes at various decodes including fw_dp_base_process_pregen and cce_add_super_7_tuple_db_entry_common.

  Conditions: IOS firewall is configured and traffic is flowing through the router.

  Workaround: There is no workaround.

- CSCtu28696

  Symptoms: A Cisco ASR 1000 crashes with **clear ip route ***.

  Conditions: The symptom is observed when you configure 500 6RD tunnels and RIP, start traffic and then stop, then clear the configuration.

  Workaround: There is no workaround.

- CSCtw45480

  Symptoms: Inbound GRE encapsulated traffic is dropped with the “Unknown-l4 sessions drop log” message on the router with ZBFW.

  Conditions: This symptom is observed when router self zone policies are applied and the GRE tunnel is in an intermediate zone between the inside and outside zones.

  Workaround: Remove the self zone policies.

- CSCtw52819

  Symptoms: OQD drops on mGRE tunnel.

Conditions: The symptom is observed with an mGRE tunnel.

Workaround: There is no workaround.

- CSCtw72952

  Symptoms: When the primary path option is deleted in a state where the primary LSP and protected LSP are up, path protection functionality is not working and the tunnel is going down. This is a specific negative testing scenario.

  Conditions: The symptom is observed under the following conditions:

  1. Configure any tunnel with path protection configured.
  2. Delete the path option of primary path.

  Path protection stops working and the tunnel goes down.

  Workaround: Configure multiple path options for the primary LSP.

- CSCtw88689

  Symptoms: A crash is seen while applying the policy map with more than 16 classes with the Cisco 3900e platform.

  Conditions: This symptom occurs when applying the policy map with more than 16 classes.

  Workaround: There is no workaround.

- CSCtx36095

  Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.

  Conditions: This symptom occurs during a line card reload.

  Workaround: There is no workaround.

- CSCtx39953

  Symptoms: KRON policy is causing a system crash.

  Conditions: The symptom is observed when using a Cisco 1921/K9 with Cisco IOS Release 15.2(T) and using KRON to schedule telnet sessions in order to check the state of VPN connections. Below is a configuration sample:

```
kron occurrence START-VPN in 1 recurring
 policy-list START-VPN
!
kron policy-list START-VPN
 cli telnet xx.xx.xx.xx 12 /source-interface GigabitEthernet 0/1 /quiet
 cli telnet yy..yy.yy.yy 42 /source-interface GigabitEthernet 0/1 /quiet
 cli telnet zz.zz.zz.zz. /source-interface GigabitEthernet 0/1 /quiet
where xx yy and zz are ip addresses of the remote hosts
```

  Workaround: There is no workaround.

- CSCtx66046

  Symptoms: The Standby RP crashes with a traceback listing db_free_check.

  Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.

  Workaround: Before removing the address, remove the network statement which covers the address of the loopback interface.

- CSCtx74051

  Symptoms: When doing an ISSU downgrade, IPv6 flexible netflow monitors may be displayed and the running configuration is shown with incorrect sub-traffic types.

  Conditions: This happens on a downgrade to Cisco IOS Release 15.2(1)S (Cisco IOS XE Release 3.5). The monitors affected are those applied to IPv6. For example, CLI such as:

  ```
  interface fa0/0/0
    ipv6 flow monitor monitor-name input
  ```

  Workaround: Netflow code should still capture packets as expected on Cisco IOS Release 15.2(1)S. However, a reboot of the device should be done before saving the running configuration as the affected configuration saved will be incorrect and so will then fail to work on start-up.

- CSCtx80535

  Symptoms: DHCP pool that is configured for ODAP assigns the same IP to multiple sessions.

  Conditions: PPP users receive pool via Radius. The pool is defined on the Cisco 10000 series router to use ODAP. ODAP is receiving the subnets from Radius correctly, and assigns IPs to PPP sessions, but sometimes two users end up having the same IP address.

  Workaround: Clear both sessions sharing the same IP.

- CSCtx85623

  Symptoms: The ATM output queue is stuck, and the dialer loses the IP address. The following error messages are displayed:

  ```
  Jul  5 10:16:45.430: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
  Jul  5 10:16:45.442: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
  Jul  5 10:16:46.430: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  Virtual-Access2, changed state to down
  Jul  5 10:16:46.430: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2,
  changed state to down
  Jul  5 10:16:46.430: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1,
  changed state to down

  Dialer Interface loses IP Address
  n0920ar101#sh ip int brief
  Interface                  IP-Address      OK? Method Status
  Protocol
  Dialer1                    unassigned      YES IPCP   up                    up


  Output Queue is Stuck at 40/40 and Drops increment at the VC Level
  n0920ar101#sh queueing int atm0/3/0
  Interface ATM0/3/0 VC 8/35
  Queueing strategy: fifo
  Output queue 40/40, 830 drops per VC << reaches 40/40 and drops increment at
  the VC level

  sn0920ar101#sh queueing int atm0/3/0
  Interface ATM0/3/0 VC 8/35
  Queueing strategy: fifo
  Output queue 40/40, 833 drops per VC << reaches 40/40 and drops increment drops
  increment at the VC level
  ```

  Conditions: This symptom is observed with a Cisco ISR G1/G2 with HWIC-1ADSL Card, SRE/WAE. Crypto is enabled under the dialer interface, and CEF is also enabled. All these conditions are be necessary to trigger the symptom.

  Workaround 1: Reconfigure PVC(PVC reset will work only 23 times, after which reload is required).

  Workaround 2: Disable the hardware crypto engine accelerator.

Workaround 3: Disable CEF.

Workaround 4: Reload the router.

- CSCty03133

  Symptoms: Memory leak in IPsec key engine process.

  Conditions: The symptom is observed with the following conditions:

  - Scale 1000 IKE * 1 Vrf * 4 IPSec, total 4K IPSec sessions.
  - Multi-SA enabled.
  - CAC=50,DPD=60 periodic.
  - ~10M bidirectional traffic.

  Workaround: There is no workaround.

- CSCty35726

  Symptoms: The following is displayed on the logs:

  ```
  InterOp:Cube-NavTel : LTI: Video Xcode Call with plain Audio FAILS
  ```

  Conditions: This symptom is seen when video Xcode call with plain audio fails.

  Workaround: There is no workaround.

- CSCty65189

  Symptoms: Incoming register packets are dropped at the RP when zone-based firewall (ZBFW) is configured on the RP.

  Conditions: The symptom is observed when ZBFW is configured.

  Workaround: There is no workaround.

- CSCty74859

  Symptoms: Memory leaks on the active RP and while the standby RP is coming up.

  Conditions: The symptom is observed when ISG sessions are coming up on an HA setup.

  Workaround: There is no workaround.

- CSCty86039

  Symptoms: Shut down the physical interface of tunnel source interface. The router crashes with traffic going through some of the tunnels.

  Conditions: This symptom is seen with tunnel interface with QoS policy installed.

  Workaround: There is no workaround.

- CSCty89224

  Symptoms: IOS router may crash under certain circumstances when receiving a mvpnv6 update.

  Conditions: Receive mvpnv6 update.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-3895 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtz01079

  Symptoms: Router crashes with chunk corruption error.

  Conditions: The symptom is observed when configuring “collect application http uri statistics” under an active MACE flow record.

  Workaround: Removing “collect application http uri statistics” will avoid the crash.

- CSCtz13465

  Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.

  Conditions: This symptom is observed with an interface with a policy installed.

  Workaround: There is no workaround.

- CSCtz26735

  Symptoms: SDP process to provision CVO router is broken in Cisco IOS Release 15.2(3)T.

  Conditions: This symptom is seen when we start the SDP process. The connection immediately breaks after the username and password are entered.

  Workaround: There is no workaround.

- CSCtz36906

  Symptoms: Alignment errors seen in a MACE flow record when that record is being exported.

  Conditions: The symptom is observed when the source MAC address is configured in that MACE flow record.

  Workaround: Remove “collect datalink mac source address input” from the MACE record.

- CSCtz37164

  Symptoms: The requests to the RADIUS server are retransmitted even though the session no longer exists, causing unnecessary traffic to RADIUS, and RADIUS getting requests for an invalid session.

  Conditions: This symptom occurs when the RADIUS server is unreachable and the CPE times out the session.

  Workaround: The fix is currently being worked upon. This issue can be seen as per the conditions mentioned above. This issue can be avoided by making sure that the RADIUS server is always reachable.

- CSCtz40460

  Symptoms: A router running Cisco IOS may crash or hang.

  Conditions: This may be seen when SSLVPN is configured with NTLM authentication. NTLM authentication is configured by default.

  Workaround: There is no workaround.

- CSCtz42421

  Symptoms: The device experiences an unexpected crash.

  Conditions: This symptom is observed when Zone-Based Firewalls are enabled. H225 and H323 inspection is being done during the crash. The actual conditions revolving around the crash is still being investigated.

  Workaround: There is no workaround.

- CSCtz44989

  Symptoms: A EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.

Conditions: The issue is seen with IPv6 link-local nexthop. When the EIGRP route is redistributed to BGP VRF, it clears the nexthop information (it become 0.0.0.0). Now this route becomes invalid and BGP is not able to export to another VRF.

Workaround: There is no workaround.

- CSCtz47309

  Symptoms: When using smart defaults in flexVPN, the mode transport may be sent from initiator even if "tunnel" is configured.

  Conditions: First seen on a Cisco ASR that is running Cisco IOS Release 15.2(2)S and a Cisco ISR running Cisco IOS Release 15.2(3)T. It is seen with flexVPN.

  Workaround: Use smart defaults on both sides on of the tunnel.

- CSCtz47595

  Symptoms: Dial string sends digits at incorrect times.

  Conditions: The symptoms are seen with a Cisco 3925 router running Cisco IOS Release 15.2(3)T using PVDM2-36DM modems with firmware version 3.12.3 connecting over an ISDN PRI to an analog modem.

  When using a dial string to dial an extension (or other additional digits), the modem should answer before the dial string is sent. If a comma is used, there should be a pause after connecting before sending the digits. The default value of the digital modem is one second per comma; two commas would be two seconds, three commas = three seconds and so on.

  1. With any number of commas in the string, debugs show the digits are sent at random intervals, sometimes before the call was answered and as much as up to 30 seconds after the call connects, i.e.: 919195551212x,22 or 1212x,,,22.
  2. With no comma in the dial string, the digits are sent immediately after being generated without waiting for a connection, i.e.: 919195551212x22.

  Dialing directly to a number with no extension or extra digits works as expected.

  Workaround: There is no workaround.

- CSCtz50204

  Symptoms: A crash is observed on EzVPN Server if VRF configuration under the ISAKMP profile is modified.

  Conditions: The crash is observed only if there are active sessions at the time of configuration change.

  Workaround: Prior to applying a configuration change, clear the sessions.

- CSCtz50683

  Symptoms: Upon removing 10 x MDLP sessions, one or more hardware adj remains. This happens due to incorrect removal of LSPs.

  Conditions: The symptom is observed when more than eight sub-LSPs occur.

  Workaround: Use no more than eight sub-LSPs.

- CSCtz52843

  Symptoms: The following messages are displayed whenever the ATM link goes down.(Cu is deploying ADSL.)

  ```
  Nov  2 05:27:49 EDT: %SYS-2-BADSHARE: Bad refcount in pak_enqueue,
  ptr=6431A7E8, count=0,
  -Traceback= 0x60BA4218 0x6035E098 0x6035FEC4 0x6064CD48 0x603676F0 0x608BABC8
  0x6065D344 0x60666798
  ```

```
0x602D6240 0x600BA8CC 0x621D75E4 0x6004A188


Nov  2 05:27:49 EDT: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=6431A7E8, count=0,
-Traceback= 0x60BA4218 0x6035937C 0x603600C4 0x6064CD48 0x603676F0 0x608BABC8
0x6065D344 0x60666798
0x602D6240 0x600BA8CC 0x621D75E4 0x6004A188

Nov  4 08:29:27 EST: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to up

Nov  4 08:29:27 EST: %SYS-4-CHUNKMALLOCFAIL: Could not allocate chunks for ATM0/1/0

Total free: 0, Total inuse: 16, Cause : Not a dynamic chunk
 -Process= "ATM Periodic", ipl= 4, pid= 65,  -Traceback= 0x60BA4218 0x6027CB94
0x6027CBF8 0x603837A0
0x6027F688
```

Conditions: This symptom occurs when OAM is used to manage the PVC and the peer interface is down.

Workaround: There is no workaround.

- CSCtz58719

  Symptoms: Watchdog timeout is seen under interrupt or process.

  Conditions: This symptom is observed with a QoS configuration applied. The issue happens because of resource contention between a process path packet and an interrupt path packet.

  Workaround: Disable QoS.

- CSCtz58941

  Symptoms: The router crashes when users execute the **show ip route XXXX** command.

  Conditions: This symptom is observed during the display of the **show ip route XXXX**, when the next-hops of “XXXX” networks are removed.

  Workaround: The **show ip route XXXX** command (without “XXXX”) does not have the problem.

- CSCtz59145

  Symptoms: A crash occurs randomly. The following error messages are often seen before the crash:

```
Mar 31 16:30:16.955 GMT: %SYS-2-MALLOCFAIL: Memory allocation of 20 bytes
failed from 0x644DA7E0, alignment 0
  Pool: Processor  Free: 274176384  Cause: Interrupt level allocation
  Alternate Pool: None  Free: 0  Cause: Interrupt level allocation
  -Process= "<interrupt level>", ipl= 1

  Mar 31 16:30:16.963 GMT: %SYS-3-BADLIST_DESTROY: Removed a non-empty
list(707C0248, name: FW DP SIP dialog list), having 0 elements
```

  This device is not actually running out of memory. There is a memory action going on at the interrupt level which is not allowed.

  Conditions: This symptom occurs when Zone-Based Firewalls inspect SIP traffic. This issue is likely related to the tracebacks and error messages given above. The actual condition is still being investigated.

  Workaround: If plausible, disabling SIP inspection could possibly prevent further crashes.

- CSCtz61599

  Symptoms: After adding performance-monitor policy map under the port-channel interface, it displays continuously “Port-channel1 has more than one active member link”:

```
it-wan-agg5-14(config)#int port-channel 1
```

```
it-wan-agg5-14(config-if)#$performance-monitor input PERF-MON-port-channel
it-wan-agg5-14(config-if)#$performance-monitor output PERF-MON-port-channel
it-wan-agg5-14(config-if)#

Port-channel1 has more than one active member link
Port-channel1 has more than one active member link
```

Conditions: The symptom is observed after adding performance-monitor policy map under the port-channel interface.

Workaround: There is no workaround.

- CSCtz69084

  Symptoms: The switch crashes when trying to enable IPsec MD5 authentication on the SVI.

  Conditions: This symptom is observed with the following conditions:

  ```
  VLAN 101
  SW1---------------SW2
  ```

  1. Configure the IPsec MD5 authentication in global configuration mode.

  ```
  ipv6 router ospf 1
   area 0 authentication ipsec spi 1000 md5 123456ABCDEF123456ABCDEF123456AB
  ```

  2. Configure the IPsec MD5 authentication as below in the interface mode with MD5 key 7 and device crashes.

  Workaround: There is no workaround.

- CSCtz71084

  Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.

  Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:

  CE0------------------PE0---------------------RR

  CE1------------------PE1----------------------|

  Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.

  This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix: no network x.x.x.x mask y.y.y.y

  Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external, and is day 1 issue with all.

  Workaround: Hard clear.

- CSCtz72390

  Symptoms: The name mangling functionality is broken. Authorization fails with the “IKEv2:AAA group author request failed” debug message.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T.

  Workaround: There is no workaround.

- CSCtz73836

  Symptoms: The router crashes.

  Conditions: This symptom is observed when the router is running NHRP.

  Workaround: There is no workaround.

- CSCtz75071

  Symptoms: CSCty98523 is not fully published in Cisco IOS Release 15.2M&T.

  Conditions: This symptom is observed with CSCty98523. CSCty98523 has changes in the “crypto” and “crypto_engine” components. However, only the “crypto” changes got published in the Cisco IOS Release 15.2M&T code branch. It was causing issues for IKEv2 crypto engine operations. This DDTS was raised to publish the “crypto_engine” change part of CSCty98523 in the Cisco IOS Release 15.2M&T code branch.

  Workaround: There is no workaround.

- CSCtz77171

  Symptoms: Subscriber drops are not reported in mod4 accounting.

  Conditions: This symptom is observed on checking policy-map interface for account QoS statistics on a port-channel subinterface.

  Workaround: There is no workaround.

- CSCtz80643

  Symptoms: A PPPoE client’s host address is installed in the LNS’s VRF routing table with the **ip vrf receive** *vrf name* command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

  Conditions: This symptom is observed only when the Virtual-access interface is configured with the **ip vrf receive** *vrf name* command via the Virtual-Template or RADIUS profile.

  Workaround: There is no workaround.

- CSCtz86763

  Symptoms: Sessions remain partially created, and memory is consumed and not returned.

  Conditions: This symptom occurs when sessions are churned and reset before they reach active state.

  Workaround: There is no workaround.

- CSCtz89334

  Symptoms: A traffic blackhole is seen while a single pair of 4-wire EFM bond connections is down on a Cisco 888E router.

  Conditions: This symptom occurs when connecting to an Ericsson DSLAM from a Cisco 888E router.

  Workaround: There is no workaround.

- CSCua01641

  Symptoms: The router's NAS-IP address contained in the RADIUS accounting-on packet is 0.0.0.0:

  ```
  RADIUS:  Acct-Session-Id     [44]  10  "00000001"
  RADIUS:  Acct-Status-Type    [40]  6   Accounting-On
          [7]
  RADIUS:  NAS-IP-Address      [4]   6   0.0.0.0

  RADIUS:  Acct-Delay-Time     [41]  6   0
  ```

Conditions: Occurs when you restart the router.

Workaround: There is no workaround.

- CSCua06598

  Symptoms: Router may crash with breakpoint exception.

  Conditions: The symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.

  Workaround: Disable SNMP IPv6 polling.

- CSCua07791

  Symptoms: A Cisco ISR G2 running Cisco IOS Release 15.2(2)T or later shows a memory leak in the CCSIP_SPI_CONTRO process.

  Conditions: The leak is apparent after 3-4 weeks. The process is CCSIP_SPI_CONTRO.

  Workaround: There is no workaround.

- CSCua10556

  Symptoms: A few IKEv2 SAs get stuck in delete state.

  Conditions: The symptom is observed when bringing up 2k flex sessions.

  Workaround: There is no workaround.

- CSCua15003

  Symptoms: When a call is canceled mid-call, the CUBE may not release the transcoder resource for the call. As a result, there is a DSP resource leak.

  Conditions: The problem can happen in the following situation:

  - CUBE receives 180 ringing with SDP session.
  - “media transcoder high-density” is enabled.

  Workaround: Disable “media transcoder high-density”.

- CSCua18166

  Symptoms: When sub appid is triggered by end points, the network does not recognize it and displays it as “Unknown identifier”.

  Conditions: This symptom occurs when the limitation results in not supporting traffic classification based on sub appid.

  Workaround: There is no workaround.

- CSCua19207

  Symptoms: A Cisco ASR 1000 is unable to support class-default shaping on subinterface used with tunnel QoS from the Cisco IOS XE 3.1 Release.

  Conditions: This occurs on a Cisco ASR 1000 when trying to configure class-default shaping on a subinterface used with tunnel QoS.

  Workaround: There is no workaround.

- CSCua19425

  Symptoms: RP crashes at the far end, pointing to Watchdog Process BGP.

  Conditions: This symptom is observed when doing an FP reload at the near end. This issue is seen with EBGP sessions with BFD configured between near end and far end routers.

  Workaround: There is no workaround.

- CSCua19933

  Symptoms: Crash at mace_dp_add_or_remove_from_feature_path.

  Conditions: The symptom is observed when mace is configured and is removed from the interface while router is passing traffic.

  Workaround: There is no workaround.

- CSCua21166

  Symptoms: Unable to form IPSec tunnels due to error: "RM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with securityk9 technology package license."

  Conditions: Even though the router does not have 225 IPsec SA pairs, error will prevent IPSec from forming. Existing IPSec SAs will not be affected.

  Workaround: Reboot to clear out the leaked counter, or install hsec9 which will disable CERM (Crypto Export Restrictions Manager).

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 2.8/2.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:M/C:N/I:N/A:P/E:U/RL:W/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCua21171

  Symptoms: Ping will not pass between a few Distributed LFI over ATM (dLFIoATM) bundles.

  Conditions: The symptom is observed after configuring a few dLFIoATM bundles. Check the ping between bundles and perform a shut/no shut of the interface.

  Workaround: There is no workaround.

- CSCua21201

  Symptoms: RP2 reloads unexpectedly.

  Conditions: The symptom is observed with one dynamic crypto map with 8k tunnels running 700Mbps 64B packets overnight.

  Workaround: There is no workaround.

- CSCua23217

  Symptoms: Ping failure observed.

  Conditions: The symptom is observed with DSL group pairs configured on controllers.

  Workaround: There is no workaround.

- CSCua24689

  Symptoms: Fragments are sent without label resulting in packet drops on the other side.

  Conditions: The symptom is observed with the following conditions:

  - MPLS enabled DMVPN tunnel on egress.
  - VFR on ingress.

  Workaround: Disable VFR if possible.

- CSCua27852

  Symptoms: Traffic loss is seen in pure BGP NSR peering environment.

Conditions: The symptom is seen on a Cisco router that is running Cisco IOS Release 15.2(2)S, and the BGP peerings to CEs and RR are all NSR enabled.

Workaround: Enable the **bgp graceful-restart** command for RR peering.

- CSCua28346

  Symptoms: A router crashes during second rekey.

  Conditions: This symptom occurs with IKEv2 with RSA authentication.

  Workaround: There is no workaround.

- CSCua30053

  Symptoms: Authentication is failing for clients after some time because the radius_send_pkt fails, because it complains about the low IOMEM condition.

  Conditions: In AAA, minimum IO memory must be 512KB to process the new request. If the memory is less than this, AAA does not process the new authentication request. This is AAA application threshold. This application barriers are not valid in dynamic memory case. Such conditions are removed for NG3K platform.

  Workaround: There is no workaround.

- CSCua32379

  Symptoms: Cisco ASR 1000 hubs crash at crypto_ss_set_ipsec_parameters.

  Conditions: The symptom is observed with dual-hubs switchover between active-standby and active-active.

  Workaround: There is no workaround.

- CSCua37898

  Symptoms: Memory leaks are observed with @crypto_ss_enable_ipsec_profile on VSS.

  Conditions: The memory leaks are seen when OSPFv3 authentication is enabled over virtual link, and the OSPFv3 process is restarted.

  Workaround: There is no workaround.

- CSCua39107

  Symptoms: In a FlexVPN Spoke to Spoke setup, Resolution reply goes via the Tunnel interface to the Hub.

  Conditions: This symptom is only observed when NHO is added for the V-Access, overriding an existing route. This issue is not seen when H route is added.

  Workaround: Distribute the summarized address from the Hub, thus avoiding addition of NHO at the Spokes. The Spokes will then add H route instead of NHO.

- CSCua39390

  Symptoms: The PRI configuration (voice port) is removed after a reload:

  ```
  interface Serial1/0:23          ^
  % Invalid input detected at '^' marker.
  no ip address
  % Incomplete command.
  encapsulation hdlc
     ^
  % Invalid input detected at '^' marker.
  isdn incoming-voice voice
         ^
  % Invalid input detected at '^' marker.
  no cdp enable
  ```

```
        ^
% Invalid input detected at '^' marker.
voice-port 1/0:23
              ^
% Invalid input detected at '^' marker.
Also getting trace back
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F0478z 0x607F72C0z 0x60722F38z 0x6070A300z
0x6070A9CCz 0x603E1680z 0x6029541Cz 0x60298F6Cz 0x6029AD48z 0x6029D384z
0x6062BC68z 0x60632424z 0x60635764z 0x60635CE0z 0x60877F2Cz
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F04E4z 0x607F7154z
```

Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T and Release 15.1(4)M4. The issue is not occurring with Cisco IOS Release 12.4(24)T6 or lower. The issue occurs after reload.

Workaround: Reapply configuration after router comes back up.

- CSCua40273

  Symptoms: The ASR1k crashes when displaying MPLS VPN MIB information.

  Conditions: Occurs on the ASR1K with version 15.1(02)S software.

  Workaround: Avoid changing the VRF while querying for MIB information.

- CSCua40790

  Symptoms: Memory leaks when SNMP polling cbgpPeer2Entry MIB.

  Conditions: This symptom occurs when BGPv4 neighbors are configured.

  Workaround: There is no workaround if this MIB is to be polled.

- CSCua42523

  Symptoms: Router crashes and reloads when “options-keepalive” is enabled on a dial-peer which has session target as sip-server.

  Conditions: The symptom is observed when enabling “options-keepalive” which has a session target as sip-server. Also, “sip-server” is configured under “sip-ua” and has a DNS address which resolves to an IPv6 address.

  Workaround: Do not enable “options-keepalive” for dial-peer.

- CSCua44462

  Symptoms: DNS reply is not cached.

  Conditions: DNS based X25 routing. DNS server is reachable via IPsec over Gig link and SHDSL links. There are Cisco devices at different locations. Few of them are communicating to DNS server via IPsec over Gig link and few of them are communicating via IPsec over ATM (EHWIC-4SHDSL-EA and HWIC-4SHDSL). It is seen that the UDP reply contains the x25 address to IP address resolution but it is not being used by the router causing X25 calls to fail.

  Workaround: There is no workaround.

- CSCua45122

  Symptoms: Multicast even log preallocated memory space needs to be conserved on the low-end platform.

  Conditions: This symptom is observed with multicast even log.

  Workaround: There is no workaround.

- CSCua47570

Symptoms: The **show ospfv3 event** command can crash the router.

Conditions: The symptom is observed when "ipv4 address family" is configured and redistribution into OSPFv3 from other routing protocols is configured.

Workaround: Do not use the **show ospfv3 event** command.

- CSCua48060

  Symptoms: A Cisco 3945 UUT router reloads after applying PPP and AAA authentication as well as authorization. The same issue is seen for other platforms, namely Cisco 1803 and Cisco 3845 for the same script.

  Conditions: The symptom is observed when applying the AAA and PPP configurations with Cisco IOS interim Release 15.2(3.16)M0.1.

  Workaround: There is no workaround.

- CSCua49764

  Symptoms: The WAAS-Express device goes offline on WCM.

  Conditions: This symptom occurs when a certificate is generated using HTTPS when using the Cisco IOS Release 15.1(3)T image. Once upgraded to Cisco IOS Release 15.2(3)T, the WAAS-Express device goes offline on WCM.

  Workaround: Configure an rsakeypair on the TP-self-signed trustpoint with the same name and execute the **enroll** command again or delete the self-signed trustpoint point and reenable the HTTP secure-server.

- CSCua51991

  Symptoms: An invalid SPI message is seen throughout the lifetime of IPsec SA.

  Conditions: This symptom is observed with SVTI-SVTI with a GRE IPv6 configuration. When bringing up 1K sessions, an invalid SPI is seen. There is also inconsistency between the number of child SAs in IKEv2 and the number of IPsec SAs on the same box.

  Workaround: There is no workaround.

- CSCua55785

  Symptoms: Build breakage due to fix of CSCtx34823.

  Conditions: This issue occurs with CSCtx34823 fix.

  Workaround: CSCtx34823 change may be unpatched from the code-base.

- CSCua55797

  Symptoms: The **privilege exec level 0 show glbp brief** command causes the memory to be depleted when the **show running** or **copy running-config startup-config** commands are used. The configurations will then show this:

```
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
brief brief brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
brief brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief
    privilege exec level 0 show glbp
    privilege exec level 0 show
```

Removing the configurations causes this to happen over and over until the telnet session is terminated:

```
priv_push : no memory available
priv_push : no memory available
priv_push : no memory available
priv_push : no memory available
priv_push : no memory available
```

If the configurations are saved and device is reloaded, the device will not fully boot until the configurations are bypassed.

Conditions: This issue happens after the **privilege exec level 0 show glbp brief** command is entered and saved.

Workaround: Reload the router before saving the configurations.

- CSCua56184

  Symptoms: Multiple RP switchovers occur within a very short span of time.

  Conditions: The symptom is observed with multiple RP switchovers on a Cisco ASR 1000 router and it fails to allocate an IPsec SPI.

  Workaround: There is no workaround.

- CSCua58100

  Symptoms: The syslog is flooded with the following traceback message:

  ```
  Jun 20 10:05:23.961 edt: %SYS-2-NOTQ: unqueue didn't find 7F3D26BDCCD8 in queue
  7F3CA5E4A240 -Process= "RADIUS Proxy", ipl= 0, pid= 223
  -Traceback= 1#e0ee0ce60492fdd11f0b03e0f09dc812  :400000+873623 :400000+2547652
  :400000+20F9217 :400000+6C70C9C :400000+6C69C71 :400000+6C682BC :400000+6C68183
  ```

  Conditions: Occurs under the following conditions:

  - You establish 36k EAPSIM sessions using a RADIUS client on server A.
  - You establish 36k roaming sessions using a RADIUS client on server B.
  - The roaming sessions have the same caller-station-id but use a different IP address than the EAPSIM sessions.

  Workaround: There is no workaround.

- CSCua60100

  Symptoms: Router crashes at ip_acl_peruser_ctxt_free while clearing the calls.

  Conditions: The symptom is observed when an ACL filter is applied on the input direction and then the session is established. When you try to clear the session, the router crashes.

  Workaround: There is no workaround.

- CSCua61814

  Symptoms: Overhead accounting configuration needs to be configured on both parent and child policy, rather than just parent.

  Conditions: The symptom is observed with overhead accounting.

  Workaround: There is no workaround.

- CSCua62545

  Symptoms: After attaching an attribute-map to a protocol, the same is not reflected at the collector when FNF export of options-attribute is enabled.

  Conditions: The symptom is observed when attribute-map is configured and an attribute-set done to one or more protocols.

Workaround: Force an NBAR restart with a reload or protocol pack load etc.

- CSCua63440

  Symptoms: Crash seen on executing **show metadata flow local-flow-id** *id*.

  Conditions: The symptom is observed when "metadata flow" is configured and metadata flows are present in the metadata table.

  Workaround: There is no workaround.

- CSCua67998

  Symptoms: System crashes.

  Conditions: This symptom occurs after adding or removing a policy-map to a scaled GRE tunnel configuration.

  Workaround: There is no workaround.

- CSCua69657

  Symptoms: Traceback is seen when executing the **show clock detail** command.

  Conditions: This symptom is seen when executing the **show clock detail** command with Cisco IOS interim Release 15.3(0.4)T image.

  Workaround: There is no workaround.

- CSCua70065

  Symptoms: CUBE reloads on testing DO-EO secure video call over CUBE when SDP passthru is enabled.

  Conditions: The symptom is observed when running Cisco IOS interim Release 15.3(0.4)T.

  Workaround: There is no workaround.

- CSCua70158

  Symptoms: NBAR fails to recognize traffic with **match protocol http url/host**.

  Conditions: The symptom is seen when "protocol discovery" is enabled.

  Workaround: There is no workaround.

- CSCua71038

  Symptoms: Router crash.

  Conditions: The symptom is observed with a Cisco router that is running Cisco IOS Release 15.2(3)T1. The router may crash during the failover test with OCSP and CRL configured.

  Workaround: Configure OCSP or CRL but not both

- CSCua73419

  Symptoms: Transform set including SHA2 does not work on ISM.

  Conditions: The symptom is observed with esp-sha256-hmac, esp-sha384-hmac, or esp-sha512-hmac.

  Workaround: There is no workaround.

- CSCua77729

  Symptoms: Embedded AP in the Cisco 1941 ISR becomes unreachable after using the "reload in" command on the Cisco ISR CLI. This issue is seen when using "reload in" on the Cisco ISR CLI and choosing the option to reload embedded AP.

  ```
  CISCO1941W-E/K9 Version 15.1(4)M4
  ```

```
AP801 Software (AP801-K9W7-M), Version 12.4(21a)JA1

Router#reload in 10

Do you want to reload the internal AP ? [yes/no]: yes


Do you want to save the configuration of the AP? [yes/no]: no

System configuration has been modified. Save? [yes/no]: no
Reload scheduled for 13:57:01 UTC Mon May 21 2012 (in 10 minutes) by console
Reload reason: Reload Command
Proceed with reload? [confirm]
Router#
May 21 13:47:03.759:
%SYS-5-SCHEDULED_RELOAD:<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi?a
ction=search&counter=0&paging=5&links=reference&index=all&query=SYS-5-SCHEDULED_RELOAD
>
Reload requested for 13:56:51 UTC Mon May 21 2012 at 13:46:51 UTC Mon May 21
2012 by console. Reload Reason: Reload Command.
```

After that, AP becomes unreachable, and the user cannot session to AP with “service-module wlan-ap 0 session”.

Conditions: This symptom is observed when using “reload in” on the Cisco ISR CLI and choosing the option to reload embedded AP. This issue is seen under the following conditions:

```
CISCO1941W-E/K9 Version 15.1(4)M4 AP801 Software (AP801-K9W7-M), Version 12.4(21a)JA1
using the "reload in" command on ISR CLI with Do you want to reload the internal AP ?
[yes/no]: yes
```

Workaround 1: Use “reload in” on the Cisco ISR CLI and do not choose the option to reload embedded AP.

```
Router#reload in 2 Do you want to reload the internal AP ? [yes/no]: no
```

Workaround 2: Use the normal **reload** command.

- CSCua78468

  Symptoms: Under a heavy load, L4F may not forward packets to the scansafe process. Unit may crash while trying to remove scansafe off the interface.

  Conditions: This issue was first identified on a Cisco ISR running the 15.2.4 image.

  Workaround: There is no workaround.

- CSCua78555

  Symptoms: Custom protocol does not retain attributes assigned to them using the attribute-map after loading protocol-pack. It shows unassigned or other (which is default for custom protocols).

  Conditions: The symptom is observed when the attributes of the custom protocol are changed using the attribute-map and any other protocol-pack loaded.

  Workaround: Reconfigure the attributes for the custom protocols after loading protocol-pack.

- CSCua84923

  Symptoms: Following a misconfiguration on a two-level hierarchical policy with a user-defined queue-limit on a child policy, the UUT fails to attach the QoS policy on the interface even when corrected queuing features are used.

  Conditions: This symptom is observed with the following conditions:

  1. The issue must have the user-defined queue-limit defined.
  2. This error recovery defected is confirmed as a side effect with the c3pl cnh compoent project due to ppcp/cce infrastructure enhancement.

Workaround: There is no workaround.

- CSCua85934

  Symptoms: A session provisioning failure is seen in the ISG-SCE interface. The deactivate or disconnect request has the message authenticator wrongly calculated.

  Conditions: This symptom is observed with the ISG-SCE interface.

  Workaround: There is no workaround.

- CSCua86620

  Symptoms: The vmware-view application is not detected/classified.

  Conditions: This symptom is observed when vmware-view applications are used.

  Workaround: There is no workaround.

- CSCua93688

  Symptoms: When pinging from the Cisco 1921 router to connected devices, the response time is unexpectedly slow.

  - round-trip min/avg/max = 8/46/92 ms

  Conditions: This symptom is observed with the EHWIC-1GE-SFP-CU module on Cisco ISR-G2 platforms.

  Workaround: Shut/no shut the EHWIC-1GE-SFP-CU interface. The ping time resumes to normal.

- CSCua94947

  Symptoms: RP crashes when downloading FreeRadius Framed-IPv6-Route on MLPPP sessions.

  Conditions: This symptom occurs when downloading radius Framed-IPv6-Route.

  Workaround: There is no workaround.

- CSCua96106

  Symptoms: MSP is not enabled on Cisco 890 platform images.

  Conditions: This symptom is observed when the **profile flow** global command is not available.

  Workaround: There is no workaround.

- CSCua96354

  Symptoms: Reload may occur when issuing the **show oer** and **show pfr** commands.

  Conditions: This symptom is observed with the following commands:

  - show oer master traffic-class performance
  - show pfr master traffic-class performance

  Workaround: There is no workaround.

- CSCua97209

  Symptoms: The **analysis-module** CLI is missing under “interface GigabitEthernet”.

  Conditions: The symptom is observed with Cisco ISRs running a Cisco IOS Release 15.2(4)M image with either SRE or UCSE modules inserted and the module software publish NAM subsystem capability.

  Workaround: There is no workaround.

- CSCua97981

Symptoms: The Cisco IOS redundancy facility is slow to come up after master router reload and gets stuck in the "final progression" state.

Conditions: This symptom was first seen in Cisco IOS Release 15.2(3)T and was also observed in Cisco IOS Release 15.2(3)T1.

Workaround: Manually reloading the Standby router will resolve the issue.

- CSCua99687

  Symptoms: BFD does not come up with Zone-Based Firewall (ZBFW) applied on the same interface.

  Conditions: This symptom is observed when BFD and ZBFW are configured on a Gigabit interface on a Cisco CGR 2010 running Cisco IOS Release 15.1(4)M4. It works fine on Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCub04345

  Symptoms: ASR-1002-X freezes after four hours with an scaled "path-jitter" sla probe configuration.

  Conditions: The symptom is observed with scaled "path-jitter" sla probe configuration.

  Workaround: There is no workaround.

- CSCub07382

  Symptoms: NHRP cache entry for the spokes gets deleted on NHRP hold timer expiry even though there is traffic flowing through the spoke-to-spoke tunnel.

  Conditions: The symptom is observed with a flexVPN spoke-to-spoke setup.

  Workaround: Configure the same hold time on both tunnel interface and the virtual-template interface.

- CSCub07673

  Symptoms: IPsec session does not come up for spa-ipsec-2g if ws-ipsec3 is also present. "Volume rekey" is disabled on Zamboni.

  Conditions: This symptom occurs if we have "volume rekey" disabled on Zamboni.

  Workaround: Do not disable the volume rekey on Zamboni.

- CSCub10951

  Symptoms: At RR, for an inter-cluster BE case, there are missing updates.

  Conditions: This symptom is observed with the following conditions:

  1. The following configuration exists at all RRs that are fully meshed:
     - bgp additional-paths select best-external
     - nei x advertise best-external
  2. For example, RR5 is the UUT. At UUT, there is,
     - Overall best path via RR1.
     - Best-external (best-internal) path via PE6 (client of RR5): for example, the path is called "ic_path_rr5".
     - Initially, RR5 advertises "ic_path_rr5" to its nonclient iBGP peers, that is, RR1 and RR3.
  3. At PE6, unconfigure the route so that RR5 no longer has any inter-cluster BE path. RR5 sends the withdrawals to RR1 and RR3 correctly.

4. At PE6, reconfigure the route so that RR5 will have "ic_path_rr5" as its "best-external (internal) path". At this point, even though the BGP table at RR5 gets updated correctly, it does not send the updates to RR1 and RR3. They never relearn the route.

Workaround: Hard/soft clear.

- CSCub13317

  Symptoms: Cisco 2900 with VWIC2-2MFT-T1/E1 in TDM/HDLC mode doesn't forward any traffic across the serial interface after certain amount of time.

  Conditions: Configure frame relay over VWIC2 channel-group in TDM/HDLC mode.

  Workaround: Configure VWIC2 channel-group in NMSI mode.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C CVE ID CVE-2012-3918 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCub16372

  Symptoms: In extremely rare cases, an ISR-G2 cannot boot up with certain ROMMON versions with the error "Signature did not verify". So far, only one image is found to have this problem: c3900-universalk9-mz.SPA.152-1.T3.bin.

  Conditions: The issue will happen when all three conditions are met at the same time:

  1. The platform is affected.
  2. The ROMMON version running at the router is within the affected ROMMON version range.
  3. The first calculated hash value is 0 during the IOS image building process.

  Since it is extremely rare that the third condition will occur, so far only one CCO image is found to have this problem.

  Workaround: Upgrading ROMMON to the latest version of 15.0(1r)M16 or 151(1r)T5 will fix the issue completely.

  The ROMMON upgrade can be done using one single CLI command in the router's enable mode:

  ```
  Router# upgrade rom-monitor file flash:<ROMMON_file_name>
  ```

  <ROMMON_file_name> is the ROMMON file name for the specific platform that is downloadable from CCO. For example, C3900_RM2.srec.SPA.150-1r.M16 is the latest ROMMON version for C39xx platforms located at CCO download site: http://www.cisco.com/cisco/software/release.html?mdfid=282774222&flowid=7437&softwareid=280805687&release=15.0%281r%29M16&relind=AVAILABLE&rellifecycle=&reltype=latest.

- CSCub17985

  Symptoms: A memory leak is seen when IPv6 routes are applied on the per-user sessions.

  Conditions: This symptom is seen if IPv6 routes are downloaded as a part of the subscriber profile. On applying these routes to the sessions, a memory leak is observed.

  Workaround: There is no workaround.

- CSCub19471

  Symptoms: Crash during boot up with MACE and SNMP configurations.

Conditions: The symptom is observed when the startup configuration contains MACE type (policy-map type mace) configured with both filter (match access-group) and action (except flow monitor). The SNMP configuration is as follows:

```
flow record type mace mace-record
 collect art all
!
!
flow exporter ndeget
 destination 172.25.215.96
!
!
flow monitor type mace mace-monitor
 record mace-record
!
!
!
class-map match-all mace-class
 match access-group name mace-acl
!
policy-map type mace mace_global
 class mace-class
  flow monitor mace-monitor
!
interface e0/0
 mace enable


ip access-list extended mace-acl
 permit tcp any any
!
snmp-server community public RO
snmp-server community cisco RW
snmp-server ifindex persist
snmp mib persist cbqos
snmp mib persist circuit
```

Reload the router, then during router boot up there will be a crash.

Workaround: Remove SNMP configuration.

- CSCub28913

  Symptoms: The Cisco ISR G2 with VPN-ISM drops packets over an IPsec tunnel-protected Tunnel interface.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T images, when there is a crypto map (static or dynamic) applied to the interface.

  Workaround:

  - Disable the ISM-VPN (issue “no crypto engine slot xx”, where xx is the slot number where the ISM is located).
  - Alternatively, change the configuration to use either static or dynamic VTIs for the tunnels where you need a crypto-map.

- CSCub33470

  Symptoms: Default profiles showing up as custom.

  Conditions: The symptom is observed with a Cisco Catalyst 3000/Catalyst 4000 platform which supports the IP SLA video operation. Has no affect on the operation itself.

  Workaround: There is no workaround.

- CSCub39124

Symptoms: Only secure cookies will be sent to HTTPS (HTTP over SSL) servers. If secure is not specified, a cookie is considered safe to be sent in the clear over unsecured channels.

Conditions: This is the current default behavior.

Workaround: There is no workaround.

Further Problem Description: This defect has been opened to ensure the default value of the webvpn cookie is hardened and includes the secure keyword as per RFC 2109.

- CSCub42920

  Symptoms: Keyserver rejects rekey ACK from GM with message (from **debug crypto gdoi ks rekey all**):

  ```
  GDOI:KS REKEY:ERR:(get:0):Hash comparison for rekey ack failed.
  ```

  The keys and policies in the rekey packet are correctly installed by the GM, but the rekey ACK does not get processed by the keyserver. This leads to rekey retransmissions, GM re-registration, and potential disruption of communication.

  Conditions: Rekey ACK validation in versions Cisco IOS Release 15.2(4)M1 (Cisco ISR-G2) and Cisco IOS Release 15.2(4)S/Cisco IOS XE Release 3.7S (Cisco ASR 1000) is incompatible with other software releases.

  A keyserver that runs Cisco IOS Release 15.2(4)M1 or Cisco IOS Release 15.2(4)S/Cisco IOS XE Release 3.7S will only be able to perform successful unicast rekeys with a GM that runs one of those two versions. Likewise, a keyserver that runs another version will only interoperate with a GM that also runs another version.

  Workaround: Use multicast rekeys.

- CSCub43088

  Symptoms: The following console messages are seen:

  ```
  Delayed UCSE configuration: Wrong module type in slot 2
  ```

  whenever the SRE-SM modules register with IOS version: c2951-universalk9-mz.SPA.152-4.M.

  Conditions: The symptom is observed when you have SM-SRE modules register with the router via RBCP. Typically when the application on the module boots up or when the you issue SRE **sm status** command in IOS.

  Workaround: There is no workaround.

  Further Problem Description: This is a benign message and can be ignored.

- CSCub45809

  Symptoms: Cisco IOS configured for Voice over IP may experience stack corruption due to multiple media loops.

  Conditions: This requires a special configuration of IP features along with disabling the recommended media flow-around command. IOS version 15.2(2)T

  Workaround: Apply media flow-around command.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:U/RL:W/RC:C CVE ID CVE-2012-5044 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCub46570

Symptoms: The image cannot be built with an undefined symbol.

Conditions: This symptom occurs as the commit error triggers the compiling issue.

Workaround: There is no workaround.

- CSCub47910

  Symptoms: Unexpected reboot is seen due to Bus Error when using software version Cisco IOS Release 15.2(4)M1.

  Conditions: This symptom is observed when SSL VPN is configured on the Cisco ISR in Cisco IOS Release 12.5(4)M1, where the CEF process running in the context of SSL is being interrupted or asked for relinquishing of CPU.

  Workaround: There is no workaround.

- CSCub49291

  Symptoms: Static tunnels between hubs and spokes fail to rebuild.

  Conditions: The symptom is observed when you reload the hub on the DMVPN IPv6 setup with DPD on-demand enabled on all spokes.

  Workaround: There is no workaround.

- CSCub51862

  Symptoms: Router crashes when MACE is applied to an interface and traffic is sent through that interface.

  Conditions: The symptom is observed when there is no flow record configured inside any of the MACE flow monitors.

  Workaround: Configure flow records and exporter inside the MACE flow monitors.

- CSCub52892

  Symptoms: Options “log” and “reset” are not configurable in URL filter policy. The existing configuration is removed if upgrading from previous/good releases.

  Conditions: The symptom is observed with the options “log” and “reset” in URL filter policy.

  Workaround: There is no workaround.

- CSCub54872

  Symptoms: A /32 prefix applied to an interface (e.g.: a loopback) is not being treated as connected. This can impact the connectivity of the /32 prefix.

  Conditions: The symptom is observed when the prefix applied to an interface is for a host route (/32 for IPv4 or /128 for IPv6).

  Workaround: Use a shorter prefix.

  Further Problem Description: This issue does not affect software switching platforms.

- CSCub58932

  Symptoms: PA export times shift one minute ahead after a certain period of time. For example, instead of exporting at times 5:00, 5:05, 5:10, 5:15 (a 5 min interval), the export times are shifted to 4:59, 5:04, 5:09 etc.

  Conditions: The conditions are unknown.

  Workaround: There is no workaround. A countermeasure would be restart the PA timer by re-issuing the command **cache timeout update ...**. This will likely remedy the issue.

- CSCub62116

Symptoms: Traceback seen when sending HTTP traffic.

Conditions: The symptom is observed when MACE is enabled on an interface. After several minutes, traceback is seen.

Workaround: There is no workaround.

- CSCub85451

  Symptoms: When scan safe is enabled on the interface, latency may be seen. Some pages may not load at all or show severe latency if the SYN request sent by the ISR does not receive an appropriate SYN ACK response from the Scan Safe Tower.

  Conditions: Scan Safe must be enabled on the interface. In this case, there was an ASA in the path that was doing sequence number randomization.

  Workaround: Disable sequence number randomization on the firewall in the path before the ISR.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2012-4651 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCub85754

  Symptoms: Ping does not work on a Cisco 897VA.

  Conditions: The symptom is observed with an upgrade to 37h DSL firmware.

  Workaround: There is no workaround.

- CSCub91111

  Symptoms: Outgoing packet drop on the HSPA+R7 cellular interface with SWI MC8705 firmware T3.5.x (not released).

  Conditions: The symptom is observed on HSPA+R7 SKU with MC8705 T3.5 firmware (not released firmware).

  Workaround: Use MC8705 firmware T1.x release.

- CSCub91815

  Symptoms: Certificate validation fails with a valid certificate.

  Conditions: This symptom is observed during DMVPN setup with an empty CRL cache. This issue is usually seen on the responder side, but the initiator can also show this behavior.

  Workaround: There is no known workaround.

- CSCuc07799

  Symptoms: The router crashes while booting with Cisco IOS Release 15.2(4)M weekly images.

  Conditions: This symptom occurs when the ISM-VPN Module is inserted in the router.

  Workaround: There is no workaround.

- CSCuc37365

  Symptoms: The **bandwidth** command under the cellular interface goes back to the default bandwidth of 50K after a reload or modem reset/power-cycle.

  Conditions: The symptom is observed when you configure the **bandwidth** command.

  Workaround: There is no workaround.

- CSCuc47675

  Symptoms: Traffic blackhole when a single pair of 4-wire EFM bond connection is down on a Cisco 888E router.

  Conditions: The symptom is observed when connecting to a third-party vendor DSLAM from a Cisco 888E router.

  Workaround: There is no workaround.

- CSCuc56259

  Symptoms: A Cisco 3945 that is running 15.2(3)T2 and running as a voice gateway may crash. Just prior to the crash, these messages can be seen:

  ```
  %VOIP_RTP-6-MEDIA_LOOP: The packet is seen traversing the system multiple times
  ```

  and

  ```
  Delivery Ack could not be sent due to lack of buffers.
  ```

  Conditions: This happens when a media loop is created (which is due to misconfiguration or some other call forward/transfer scenarios).

  Workaround: Check the configurations for any misconfigurations, especially with calls involving CUBE and CUCM.

- CSCuc82992

  Symptoms: The router crashes upon execution of “no crypto engine slot 0”.

  Conditions: This symptom occurs when RG-Infra and ISM-VPN are configured and when issuing “no crypto engine slot 0”.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)M1

Cisco IOS Release 15.2(4)M1 is a rebuild release for Cisco IOS Release 15.2(4)M. The caveats in this section are resolved in Cisco IOS Release 15.2(4)M1 but may be open in previous Cisco IOS releases.

- CSCub34396

  Symptoms: Because of the fix for CSCtw52819, non-NHRP process-switched packets are noticed to go as clear text.

  Conditions: This symptom is noticed with a DMVPN configuration.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(4)M

All the caveats listed in this section are open in Cisco IOS Release 15.2(4)M. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCth20872

  Symptoms: The following error message is seen accompanied by a reset of the fastethernet:

  ```
  %C870_FE-3-TXERR: FastEthernet0: Fatal transmit error. Restarting...
  ```

  Conditions: The symptom is observed on a Cisco 877 router that is running Cisco IOS Release 12.4(24)T3.

  Workaround: There is no workaround.

- CSCth71093

  Symptoms: Routers configured to dump core to flash: or flash0: fail to dump correctly to 4GB CompactFlash card.

  Conditions: The symptom is observed with the following configuration:

  ```
  (Cisco 3925) exception flash all flash0:
  (Cisco 3825) exception flash all flash:
  ```

  Then when you issue a **wr core**, it fails to dump core files.

  Workaround: Dump cores to TFTP.

- CSCto08904

  Symptoms: RTP operations fail to run when using multiple operations.

  Conditions: The symptom is observed when more than 16 RTP operations are running. Operations start failing due to scaling issues.

  Workaround: There is no workaround.

- CSCtq23960

  Symptoms: A Cisco ISRG2 3900 series platform using PPC architecture crashes and generates empty crashinfo files:

  ```
  show flash: all
  -#- --length-- -----date/time------ path
  <<snip>>
  2           0 Mar 13 2011 09:40:36 crashinfo_<date>
  3           0 Mar 13 2011 12:35:56 crashinfo_<date>
  4           0 Mar 17 2011 16:14:04 crashinfo_<date>
  5           0 Mar 21 2011 05:50:58 crashinfo_<date>
  ```

  Conditions: The symptom is observed with a Cisco ISRG2 3900 series platform using PPC architecture.

  Workaround: There is no workaround.

- CSCtr47084

  Symptoms: Changing zone from multilink interface and replacing the entire configuration by doing a **config replace flash:***config-file-name* crashes the router.

  Conditions: The symptom is observed when traffic is running.

  Workaround: There is no workaround.

- CSCtr63128

  Symptoms: A Cisco 2951 crashes with “Unexpected exception to CPU: vector 1400, PC = 0x55629DC , LR = 0x5562948” and following traceback:

  ```
  -Traceback= 0x55629DCz 0x5977F74z 0x5584BC4z 0x5584134z 0x5507988z 0x5509DB8z
  0x83D0DE8z 0x83D82C4z 0x67F14A8z 0x67F6EB8z 0x67F7150z 0x87ADE04z 0x87AD7DCz
  0x87AFB00z 0x87B0830z 0x87B0910z
  ```

  Conditions: The symptom is observed with a Cisco 2951 router that is configured with IPSec/GRE tunnels, QoS and netflow configured. Same crash is seen on c3925 as well. But crash is not seen on c1921router with same identical conditions. Crash is seen with/without QoS config. Disabling MFIB from all the tunnel interface works fine. Disable the Hardware crypto engine also works fine.

  Crash seen when maximum multicast throughput is reached with the following traffic mix: packet size of 66, 256, 512, and 1024 bytes with a weight of 40, 30, 5 and 21 respectively.

  With the mix causing the crash, the maximum observed multicast throughput seen is 170 Mbps, 27.44 Mbps, and 42 Mbps for c3925, c2951, and c1951 respectively. This seems to indicate a multicast performance issue.

Workaround: There is no workaround.

- CSCts53278

  Symptoms: Garbled voice quality with occasional periods of silence followed by a loud pop when analog STE is in secure mode with LOW line quality setting.

  Conditions: The symptom is observed with a VG224 or Cisco 2811 that is running Cisco IOS Release 15.1(4)M and connected to analog STEs with LOW line quality setting.

  Workaround: Use Cisco IOS Release 12.4(15)T14 where voice quality is still a bit garbled but there are no periods of silence or loud pops.

- CSCtt40285

  Symptoms: There is a router crash. The following message is seen:

  ```
  System returned to ROM by bus error at PC 0x629D2EBC, address 0xB0D0B11 at Address
  Error (load or instruction fetch) exception, CPU signal 10, PC = 0x629D2EBC
  ```

  Conditions: The symptom is observed when using Cisco IOS Release 15.1(4)M2 and with NAT configured.

  Workaround: There is no workaround.

- CSCtu02543

  Symptoms: The assigned address for an EzVPN client is not freed up after a disconnect.

  Conditions: This is seen if there is another L2L tunnel terminating on the same interface of the EzVPN server.

  Workaround: There is no workaround.

- CSCtu08373

  Symptoms: Router crashes at various decodes including fw_dp_base_process_pregen and cce_add_super_7_tuple_db_entry_common.

  Conditions: IOS firewall is configured and traffic is flowing through the router.

  Workaround: There is no workaround.

- CSCtu54300

  Symptoms: Router crashes when you try to unconfigure the crypto.

  Conditions: The symptom is observed when you clear the crypto and VRF configuration using automated scripts. The crash seen after the test is repeated three or four times. Before the crash the VRF and crypto features/functions are working fine.

  Workaround: There is no workaround.

- CSCtw73696

  Symptoms: Router crashes while running in an exec session.

  Conditions: The symptom is observed when an exec session is present.

  Workaround: There is no workaround.

- CSCtw80814

  Symptoms: Crash may be seen when trying to disconnect an SSH session.

  Conditions: The conditions are still under investigation.

  Workaround: There is no workaround.

- CSCtw89123

  Symptoms: A router may crash after configuring “ppp fragment delay”.

Conditions: The symptom is observed when "ppp fragment delay" is configured on a multilink interface and traffic crosses the device.

Workaround: There is no workaround.

- CSCtx23421

  Symptoms: Leaks at crypto_ceal_duplicate_pak and pak_subblock_allocate.

  Conditions: The symptom is observed when the DMVPN spoke has an IPSLA configuration and link flapping is done.

  Workaround: There is no workaround.

- CSCtx37569

  Symptoms: A BLF button (with a ephone-dn) that has been configured for park-slot turns red when a call is parked. But sometimes, after the call has been retrieved, the button stays red and remains red until the phone restarts.

  Conditions: The symptom is observed with a BLF button (with a ephone-dn) that has been configured for park-slot.

  Workaround: Restart the phone to clear the BLF button.

- CSCtx39953

  Symptoms: KRON policy is causing a system crash.

  Conditions: The symptom is observed when using a Cisco 1921/K9 with Cisco IOS Release 15.2(T) and using KRON to schedule telnet sessions in order to check the state of VPN connections. Below is a configuration sample:

```
kron occurrence START-VPN in 1 recurring
 policy-list START-VPN
!
kron policy-list START-VPN
 cli telnet xx.xx.xx.xx 12 /source-interface GigabitEthernet 0/1 /quiet
 cli telnet yy..yy.yy.yy 42 /source-interface GigabitEthernet 0/1 /quiet
 cli telnet zz.zz.zz.zz. /source-interface GigabitEthernet 0/1 /quiet
where xx yy and zz are ip addresses of the remote hosts
```

  Workaround: There is no workaround.

- CSCtx52157

  Symptoms: SM-ES3G-24-P module installed in a Cisco 3925E chassis shows status as failed.

  Conditions: The symptom is observed with an SM-ES3G-24-P module installed in a Cisco 3925E chassis.

  Workaround: Reload SM-ES3G-24-P switch module.

- CSCtx55113

  Symptoms: A device running Cisco IOS Release 15.2(2)T with an EHWIC-1GE-SFP-CU may experience a situation where the tx is stuck, and the interface stops transmitting traffic.

  Conditions: The issue can be seen in the **show interface** output where the output queue fills to the maximum and does not decrease:

```
Output queue: 40/40 (size/max)
```

  And output drops continue to increment:

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: XXXXXX
```

  The link appears to be unidirectional (for example: CDP neighbors are still seen, but device is not viewed as a CDP neighbor by the peer). If pings are sent from the adjacent device they appear to arrive, but are not responded to.

Workaround 1: Issuing a **shutdown** and then a **no shutdown** on the interface resolves the issue temporarily.

Workaround 2: Enable “flow control” on the peer device.

- CSCtx56183

  Symptoms: Router crashes due to block overrun:

  ```
  %SYS-3-OVERRUN: Block overrun at 49156754 (red zone 66616365)
  -Traceback= 42806C04z 42809B20z 42809D14z 427AD988z 427AD96Cz
  .
  .
  %SYS-6-BLKINFO: Corrupted redzone blk 49156754....
  .
  %SYS-6-MEMDUMP: 0x49156754: 0xAB1234CD 0x12A0000 0x12C 0x44395148
  %SYS-6-MEMDUMP: 0x49156764: 0x419B243C 0x49157154 0x49156658 0x800004E8
  %SYS-6-MEMDUMP: 0x49156774: 0x1 0x0 0x1000133 0x47D7699C
  ```

  Conditions: This issue is seen when Websense URL filtering enabled and long URLs have been accessed.

  Workaround 1: Disable URL filtering.

  Workaround 2: Do not invoke long URLs.

- CSCtx65384

  Symptoms: L2TPv3 session is not re-established when pseudowire is configured with loopback address and the loopback interface is deleted and re-added.

  Conditions: This issue is seen when the local interface used is a loopback interface and the loopback is removed and re-added. This issue was seen with a Cisco 2800 router loaded with Cisco IOS interim Release 15.2(1)T1.11.

  Workaround: Remove and re-add the pseudowire-class after adding the loopback interface.

- CSCtx66904

  Symptoms: The router will hang until manually power cycled. The device will crash and recover if the **scheduler isr-watchdog** command is configured.

  Conditions: The issue occurs when inspecting H.323 traffic. The issue appears to happen shortly after seeing a %FW-4-TCP_OoO_SEG log such as this one:

  ```
  %FW-4-TCP_OoO_SEG: Deleting session as expected TCP segment with
   seq:3661972009 has not arrived even after 25 seconds - session
  xxx.xx.xx.xxx:53338 to
   xxx.xxx.xx.11:1720
  ```

  Workaround: Disable H.323 inspection.

- CSCtx72992

  Symptoms: GRE tunnel output is suddenly stuck.

  Conditions: The symptom is observed with the following conditions:

  - Cisco 3945
  - Cisco IOS Release 15.2(1)T.
  - Using GRE with IPsec.
  - There seems to be no trigger.

  Workaround: Reload the router.

- CSCty09784

  Symptoms: SS7 link does not come up.

Conditions: The symptom is observed with the fix of DDTS CSCta18342.

Workaround: Use the version of IOS that has the issue of "D channel is not recovering after IP flapping IUA".

CSCty19798

Symptoms: A Cisco 3925 router crashes with memory corruption.

Conditions: This has been observed under the following conditions:

1. The issue is only seen with CPU version 2.0 on a Cisco 2951.
2. It is not reproducible with Cisco IOS Release 15.1(3)T onwards (including later M versions based on that).
3. It is not seen 15.1(4)M onwards.

Workaround: There is no workaround.

- CSCty27687

  Symptoms: A core dump generated by a Cisco 3900/3900e with 2GB or more shows up as being corrupt in GDB. This prevents the core dump from being used to do a more detailed analysis of a crash.

  Conditions: The symptom is observed with a core dump generated on a Cisco 3900 or Cisco 3900e with more than 2GBs. Cores generated with 1GB of memory can be loaded into informers.

  Workaround: There is no workaround.

- CSCty47860

  Symptoms: The same /32 client address in a VRF gets associated with two different virtual interfaces. When this happens the **show ip route** shows that one /32 network is directly connected via two different virtual interfaces.

  Conditions: The conditions are under investigation.

  Workaround:

  1. Use **clear int Virtual-AccessX.X**.
  2. Use **clear ip route vrf xxx**.

- CSCty82414

  Symptoms: A crash is seen.

  Conditions: The symptom is observed when all of ZBFW, SGFW, IPS and Scansafe are configured on the router and traffic as in the traffic profile is sent (http- [tcp], dhcp -[udp] traffic).

  Workaround: Unconfigure IPS.

- CSCty91566

  Symptoms: A Cisco 3845 that is running Cisco IOS Release 15.1(4)M2 may have a processor pool memory leak in CCSIP_SPI_CONTROL.

  Conditions: The conditions are not known at this time.

  Workaround: There is no workaround.

- CSCtz15274

  Symptoms: When attempting a T.38 fax call on gateway, you may see the following in the logs:

```
006902: %FLEXDSPRM-3-UNSUPPORTED_CODEC: codec cisco is not supported on dsp 0/0
006903: %FLEXDSPRM-5-OUT_OF_RESOURCES: No dsps found either locally or globally.
```

  Conditions: The symptom is observed with a T.38 fax call.

Workaround: There is no workaround.

- CSCtz28855

  Symptoms: Router may crash after printing several error messages:

  ```
  %SYS-2-NOTQ: unqueue didn't find 87FFED94 in queue 865335D8 -Process= "IP
  Input", ipl= 0, pid= 113
  %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 87FFEDCC. -Process=
  "IP Input", ipl= 0, pid= 113
  ```

  Conditions: The symptom is observed with Cisco IOS Release 15.2(2)T1 with Trend URL Filtering configured.

  Workaround: There is no workaround.

- CSCtz35999

  Symptoms: A device crashes in the TCP to PAD process.

  Conditions: The issue occurs with X.25 and PAD enabled. The actual condition that is triggering the issue is still under investigation.

  Workaround: There is no workaround.

- CSCtz40460

  Symptoms: Router gets hung intermittently.

  Conditions: The issue is seen with G2 routers.

  Workaround: There is no workaround.

- CSCtz47309

  Symptoms: When using smart defaults in flexVPN, the mode transport may be sent from initiator even if "tunnel" is configured.

  Conditions: First seen on a Cisco ASR that is running Cisco IOS Release 15.2(2)S and a Cisco ISR running Cisco IOS Release 15.2(3)T. It is seen with flexVPN.

  Workaround: Use smart defaults on both sides on of the tunnel.

- CSCtz47595

  Symptoms: Dial string sends digits at incorrect times.

  Conditions: The symptoms are seen with a Cisco 3925 router running Cisco IOS Release 15.2(3)T using PVDM2-36DM modems with firmware version 3.12.3 connecting over an ISDN PRI to an analog modem.

  When using a dial string to dial an extension (or other additional digits), the modem should answer before the dial string is sent. If a comma is used, there should be a pause after connecting before sending the digits. The default value of the digital modem is one second per comma; two commas would be two seconds, three commas = three seconds and so on.

  1. With any number of commas in the string, debugs show the digits are sent at random intervals, sometimes before the call was answered and as much as up to 30 seconds after the call connects, i.e.: 919195551212x,22 or 1212x,,,22.
  2. With no comma in the dial string, the digits are sent immediately after being generated without waiting for a connection, i.e.: 919195551212x22.

  Dialing directly to a number with no extension or extra digits works as expected.

  Workaround: There is no workaround.

- CSCtz54775

  Symptoms: The Spanning-tree protocol (STP) takes almost 5 minutes to converge and create tree path to reach stations on the ethernet. Though the port is moved to forwarding state from blocked state in 45 seconds, the creation of the complete path takes almost 5 minutes. Because of this, the dynamic MAC address are not learned immediately.

  Conditions: In order to avoid a loop, the STP creates redundant paths by putting one the ports to a blocked state. When the primary link goes down the STP runs again to move the blocked state to forwarding and create a complete tree path again.

  Workaround: There is no workaround.

- CSCtz57013

  Symptoms: UC540 crashes randomly every few weeks.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(2)T2 and Release 15.1(2)T4.

  Workaround: There is no workaround.

- CSCtz58719

  Symptoms: Watchdog timeout under interrupt (level 0 or level 2).

  Conditions: The symptom is observed with a QoS configuration applied.

  Workaround: Disable QoS.

- CSCtz81595

  Symptoms: Unable to deploy or connect with AnyConnect 3.0.07059 to Cisco IOS. Mac OS Error:

  ```
  Failed to get configuration from secure gateway. Contact your system administrator
  ```

  Conditions: The symptom is observed with:

  - AnyConnect 3.0.0.0759 or higher.
  - Mac OS X
  - Cisco IOS headend.

  Workaround: Use 3.0.5080 or below. Downgrade both the client system and the headend.

- CSCtz84199

  Symptoms: DMVPN spoke crashes randomly on a Cisco 3945e.

  Conditions: The symptom is observed when traffic is going through.

  Workaround: There is no workaround.

- CSCtz84873

  Symptoms: A crash is observed due to stack overflow:

  ```
  %SYS-6-STACKLOW: Stack for process CCSIP_SPI_CONTROL running low, 0/60000
  ```

  Conditions: The issue is seen on a SIP gateway. The conditions are still being investigated.

  Workaround: There is no workaround.

- CSCtz88796

  Symptoms: When shaping is enabled on a GRE tunnel interface, and GRE-encapsulated traffic from this interface is routed to an NME-RVPN module via a Special Service Engine interface, the router can also automatically enable CBFQ on the interface Special Services Engine. This is done intentionally by the HQF feature implemented in Cisco IOS Release 12.4(20)T and later. HQF automatically enables CBFQ on the egress physical interface used to forward out GRE-encapsulated traffic from shaped tunnel interface.

The default state for the Special Services Engine interface is FIFO queuing.

When the router enables CBFQ on the Special Services Engine interface, very long packet delays (10-30 seconds) and some packet loss may intermittently occur on this interface in single direction: router --> NME-RVPN module.

Packets are stuck in the output queue of this interface: it is increasing or bouncing up and down.

The opposite direction (NME-RVPN module --> router) seems to be not affected (no packet loss, no delays). The GRE interface itself, which has triggered this issue, seems to be not affected as well (no loss, no delays).

Here, **show interface** shows CBFQ enabled and some packets stuck in the output queue of the Special Services Engine interface:

```
Special-Services-Engine1/0 is up, line protocol is up
Hardware is BCM5703, address is ...
Internet address is ...
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
Full Duplex, 1Gbps, link type is force-up, media type is internal
output flow-control is XON, input flow-control is XON
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:01, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 8641
Queueing strategy: Class-based queueing
Output queue: 13/1000/0 (size/max total/drops)
5 minute input rate 61000 bits/sec, 45 packets/sec
5 minute output rate 55000 bits/sec, 45 packets/sec
1667077 packets input, 462346265 bytes, 0 no buffer
Received 21 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
1662050 packets output, 459849577 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

If shaping is removed from the GRE tunnel interface, or policing is configured on it instead of shaping, the router reverts back to FIFO queuing on the Special Services Engine interface. The problem disappears, no packet loss/delay anymore:

```
Special-Services-Engine1/0 is up, line protocol is up
Hardware is BCM5703, address is ...
Internet address is ...
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
Full Duplex, 1Gbps, link type is force-up, media type is internal
output flow-control is XON, input flow-control is XON
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/512 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
2411963 packets input, 405030746 bytes, 0 no buffer
Received 11 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
2425958 packets output, 409829574 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

Conditions: The following conditions are seen:

- NME-RVPN module is installed (router is communicating to this module via a Special Services Engine interface).
- QoS shaping is enabled on some GRE tunnel interfaces on this router.
- GRE-encapsulated traffic of shaped GRE interface is routed to the NME-RVPN module for encryption via Special Service Engine interface (i.e.: tunnel destination IP is routed to this interface).
- Packet loss/delay issue is intermittent and may not start immediately after enabling shaping on GRE and CBFQ on Special Service Engine. It can be triggered later by some additional events, such as rebooting the NME-RVPN module when traffic is sent through.

Workaround: Currently, known workarounds are:

1. Disable shaping on GRE tunnels interfaces, or enable policing instead of shaping. GRE policing does not cause HQF to enable CBFQ on Special Service Engine interface.
2. Downgrade IOS to any version earlier than 12.4(20)T. IOS versions before that do not have the HQF feature and do not enable CBFQ on Special Service Engine interface.

- CSCua04185

  Symptoms: CRC/input errors are seen with moderate traffic on a Cisco 29xx for NM-1T3E3.

  Conditions: The symptom is observed with bi-directional traffic with 64 byte packet size.

  Workaround: Issue is not seen if traffic rate is more than 150 bytes.

- CSCua04722

  Symptoms: Crash while booting.

  Conditions: The symptom is observed at bootup.

  Workaround: Disable the QoS configuration, if possible.

- CSCua05196

  Symptoms: CPU hogs are seen leading to watchdog timeout.

  Conditions: The symptom is observed with a Cisco 2900 router.

  Workaround: Do not enter the **reload** command.

- CSCua12945

  Symptoms: Applying QoS under the serial interface is causing the interface to flap and most of the time causes line protocol to be DOWN.

  Conditions: Issue happens during both congestion and non-congestion on the link.

  Workaround: Doing a shut/no shut on the interface makes the interface come UP and running.

- CSCua21166

  Symptoms: Unable to form IPsec tunnels due to error:

  ```
  %CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality
  with securityk9 technology package license.
  ```
  even though the router does not have 225 IPsec SA pairs.

  Conditions: The symptom is observed with a Cisco ISR G2 router without HSECK9 license.

  Workaround: Reboot to clear out the leaked counter.

- CSCua23764

  Symptoms: Throughput performance drop has been seen between Cisco IOS interim Release 15.2(2.9)T and interim Release 15.2(3.14)T.

  Conditions: The symptom is observed when you upgrade from Cisco IOS interim Release 15.2(2.9)T to interim Release 15.2(3.14)T.

  Workaround: There is no workaround.

- CSCua28693

  Symptoms: One way audio is experienced. Gateway is streaming G.729 instead of G.711 which was negotiated through SIP signaling.

  Conditions: Issue was found with a Cisco 2821 and Cisco IOS Release 15.1(4)M1.

  Workaround: Use G.729 instead of G.711.

- CSCua29351

  Symptoms: Router crash.

  Conditions: The symptom is observed when NHRP is configured with SNMP.

  Workaround: There is no workaround.

- CSCua31157

  Symptoms: One way traffic is seen on a DMVPN spoke-to-spoke tunnel one minute after the tunnel is built. Issue is only seen intermittently.

  Logs on the spoke that fails to receive the traffic show “Invalid SPI” error messages exactly one minute after the tunnel between the spokes came up.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T1.

  Workaround: There is no workaround.

- CSCua33158

  Symptoms: IPv6 VRF ping fails between CE routers.

  Conditions: The symptom is only observed with IPv6.

  Workaround: There is no workaround.

- CSCua38876

  Symptoms: Router is forced to reload after a few minutes of passing traffic through VPN tunnels.

  Conditions: The symptom is observed with a tunnel protection configuration when an ISM-VPN module is enabled.

  Workaround: Disable ISM-VPN crypto-engine module.

  CSCua39390

  Symptoms: The PRI configuration (voice port) is removed after a reload:

```
interface Serial1/0:23          ^
% Invalid input detected at '^' marker.
no ip address
% Incomplete command.
encapsulation hdlc
   ^
% Invalid input detected at '^' marker.
isdn incoming-voice voice
       ^
% Invalid input detected at '^' marker.
no cdp enable
        ^
% Invalid input detected at '^' marker.
voice-port 1/0:23
           ^
% Invalid input detected at '^' marker.
Also getting trace back
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F0478z 0x607F72C0z 0x60722F38z 0x6070A300z
0x6070A9CCz 0x603E1680z 0x6029541Cz 0x60298F6Cz 0x6029AD48z 0x6029D384z
0x6062BC68z 0x60632424z 0x60635764z 0x60635CE0z 0x60877F2Cz
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F04E4z 0x607F7154z
```

Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T and Release 15.1(4)M4. The issue is not occurring with Cisco IOS Release 12.4(24)T6 or lower. The issue occurs after reload.

Workaround: Reapply configuration after router comes back up.

- CSCua42523

  Symptoms: Router crashes and reloads when “options-keepalive” is enabled on a dial-peer which has session target as sip-server.

  Conditions: The symptom is observed when enabling “options-keepalive” which has a session target as sip-server. Also, “sip-server” is configured under “sip-ua” and has a DNS address which resolves to an IPv6 address.

  Workaround: Do not enable “options-keepalive” for dial-peer.

- CSCua43850

  Symptoms: Call fails with error:

  ```
  **ERROR**: host_disconnect_ack: VOICE ERROR: NULL VDEV Common(0xFC): b channel 0, call
  id 0x831F
  ```

  Conditions: The symptom is observed with a V110 dial out call (VIC2-2BRI-NT/TE + TA).

  Workaround: There is no workaround.

- CSCua48060

  Symptoms: A Cisco 3945 UUT router reloads after applying PPP and AAA authentication as well as authorization. The same issue is seen for other platforms, namely Cisco 1803 and Cisco 3845 for the same script.

  Conditions: The symptom is observed when applying the AAA and PPP configurations with Cisco IOS interim Release 15.2(3.16)M0.1.

  Workaround: There is no workaround.

- CSCua50247

  Symptoms: Dropped ping packets on an NM-16ESW module.

Conditions: The symptom is observed with ping packets with a size between 1501-1524 and between NM-16-ESW modules.

Workaround: There is no workaround.

- CSCua51354

  Symptoms: WIC-1SHDSL-V3 keeps flapping once you have upgraded to Cisco IOS Release 15.1(4)M4. It becomes stable after couple of minutes.

  Conditions: The symptom is observed when upgrading from Cisco IOS Release 12.4(25d) to Cisco IOS Release 15.1(3)T4.

  Workaround: There is no workaround, other than to revert back to Cisco IOS Release 12.4(25d).

- CSCua53874

  Symptoms: A router configured for conferencing as a voice gateway may experience an unexpected reset while running Cisco IOS Release 15.1(4)M4.

  Conditions: The reset is seen when a conference call is initiated using local DSP resources.

  Workaround: Disable the dspfarm with the **shutdown** command. This requires that conferencing is handled by another device.

- CSCua59544

  Symptoms: CPU usage shoots up as soon as a file download starts via a tunnel between Anyconnect and an IOS headend. This happens irrespective of whether DTLS is enabled.

  Conditions: The symptom is observed with a file download via a tunnel between Anyconnect and an IOS router.

  Workaround: There is no workaround.

- CSCua60100

  Symptoms: Router crashes at ip_acl_peruser_ctxt_free while clearing the calls.

  Conditions: The symptom is observed when an ACL filter is applied on the input direction and then the session is established. When you try to clear the session, the router crashes.

  Workaround: There is no workaround.

- CSCua61097

  Symptoms: WAAS Express is causing corruption of packets within the TCP data which causes the WAAS appliance at the data center to reset the connection and in some cases the WAAS device will produce a DRE core file.

  Conditions: The symptom is observed with WAAS Express.

  Workaround: Upgrade the WAAS appliance to a code where DDTS CSCtu00021 is fixed. This will stop the WAE from producing a core file and only the corrupted frames will be reset.

  Further Problem Description: The WAAS DDTS CSCtu00021 will stop the WAE from producing a core file but the incorrectly formatted packets will still be reset.

- CSCua63087

  Symptoms: A Cisco 2800 will reload due to a bus error.

  Conditions: The symptom is observed with C2800NM-ADVIPSERVICESK9-M, version 15.1(4)M3.

  Workaround: There is no workaround.

- CSCua65278

  Symptoms: Modem disappears with the **cellular 0 cdma mode evdo** command.

  Conditions: The symptom is observed with the **cellular 0 cdma mode evdo** command when loaded with Cisco IOS interim Release 15.3(0.4)T.

  Workaround: There is no workaround.

- CSCua69346

  Symptoms: Memory leak at SSLVPN_PROCESS in processor pool.

  Conditions: The symptom is observed when "ssl-vpn" is configured on the router.

  Workaround: There is no workaround.

- CSCua70065

  Symptoms: CUBE reloads on testing DO-EO secure video call over CUBE when SDP passthru is enabled.

  Conditions: The symptom is observed when running Cisco IOS interim Release 15.3(0.4)T.

  Workaround: There is no workaround.

- CSCua70158

  Symptoms: NBAR fails to recognize traffic with **match protocol http url/host**.

  Conditions: The symptom is seen when "protocol discovery" is enabled.

  Workaround: There is no workaround.

- CSCua71038

  Symptoms: Router crash.

  Conditions: The symptom is observed with a Cisco router that is running Cisco IOS Release 15.2(3)T1. The router may crash during the failover test with OCSP and CRL configured.

  Workaround: Configure OCSP or CRL but not both

- CSCua72019

  Symptoms: AP802 radio goes into admin disable state and you will be unable to bring it back via AP CLI. On the AP CLI you will see messages similar to:

  ```
  soap_pci_reconfig_radio: bus 1 slot 0 bar0 0x60000000 bar1 0x60010000 bar2 0x0
  ap802_pci_reset_radio: reconfig radio 0
  %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
  soap_pci_reconfig_radio: bus 1 slot 0 bar0 0x60000000 bar1 0x60010000 bar2 0x0
  ap802_pci_reset_radio: reconfig radio 0
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to
  dosoap_pci_reconfig_radio: bus 1 slot 0 bar0 0x60000000 bar1 0x60010000 bar2 0x0
  ap802_pci_reset_radio: reconfig radio 0
  soap_pci_reconfig_radio: bus 1 slot 0 bar0 0x60000000 bar1 0x60010000 bar2 0x0
  ap802_pci_reset_radio: reconfig radio 0
  ```

  Conditions: The conditions are unknown.

  Workaround: Reboot the AP.

- CSCua72801

  Symptoms: IPS + WAAS shows inconsistent behavior.

  Conditions: The symptom is observed with WCCP and WAAS configured together. When IPS is configured only on WAN and not on LAN, traffic does not go through.

Workaround: Enable IPS on both WAN and LAN interfaces (this would hinder customers who would want to enable IPS only on WAN).

- CSCua73191

  Symptoms: Anyconnect fails to work with IOS SSL VPN and reports the following message:

  ```
  The AnyConnect package on the secure gateway could not be located. You may be
  experiencing connectivity issues. Please try connecting again
  ```

  Conditions: The issue was seen after upgrading to Cisco IOS Release 15.2(3)T.

  Workaround: Connecting via the portal might help.

- CSCua74224

  Symptoms: GETVPN rekey fails.

  Conditions: The issue was first seen on Cisco IOS Release 15.2(01)T. The keyserver is available over routes locally leaked.

  Workaround 1: Use older software. Cisco IOS Release 15.0(1)M7 and on have not shown this behavior.

  Workaround 2: Use a loopback cable instead of leaking routes (not recommended).

  Workaround 3: Use other mechanisms to perform leaking, for example: VASI (VRF-Aware Service Infrastructure).

- CSCua75666

  Symptoms: A "%DSMP-3-DSP_TIMEOUT:" is seen.

  Conditions: The symptom is observed under the following conditions:

  - Cisco IOS Release 15.1(4)M.
  - SRTP.
  - GCP.
  - Issue is load related.

  Workaround: Reduce load.

- CSCua75781

  Symptoms: CME reloads for E911 call ELIN translation for incoming FXS/FXO trunk.

  Conditions: The symptom is observed from Cisco IOS interim Release 15.3(0.2)T.

  Workaround: There is no workaround.

- CSCua76337

  Symptoms: Device crashes upon removing a numbered ACL.

  Conditions: The symptom is observed when traffic is hitting the policies where ACL is being used.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)M

All the caveats listed in this section are resolved in Cisco IOS Release 15.2(4)M. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCej11786

  Symptoms: A Cisco 2600 router reloads when a **clear counter** is performed on the router. This crash is reproducible only after making a number of calls first.

  Conditions: This symptom has been observed on a Cisco 2600 router.

  Workaround: There is no workaround.

- CSCsw95673

  Symptoms: When the RADIUS server is configured with one-time passwords (OTP) using RADIUS access-challenge message, the RADIUS server sends this message to the SSL VPN gateway after initial user authentication asks the user to enter OTP. This message is expected to be forwarded to the client, and to be shown on the client PC as a separate pop-up window.

  If an ASA 8.x is used as the SSL VPN gateway, the message is shown on the client PC. If it is an IOS SSL VPN gateway, the message is not shown.

  Conditions:

  - IOS is configured as SSL/WebVPN gateway with RADIUS user authentication.
  - RADIUS server is configured with OTP using RADIUS access-challenge message.

  Workaround: Use an OTP server which requests the user to enter OTP in standard username/password login window. Do not use an OTP server that asks for an OTP in a separate window after initial authentication.

  Further Problem Description: IOS SSL VPN gateway currently does not support RADIUS access-challenge message and this message is simply ignored by IOS (ASA 8.x SSL VPN gateway supports access-challenge).

- CSCtd43540

  Symptoms: Memory leak at cdp_handle_version_info. This problem was triggered by misbehavior of peer switch running Cisco IOS Release 12.2(46)SE which has been fixed in CSCsm63025 (Memory Leak @ cdp_handle_version_info).

  Conditions: The symptom is observed with link flapping.

  Workaround: Disable CDP on the flapping interface.

- CSCtd67668

  Symptoms: A router running Cisco IOS may crash.

  Conditions: The symptom is observed with netflow configured on a virtual-template interface.

  Workaround: There is no workaround.

- CSCtd86428

  Symptoms: SSH session does not accept IPv6 addresses in a VRF interface, but will accept IPv4 addresses.

  Conditions: The symptom is observed when you specify the VRF name with an SSH that belongs to an IPv6 interface.

  Workaround: You can specify the source interface.

Further Problem Description: SSH sessions not accept IPv6 addresses in VRF interface, but accepts IPv4 address:

  - Telnet session accepts both v6 and v4 addresses in VRF interface.
  - "Destination unreachable; gateway or host down" message shows in SSH session to IPv6 address in VRF interface.

- CSCtj48387

  Symptoms: After a few days of operation, a Cisco ASR router running as an LNS box, crashes with DHCP related errors.

  Conditions: This symptom occurs when DHCP enabled and sessions get DHCP information from a RADIUS server.

  Workaround: There is no workaround.

- CSCtj95182

  Symptoms: Scanning for security vulnerabilities may cause high CPU condition on Cisco Catalyst 3750.

  Conditions: This symptom is observed when network scanner runs against a Cisco Catalyst 3750 that is running Cisco IOS Release 12.2(55)SE.

  Workaround: There is no workaround.

- CSCtq17444

  Symptoms: A Cisco AS5400 crashes when performing a trunk call.

  Conditions: The following conditions are observed:

  - Affected Cisco IOS Release: 15.1(3)T.
  - Affected platforms: routers acting as voice gateway for H.323.

  Workaround: There is no workaround.

- CSCtq24557

  Symptoms: Router crash after deleting multiple VRFs. This happens very rarely.

  Conditions: The symptom is observed in a large scale scenario.

  Workaround: There is no workaround.

- CSCtq27016

  Symptoms: A QoS-related memory leak is seen.

  Conditions: The symptom is observed when a QoS policy is removed and added on a SIP-400 or ES-40 interface.

  Workaround: There is no workaround.

- CSCtq39602

  Symptoms: DMVPN tunnel is down with IPsec configured. The **show dmvpn** command from the spoke shows the state is IKE.

  Conditions: After heavy traffic was pumping from DMVPN hub to spoke for some time: from a few minutes to a couple of hours.

  Workaround: Configuring "crypto ipsec security-association lifetime kilobytes disable" to disable volume-based rekeying will reduce the problem.

- CSCtq51039

  Symptoms: Traffic is dropped with VFR + Cisco Wide Area Application Services (WAAS).

  Conditions: The issue is seen when a flow with fragmented packets is placed in pass through, either because of configuration or because max flows in WAAS is reached. Fragmented packets can occur in the network for a wide variety of reasons.

  Workaround: Resolve the fragmentation cause. A possible solution is configuring TCP MSS on interface:

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t4/feature/guide/ft_admss.html

- CSCtq84313

  Symptoms: Router hangs and then crashes due to watchdog timer expiry.

  Conditions: This symptom is observed when IP SLA probes are configured, and then the configuration is replaced with one that has no IP SLA probes.

  Workaround: Reset the ip sla.

- CSCtq95384

  Symptoms: Even after the removal of NSR configurations, BGP still holds memory.

  Conditions: The symptom is observed after the removal of NSR configurations.

  Workaround: There is no workaround.

- CSCtr25127

  Symptoms: When switching between ATM and 3G interfaces, the following traceback is observed.

  ```
  %ALIGN-3-CORRECT: Alignment correction made at 0x23D242DCz reading 0xE85C77B
  %ALIGN-3-TRACE: -Traceback= 0x23D242DCz 0x23CDE700z 0x23CFDF50z 0x225C0594z
  0x225C1368z 0x22DD4564z 0x21F88D28z 0x2173449Cz
  %ALIGN-3-CORRECT: Alignment correction made at 0x23D2430Cz writing 0xE85C77B
  %ALIGN-3-TRACE: -Traceback= 0x23D2430Cz 0x23CDE700z 0x23CFDF50z 0x225C0594z
  0x225C1368z 0x22DD4564z 0x21F88D28z 0x2173449Cz
  ```

  Conditions: This symptom is observed when switching between ATM and 3G interfaces.

  Workaround: There is no workaround.

- CSCtr36083

  Symptoms: IKE SAs are not cleared. Ping fails over the IPsec tunnel.

  Conditions: This symptom occurs when SAs are cleared by using the **clear crypto session local** *address* command.

  Workaround: There is no workaround.

- CSCtr45287

  Symptoms: Router crashes in a scale DVTI scenario.

  Conditions: The symptom is observed when the IPsec tunnel count reaches around 2500.

  Workaround: Use fewer tunnels or use a different platform.

- CSCtr87070

  Symptoms: Enable login failed with error "% Error in authentication".

  Conditions: The symptom is observed with TACACS single-connection.

  Workaround: Remove TACACS single-connection.

- CSCtr93412

  Symptoms: Crash seen on mwheel process.

  Conditions: The symptom is observed with GETVPN multicast followed by **clear crypto gdo**.

  Workaround: There is no workaround.

- CSCts00341

  Symptoms: When executing a CLI that requires domain-name lookup such as **ntp server** *server.domain.com*, the command fails with the following message on the console:

  ```
  ASR1k(config)#ntp server server.domain.com <<< DNS is not resolved with dual RPs on
  ASR1k
  Translating "server.domain.com "...domain server (10.1.1.1) [OK]
  %ERROR: Standby doesn't support this command ^ % Invalid input detected at '^' marker.
  ASR1k(config)#do sh run | i ntp
  ASR1k(config)#
  ```

  Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

  Workaround: Instead of using *hostname* in the command, specify the IP address of the host.

- CSCts27333

  Symptoms: Multicast traffic is forwarded in software due to MTU failures.

  Conditions: This symptom is seen with packet size greater than the standard interface MTU being forwarded on the standby supervisor in a VSS setup. The problem is only seen with GRE tunnel OIF, where the tunnel MTU is incorrect in spite of the underlying interface being configured to accept a higher MTU.

  Workaround: There is no workaround.

- CSCts32708

  Symptoms: Similar to CSCth80642, IOS SSLVPN router fails to accept new sessions. The users will not be able to load the webvpn login page. If you enable debug sdps you may see: Sev 4:sdps_get_pak_from_tcp(),line 1080:tcp_getpacket returned error 2, tcb=0x6A9EFFEC

  Conditions: The router remains reachable otherwise (ie you can ping the webvpn IP) SSL process is running and listening on the right port. "Show tcp tcb" and "show tcp brief all numeric" will show connections stuck in CLOSED and CLOSEWAIT state. Clearing the tcp tcb sessions does not restore connectivity. Taking webvpn in/out of service does not restore connectivity. Disabling webvpn cef and rebooting does not prevent the issue. Rebooting does resolve the issue temporarily

  Workaround: 1. Reboot.

  2. If available for your platform, get the fix for CSCth80642 AND disable webvpn cef (you should reboot or clear the tcb connections after disabling webvpn cef). This may prevent the problem.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2011-3286 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts37446

  Symptoms: Traceback is observed while testing the antireplay feature.

  Conditions: Traceback is observed while configuring the routers randomly. It is not observed manually.

Workaround: There is no workaround.

- CSCts38674

  Symptoms: UUT/modem fails to make a call using external dialer interface.

  Conditions: The symptom is observed when the cellular interface is configured with “o ip address” and when using an external dialer interface, UUT/modem will fail to make a call.

  Workaround: Configure cellular interface with “ip address negotiated”.

- CSCts44393

  Symptoms: A Cisco ASR 1000 crashes.

  Conditions: The symptom is more likely to occur when a large number of VRFs are repeatedly configured and deleted.

  Workaround: There is no workaround.

- CSCts56278

  Symptoms: A Cisco 2951, 3925, or 3945 platform may stop at ROMmon during IOS boot.

  Conditions: The symptom is observed on some Cisco 2951, 3925 or 3945 systems when the following conditions are met:

  1. IOS boot from HW power on (it does not occur with a software reload).
  2. A service module installed in slot 1.
  3. System has 15.0(1r)M12 ROMmon.
  4. The **show diag** output for “Slot 0:” has the following “Top Assy. Part Number”:

  ```
  2951: 800-36886-01 3925: 800-36888-01 3945: 800-36887-01
  ```

  Workaround: Upgrade to ROMmon 15.0(1r)M13:

  2951 ROMMON location:
  http://www.cisco.com/cisco/software/release.html?mdfid=282774230&flowid=7445&softwareid=280805687&release=15.0%281r%29M13&rellifecycle=&relind=AVAILABLE&reltype=all

  3900 ROMMON location:
  http://www.cisco.com/cisco/software/release.html?mdfid=282774222&flowid=7437&softwareid=280805687&release=15.0%281r%29M13&rellifecycle=&relind=AVAILABLE&reltype=all

  Instructions on how to upgrade ROMmon can be found at:
  http://www.cisco.com/en/US/docs/routers/access/2600/hardware/notes/piperrom.html

- CSCts65564

  Symptoms: In a large scale DMVPN environment, a DMVPN hub router may crash in the IOS process under high scale conditions.

  Conditions: This only occurs if CRL caching is disabled (with the command **crl cache none** under the pki trustpoint configuration).

  Workaround: Enable CRL caching (this is the configured default).

- CSCts68626

  Symptoms: PPPoE discovery packets causes packet drop.

  Conditions: The symptom is observed when you bring up a PPPoE session and then clear the session.

  Workaround: There is no workaround.

- CSCts72911

  Symptoms: In case of a GR/NSF peering, after an SSO switchover, the restarting router (PE, in this case) does not advertise RT constrain filters to the non-restarting peer (RR, in this case).

  Conditions: The symptom is observed after an SSO switchover in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the non-restarting router does not send back the corresponding VPN prefixes towards the restarted router.

  Workaround: There is no workaround.

- CSCts82058

  Symptoms: Creation of Overlay interface leads to router crash.

  Conditions: This symptom is seen when configuring overlay interface and enabling OTV commands followed by the **otv join-interface** command on the core facing interface.

  Workaround: There is no workaround.

- CSCts83046

  Symptoms: Back-to-back ping fails for P2P GRE tunnel address.

  Conditions: The symptom is observed when HWIDB is removed from the list (through **list remove**) before it gets dequeued.

  Workaround: There is no workaround.

- CSCts85459

  Symptoms: Upon a reload, the cellular interface will not negotiate if a crypto map is applied to it.

  Conditions: The symptom is observed on a Cisco 881 router that has a cellular interface which dials to get an IP address and also acts as the VPN gateway. When we reload the router, the cellular interface does not connect if a crypto map is applied and we see IPsec fails to initialize because we do not have an IP address.

  Workaround: This situation remains until we manually remove the crypto map from the cellular interface. Then we see the chat-script starting and the whole dialing procedure starts, then the cellular link is up with an IP address. Then we re-apply the crypto map again and the tunnel works fine.

- CSCtt04093

  Symptoms: VC is not coming up after unshutting the preferred path/Tunnel.

  Conditions: This symptom is seen when configuring ATOM Tunnel from CE1 to CE2 using next hop destination address as preferred path and disabling fall back option.

  Shut down the preferred path and verify that AToM VC is not routed to another available route and that AToM VC is down.

  Now the preferred path is not found, and VC is down.

  Workaround: There is no workaround.

- CSCtt17762

  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.

  Conditions: The symptom is observed on an IP PIM multicast network.

  Workaround: There is no workaround.

- CSCtt20719

  Symptoms: Incremental leaks at shdsl_efmEndpointCurrEntry_get and shdsl_efmInventoryEntry_get.

Conditions: The symptom is observed with an SNMP walk on a Cisco 888E router and with a Cisco ISR-G2 with HWIC-2SHDSL-EFM.

Workaround: There is no workaround.

- CSCtt26208

  Symptoms: A Cisco 3845 running Cisco IOS Release 15.1(4)M1 may have a processor pool memory leak in CCSIP_SPI_CONTROL.

  Conditions: Not known at this time.

  Workaround: There is no workaround.

- CSCtt26692

  Symptoms: Router crashes due to memory corruption. In the crashinfo you may see:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk xxxxxxx data xxxxxxxx
  chunkmagic xxxxxxxx chunk_freemagic EF4321CD - Process= "CCSIP_SPI_CONTROL", ipl= 0,
  pid= 374 chunk_diagnose, code = 1 chunk name is MallocLite
  ```

  Conditions: Router is configured for SIP. When a translation-rule is configured to translate a number to one with more digits, the router may crash when the translation takes effect, such as when a call is forwarded.

  Workaround: Configuring “no memory lite” configurations can be used as a workaround in some cases (depending on the length of the phone numbers), but will cause the router to use more memory. If the translation-profile is configured to translate forwarded calls, then avoid or disable the option to forward the call.

- CSCtt35379

  Symptoms: BGP Processing Enhancements.

  Conditions: None.

  Workaround: None.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt61762

  Symptoms: IPv6 host connected to EHWIC-*ESG layer 2 ports are not able to communicate to each other locally (at layer 2).

  Conditions: This issue was first noticed on a Cisco ISR G2 with EHWIC-*ESG and directly-connected IPv6.

  Workaround: There is no workaround.

- CSCtt70133

  Symptoms: The RP resets with FlexVPN configuration.

  Conditions: This symptom is observed when using the **clear crypto session** command on the console.

  Workaround: There is no workaround.

- CSCtt94440

  Symptoms: The Cisco ASR 1000 series router RP may reload.

  Conditions: This symptom is observed when an etoken is in use and the **show crypto eli all** command is issued.

  Workaround: Avoid using the **show crypto eli all** command. However, you can use the **show crypto eli** command.

- CSCtt96597

  Symptoms: Unable to power-cycle modem using **test cellular** *unit* **modem-power-cycle**.

  Conditions: The symptom is observed when a router cannot communicate with the modem due to a possible modem firmware crash or device disconnect.

  Workaround: Reload router.

- CSCtu07968

  Symptoms: A Cisco 890 router may provide incorrect performance monitor statistics and omit some incoming packets from being handled by flexible netflow.

  Conditions: This is observed when performance monitoring or flexible netflow is enabled with IPsec over a tunnel on an input interface.

  Workaround: There is no workaround.

- CSCtu14409

  Symptoms: The “Insufficient bandwidth 2015 kbps for bandwidth guarantee” error message is displayed when configuring a policy map with “priority level xxx” and then updating it with “police cir xxx”.

  Conditions: This symptom occurs when the priority is configured without a specific rate. This issue is only seen with a Cisco ASR 1000 series router.

  Workaround: Configure police before priority.

- CSCtu16862

  Symptoms: L4F tracebacks observed with SMB stress test traffic. You may experience a couple of retransmissions due to that and some small performance degradation.

  Conditions: The symptom is observed with stress testing.

  Workaround: There is no workaround.

- CSCtu22167

  Symptoms: SP crashes.

  Conditions: This symptom is observed under the following conditions:

  - When unicast prefixes have local labels.
  - When the tunnel is the next-hop for those prefixes.
  - When the topology is modified (that is, when you remove or shut down the physical interface) so that the tunnel’s destination address is reachable via the tunnel.

  Workaround: Ensure that the tunnel endpoint peer does not advertise the prefixes to reach the tunnel endpoint.

- CSCtu23195

  Symptoms: SNMP ifIndex for serial interfaces (PA -4T/8T) becomes inactive after PA OIR.

  Conditions: The symptom is observed with a PA OIR.

Workaround: Unconfigure and reconfigure the channel-groups of the controller and reload the router.

- CSCtu32301

  Symptoms: Memory leak may be seen.

  Conditions: This is seen when running large **show** commands like **show tech-support** on the linecard via the RP console.

  Workaround: Do not run the show commands frequently.

- CSCtu34207

  Symptoms: CoA for SessProv request timeout from ISG to SCE.

  Conditions: Issue is seen after an upgrade to Cisco IOS 15.1S train (seen in Cisco IOS Release 15.1(2)S1 too).

  Workaround: There is no workaround.

  Further Problem Description: The packet is seen in the TCPDUMP on the SCE. Cisco IOS Release 12.2(33)XNF2 does not show the issue. SCE shows in the debug:

  ```
  bad authentication validate failed
  ```

- CSCtu35116

  Symptoms: VPDN session keeps on trying to come up with MPLS MTU higher than 1500.

  Conditions: The symptom is observed when you upgrade a Cisco 7200VXR from the c7200-a3jk91s-mz.122-31.SB18 to the c7200-adventerprisek9-mz.122-33.SRE4 image.

  Workaround: There is no workaround.

- CSCtu40028

  Symptoms: The SCHED process crashes.

  Conditions: The issue occurs after initiating TFTP copy.

  Workaround: There is no workaround.

- CSCtu43120

  Symptoms: Service accounting start is not sent for L2TP sessions.

  Conditions: This symptom is observed with L2TP.

  Workaround: There is no workaround.

- CSCtv28434

  Symptoms: GDOI cannot start negative GM re-register timer and prints out traceback at func crypto_gdoi_start_re_register_timer().

  Conditions: The symptom is observed with both IP (v4/v6) GDOI crypto maps configured on the dual-stack interface and GMs re-registration triggered.

  Workaround: Do not trigger GMs to re-register.

- CSCtv36812

  Symptoms: Incorrect crashInfo file name is displayed during crash.

  Conditions: The symptom is observed whenever a crash occurs.

  Workaround: There is no workaround.

- CSCtw46061

  Symptoms: The following output shows the leaked SA object continuing to be in the "OBJECT_IN_USE" state. The state is supposed to be changed to OBJECT_FREEING by crypto_engine_delete_ipsec_sa(). This is in turn being called by ident_free_outbound_sa_list().

  ```
  shmcp-fp40#sh crypto eli Hardware Encryption : ACTIVE Number of hardware crypto
  engines = 1
  CryptoEngine IOSXE-ESP(14) details: state = Active Capability : DES, 3DES, AES, RSA,
  IPv6, GDOI, FAILCLOSE
  IKE-Session : 0 active, 12287 max, 0 failed DH : 211 active, 12287 max, 0 failed
  IPSec-Session : 323 active, 32766 max, 0 failed
  ```

  Conditions: This symptom is observed on a Cisco ASR 1000 series router

  Workaround: There is no workaround.

- CSCtw46229

  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.

  Conditions: The symptom is observed with PPP negotiations and the session involving PPPoA.

  Workaround: Ensure all your PPP connections stay stable.

- CSCtw50952

  Symptoms: A Cisco ASR series router crashes due to memory exhaustion after issuing the **clear ip ospf**. This symptom was not observed before issuing this command.

  ```
  ACC-CDC-NET-Pri#sh mem stat
            Head        Total(b)       Used(b)    Free(b)     Lowest(b) Largest(b)
  Processor  30097008   1740862372      279628560  1461233812 14604778041453167736
  lsmpi_io   97DD61D0    6295088        6294120    968        968        968
  ```

  Conditions: This symptom is observed upon executing the **clear ip ospf** causing tunnel interfaces to flap.

  Workaround: There is no workaround.

- CSCtw55424

  Symptoms: SSH with "vrf" in command line for IPv6 addr/host is not working. For example: **ssh -l** *username* **-vrf** *vrfname ipv6 add/host*.

  Conditions: The symptom is observed when **ip ssh source-interface** is not defined and the user specifies the VRF by command line (e.g.: **ssh -l** *username* **-vrf** *vrfname ipv6 add/host*).

  Workaround: Use **ip ssh source-interface** *interface-name* and connect with **ssh -l** *username (IPv4/IPv6)(addr/host)*.

- CSCtw58664

  Symptoms: SSL VPN for SCCP causes a crash when clearing a WebVPN session.

  Conditions: The symptom is observed when using the SSL VPN for SCCP phones feature and when clearing the WebVPN session:

  ```
  clear webvpn session context SSLVPNphone
  [WV-TUNL-EVT]:[0] Returning address 10.0.112.200 to pool
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x2601227C
  -Traceback= 0x26008B3Cz 0x25F9D7E8z 0x25F94A3Cz 0x224B66A8z 0x224BCBA8z 0x224CBF70z
  0x23D22684z 0x23D189C0z 0x237F0144z 0x237F0128z -Traceback= 0x26008B3Cz 0x25FCEAA8z
  0x238561D8z
  ```

  The frequency of the issue is rare.

  Workaround: There is no workaround.

- CSCtw59338

  Symptoms: A crash is experienced following a switch bootup into Cisco IOS Release 12.2(53)SG5 due to an apparent memory corruption.

  Conditions: The issue is seen on a device if a neighboring device is configured with an IP address. Device crashes rarely when using the **sh cdp nei de** command.

  Workaround: Disable CDP.

- CSCtw61192

  Symptoms: When the **redistribute static** command has the *route-map* and the *set tag* arguments, and you enter the **no redistribute static** command, the router sends out only one query and the remaining routes get stuck in active state indefinitely.

  Conditions: This symptom is observed only when you set a tag to a redistributed route.

  Workaround: There is no known workaround.

- CSCtw61872

  Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.

  Conditions: The symptom is observed when executing a complex sort with top- talkers on a show command from multiple CLI sessions (note that normal show commands without top-talkers are fine):

  ```
  sh flow monitor QoS_Monitor cache sort highest counter packets top 1000
  sh flow monitor QoS_Monitor cache sort highest counter packets top 10000
  ```

  Workaround: Do not execute complex sorts with top-talkers on the show output from multiple CLI sessions.

- CSCtw62213

  Symptoms: When two Cisco 3945E routers are connected to each other and are performing IPSLA operations, the responder sees a drop in packets coinciding with license update process execution

  Conditions: This symptom is observed when two Cisco 3945E routers are connected back to back while performing IPSLA UDP-jitter operation.

  Workaround: Increasing the input queue length on the interface and SPD queue length is a valid workaround

- CSCtw62310

  Symptoms: The **cells** keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service- policy”.

  Conditions: The symptom is observed when removing the policy-map from map-class.

  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw67283

  Symptoms: A router receives either an “Illegal access to a low address” or an “Unexpected exception to CPU” crash depending on the platform. The crash occurs within several minutes of starting traffic.

Conditions: The router is configured with NBAR2, FNF, and HQoS. While running a mix of HTTP, FTP, SMTP, and DNS traffic, the router crashes within several minutes of starting traffic. The crash has been seen on the Cisco 891, 1941, and 2901 (Cavium based), but has not been seen on the Cisco 2951, 3925, or 3945.

Workaround: There is no workaround.

- CSCtw73530

  Symptoms: Unable to delete metadata sessions.

  Conditions: This symptom is observed when more than 100 metadata sessions are created.

  Workaround: Disable metadata and then enable it. Note that this will remove all the flows.

- CSCtw78064

  Symptoms: The **display-logout** message on a Cisco SCCP Phone is not cleared even after pressing other buttons on the phone.

  Conditions: This symptom is observed on the Cisco SCCP phone (also known as Skinny Phone or ePhone) when the last extension mobility (EM) user in a hunt group logs out using the HLog button. This symptom is observed even if the last EM user logs out of the hunt group and logs back in.

  Workaround: There is no workaround.

- CSCtw78451

  Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running show commands.

  Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.

  Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

- CSCtw79510

  Symptoms: Cannot force VPN client users to change their passwords in the next login.

  Conditions: The symptom is observed with an authentication problem while using password change option.

  Workaround: There is no workaround.

- CSCtw86212

  Symptoms: ISG is failing to support radius attribute filter configuration.

  Conditions: ISG is setting up a session via EAP/RP authentication, whereas authorization radius attribute(s) should be passed on by ISG to its radius client and ISG should ignore it locally when creating the session. It occurs only in the case of radius proxy.

  Workaround: Possibly do not send the undesired radius attributes to ISG in authentication/authorization replies and configure the required parameters on each radius-client (from an ISG perspective).

- CSCtw86712

  Symptoms: RP crashes.

  Conditions: The symptom is observed when you apply certain tunnel configurations.

  Workaround: There is no workaround.

- CSCtw94598

  Symptoms: Web authentication does not work after an upgrade. NAS-Port-Type = Async.

Conditions: The symptom is observed when you upgrade to Cisco IOS Release 12.2(58)SE2 or later or to the Cisco IOS 15.0(1)SE train.

Workaround: Change NAS-Port-Type on AAA Server to match the new value.

- CSCtw95189

  Symptoms: The "%Unknown DHCP problem. No allocation possible" error is observed in the DHCP error log.

  Conditions: This symptom occurs when open access is enabled and the supplicant is authz failed. Then, DHCP IP address assignment does not take place.

  Workaround: There is no workaround.

- CSCtw98456

  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.

  Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

  For example, the IVRF routing table should show:

  ```
  S 10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
  ```

  but instead it shows:

  ```
  S 10.0.0.0 [1/0] via 192.168.0.1
  ```

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

  Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in **show crypto ipsec sa**) remain at zero.

  Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other IOS versions and other hardware platforms may be affected.

  Workaround: Configure a static route to the remote network. For example:

  ```
  ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
  ```

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtx04709

  Symptoms: Some EIGRP routes may not be removed from the routing table after a route is lost. The route is seen as "active" in the EIGRP topology table, and the active timer is "never".

  Conditions: This symptom is seen when a multiple route goes down at the same time, and query arrives from neighbor router. Finally, neighbor detects SIA for affected router and neighbor state is flap. However, active entry is remaining after that, and route is not updated.

  Workaround: The **clear ip eigrp topology** *network mask* command may remove unexpected active entry.

- CSCtx04712

  Symptoms: Removal of crypto map hangs the router.

  Conditions: The symptom is observed following removal of "gdoi crypto map" from interface.

  Workaround: There is no workaround.

- CSCtx06801

  Symptoms: Certain websites may not load or load very slowly when content-scan is enabled. Delays of up to 30 seconds or more may be seen.

  Conditions: The symptom is observed when content-scan is enabled.

  Workaround: Though not always, refreshing the page sometimes helps.

  Further Problem Description: The problem is due to GET request being segmented. For example, a huge get request of 1550 may come from the client in two different packets such as 1460+90=1550.

- CSCtx06813

  Symptoms: Installation fails, “rwid type l2ckt” error messages appear, and the VC may fail to come up on Quad-Sup router only. Though this error may appear for multiple other reasons, this bug is specific to Cisco Catalyst 6000 Quad-Sup SSO only.

  Conditions: The symptom is observed in a scaled scenario, doing second switchover on Quad-Sup router.

  Workaround: There is no workaround.

- CSCtx22322

  Symptoms: If an over-temperature interrupt occurs when the CPU utilization is high, the system may crash.

  Conditions: The symptom is observed when CPU utilization of the system is high Cisco 880 series routers.

  Workaround: There is no workaround.

- CSCtx23534

  Symptoms: The reverse route of an EzVPN client is not being copied over to the HA peer.

  Conditions: The symptom is observed when using stateful failover via IPsec HA.

  Workaround: Manually add routes for the remote peers into the routing table using static routes.

- CSCtx28483

  Symptoms: A router set up for Cisco Unified Border Element-Enterprise (CUBE- Ent) box-to-box redundancy will reload when certain configuration commands are deconfigured out of the recommended sequence.

  Conditions: The symptom is observed when deconfiguring CUBE-Ent box-to-box redundancy once it is already configured (for CUBE-Ent box-to-box redundancy) on the Cisco ASR platform. You cannot change the configuration under the “application redundancy group” submode without first removing the redundancy-group association under “voice service voip” submode. If you do not remove this association first before changing the configuration under “application redundancy group”, the ASR will reload. You are not provided any other option.

  Workaround: Always first remove the redundancy-group association under “voice service voip” submode first and then you can change the configuration under “application redundancy group”.

- CSCtx31175

  Symptoms: Framed-IP-Address added twice in PPP service-stop accounting record.

  Conditions: The symptom is observed with the following conditions:

  1. User session exists on ASR1001.
  2. Stop one user’s session by using **clear subscriber session username xxx** on ASR1001.
  3. ASR1001 sends double “Framed-IP-Address” in service-stop accounting for one user’s session.

Workaround: Do not use **clear subscriber session** command to clear the session, instead use **clear pppoe**.

- CSCtx31294

  Symptoms: Anyconnect is unable to connect to the Cisco IOS headend (ISR-G2) when cert-based authentication is in use.

  Conditions: This symptom is observed with the following conditions:

  1. Cert-based authentication is configured using “authentication local rsa-sig” on the Cisco IOS headend.
  2. Remote authentication on the Cisco IOS headend can be EAP or rsa-sig. The Anyconnect client is unable to connect, and hence the tunnel is not established.

  Workaround: There is no workaround.

- CSCtx31329

  Symptoms: IKEv2 process memory is increasing over time.

  Conditions: The symptom has been seen on an IKEv2 flexVPN hub.

  Workaround: There is no workaround.

- CSCtx32329

  Symptoms: When using the **show ipv6 rpf** command, the router crashes or displays garbage for RPF idb/nbr.

  Conditions: This symptom can happen when the RPF lookup terminates with a static multicast route that cannot be resolved.

  Workaround: Do not use static multicast routes, or make sure that the next hop specified can always be resolved. Do not use the **show** command.

- CSCtx32527

  Symptoms: The **show crypto session** command reveals the flexVPN GRE tunnel is in a DOWN state instead of DOWN-negotiating.

  Conditions: The symptom is observed with “ip address negotiated” configured on the GRE tunnel interface (with tunnel protection). The tunnel is unable to reach the gateway initially.

  Workaround: Configure an IP address on the tunnel interface instead of “ip address negotiated”.

- CSCtx34643

  Symptoms: MPLS pseudowire ping fails.

  Conditions: The symptom is observed when you configure MPLS with xconnect.

  Workaround: There is no workaround.

- CSCtx35064

  Symptoms: Traffic remains on blackholed path until holddown timer expires for PfR monitored traffic class. Unreachables are seen on path, but no reroute occurs until holddown expires.

  Conditions: This symptom is seen under the following conditions:

  - MC reroutes traffic-class out a particular path (BR/external interface) due to OOP condition on the primary path.
  - Shortly after enforcement occurs, an impairment on the new primary path occurs causing blackhole.

  - PfR MC does not declare OOP on the new primary path and attempt to find a new path until Holddown timer expires. Causes traffic loss.

  Workaround: Reduce the holddown timer to 90 seconds (minimum value) to minimize impact.

- CSCtx40818

  Symptoms: Traffic drops in a Cisco and displays the error message "%IP-3- LOOPPAK: Looping packet detected and dropped - src=122.0.0.11, dst=121.0.0.11, hl=20, tl=40, prot=6, sport=80, dport=57894"

  Conditions: This symptom is observed if the WAAS, NAT and firewall are enabled.

  Workaround: Disable WAAS.

- CSCtx44060

  Symptoms: Flexvpn spoke-to-spoke tunnels do not come up.

  Conditions: None.

  Workaround: Once tunnels fail to come up, clear the NHRP cache on one spoke alone.

- CSCtx45373

  Symptoms: Under **router eigrp virtual-name** and **address-family ipv6 autonomous-system 1**, when you enter **af-interface Ethernet0/0** to issue a command and exit, and later, under **router bgp 1** and **address-family ipv4 vrf red**, you issue the **redistribute ospf 1** command, the "VRF specified does not match this router" error message is displayed. When you issue the **redistribute eigrp 1** command, it gets NVGENd without AS number.

  Conditions: This symptom occurs under **router eigrp virtual-name** and **address-family ipv6 autonomous-system 1**, when you enter **af-interface Ethernet0/0** to issue a command and exit, and later, under **router bgp 1** and **address-family ipv4 vrf red**, you issue the **redistribute ospf 1** command.

  Workaround: Instead of using the **exit-af-interface** command to exit, if you give a parent mode command to exit, the issue is not seen.

- CSCtx45970

  Symptoms: A crash is seen only in the negative case, when the frequency is not a multiple of history interval.

  Conditions: The symptom is observed when the value is not initialized.

  Workaround: Configure the right configuration with frequency being the multiple of interval.

- CSCtx48753

  Symptoms: Higher memory usage with PPP sessions than seen in Cisco IOS XE Release 3.4/3.5.

  Conditions: The symptom is observed with configurations with PPP sessions. These will see up to 10% higher IOS memory usage than in previous images.

  Workaround: There is no workaround.

- CSCtx49098

  Symptoms: A crash occurs at udb_pre_feature_unbind_cleanup.

  Conditions: This symptom is observed when a complex 3 level HQoS policy is configured on the interface and it is manipulated with changes.

  Workaround: Do not manipulate the QoS policy while it is being used or avoid using the same child policy multiple times in the parent policy.

- CSCtx49766

  Symptoms: GETVPN does not allow traffic in a Cisco HWIC-3G-CDMA-V modem.

  Conditions: This symptom is observed on a Cisco HWIC-3G-CDMA-V modem running Cisco IOS Release 15.1(4)M3.

  Workaround: Use Cisco IOS Release 15.1(3)T3 with the Cisco HWIC-3G-CDMA-V modem.

- CSCtx50176

  Symptoms: RP crashes @ be_ikev2_abort_negotiation.

  Conditions: The symptom is observed while bringing up 4K SVTI_BGP with ike_group 16.

  Workaround: There is no workaround.

- CSCtx51420

  Symptoms: After reloading the router on Cisco IOS Release 15.2(2)S (or other affected code), the router begins to crash on boot-up. The following error may also be seen:

  ```
  %SYS-2-NOBLOCK: printf with blocking disabled. -Process= "TPLUS", ipl= 7, pid= 459
  ```

  Conditions: The symptom is observed when AAA/TACACS is configured and is operational on the device.

  Workaround: Removal of AAA system accounting will prevent the crash.

- CSCtx52042

  Symptoms: PMIP crash when using **clear ipv6 mobile pmivp6** *lma/mag* **bindings** *peerid* for the peer.

  Conditions: The symptom is observed when using **clear ipv6 mobile pmivp6** *lma/mag* **bindings** *peerid* command.

  Workaround: There is no workaround.

  Further Problem Description: This only occurs with IPv6 mobile nodes. This problem is not seen with IPv4 mobile nodes.

- CSCtx52095

  Symptoms: I/O leak for middle buffer at nhrp_getbuffer.

  Conditions: The symptom is observed with the following conditions:

  - Cisco 3925.
  - c3900-universalk9-mz.SPA.151-3.T1.bin image.
  - The following is shown:

  ```
  Middle buffers, 600 bytes (total 25951, permanent 25, peak 25951 @ 00:00:04):
      30 in free list (10 min, 150 max allowed)
      181198 hits, 8664 misses, 119 trims, 26045 created
      0 failures (0 no memory)
  ```

  Workaround: Assigning overlay IP address to the tunnel interface at spoke will prevent memory leak.

- CSCtx53448

  Symptoms: Traffic destined to an unauthenticated client is not being blocked.

  Conditions: This happens when the client is allowed to authenticate once. The issue surfaces when the port now goes for a shutdown and is then brought back up again.

  Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 2.6/2.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:P/I:N/A:N/E:POC/RL:U/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtx54882

  Symptoms: A Cisco router may crash due to Bus error crash at voip_rtp_is_media_service_pak.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 15.1(4)M2.

  Workaround: There is no known workaround.

- CSCtx55357

  Symptoms: Auto RP messages are permitted through "ip multicast boundary".

  Conditions: The symptom is observed when the ACL associated with the multicast boundary matches 224.0.1.39 and 224.0.1.40. It is seen on the Cisco ASR 1000 platform.

  Workaround: Use "no ip pim autorp" which will disable Auto RP completely from this device.

- CSCtx56174

  Symptoms: Cisco router hangs until a manual power cycle is done. If the **scheduler isr-watchdog** command is configured, the device will crash and recover instead of hanging until a power cycle is done.

  Conditions: This is seen with websense URL filtering enabled and with zone based firewalls.

  Workaround: Disable URL-based filtering.

- CSCtx57073

  Symptoms: A Cisco router may crash with the following error: "Segmentation fault(11), Process = Metadata HA".

  Conditions: This symptom is observed while upgrading the router from Cisco IOS XE Release 3.6 to mcp dev.

  Workaround: The required changes have been made with this DDTS to prevent the crash.

- CSCtx57584

  Symptoms: SIP basic call fails with 500 internal server error.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.2(02.14) T.

  Workaround: There is no workaround.

- CSCtx57784

  Symptoms: Device crashes while configuring "logging persistent url".

  Conditions: Occurs when the destination file system has zero free bytes left.

  Workaround: There is no workaround.

- CSCtx61557

  Symptoms: The switch crashes after logging "success" from "dot1x" for client (Unknown MAC).

  Conditions: The symptom is observed with the following conditions:

  1. A switchport is configured with both of the following:

  ```
  authentication event server dead action authorize...
  ```

```
authentication event server alive action reinitalize
```

2. The radius server was down previously, and a port without traffic (for example: a hub with no devices attached) was authorized into the inaccessible authentication bypass (IAB) VLAN without an associated MAC address.
3. The radius server becomes available again, and a dot1x client attempts to authenticate.

Workaround: There is no workaround.

- CSCtx62920

  Symptoms: A connection hang is observed with stress traffic when SSL Express and HTTP Express accelerators are enabled and the client is misbehaving and sending a FIN after sending a request.

  Conditions: The issues exist in Cisco IOS Release 15.2(3)T and higher. WAAS Express, HTTP Express accelerator and SSL Express accelerator need to be enabled. The HTTP client is sending a FIN instead of reset to close the connection that has timed out.

  Workaround: Use the **clear waas connection** command to terminate the connection.

- CSCtx63545

  Symptoms: Router will crash in case of all the configured radius servers are dead and tried to authenticate client against RADIUS in the radius-proxy case.

  Conditions: This will happen only for radius-proxy scenario and if all the configured radius servers are dead.

  Workaround: At least configure one of the alive RADIUS servers.

- CSCtx64347

  Symptoms: Despite open access being configured on the port, traffic to/from the client is blocked.

  Conditions: This symptom occurs when an authenticating port with open-access and multi-auth hostmode configured, is interrupted.

  Workaround: There is no workaround.

- CSCtx64684

  Symptoms: While configuring the ISIS on two Cisco 2921 routers connected back to back, the ISIS neighbors do not come up.

  Conditions: This symptom is observed only on the SVI interface. This issue is only seen with EHWIC.

  Workaround: If the router has an L3 port, form a neighborship on a physical interface directly or create dot1q subinterfaces if peering is required on multiple VLANs.

- CSCtx66030

  Symptoms: A Cisco router handling SIP registrations/unregistrations may unexpectedly reload. This symptom is observed on the following devices:

  - SIP-CME
  - SIP-SRST GW
  - CUBE

  Conditions: This symptom is observed when the number of SIP registrations/unregistrations handled is more than 320.

  Workaround: Limit the number of registrations/unregistrations to less than 320.

- CSCtx66804

  Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFREQ.

  Conditions: The symptom is observed with the following conditions:

  - “ppp lcp delay 0” is configured.
  - The symptom can be seen on Cisco IOS Release 15.0(1)M5.

  Workaround: Set delay timer without 0.

- CSCtx67290

  Symptoms: A Cisco Session Border Controller crashes when receiving an oversize rtcp-fb element in the SDP.

  Conditions: The symptom is observed when there is an oversize rctp-fb element in the SDP.

  Workaround: There is no workaround.

- CSCtx67474

  Symptoms: Update message is sent with an empty NLRI when the message consists of 2byte aspath in ASPATH attribute and 4byte value aggregate attribute.

  Conditions: This can happen when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.

  Workaround: Move all the 2byte AS peers to a separate update-group using a non-impacting outbound policy like “advertisement-interval”.

- CSCtx71185

  Symptoms: Router crashes due to corrupted program counter.

  Conditions: The symptom is observed with packets being switched across the dialer interface.

  Workaround: There is no workaround.

- CSCtx73612

  Symptoms: A Cisco ASR 1000 may reload while reading IPsec MIBs via SNMP and write a crashfile.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.1(1)S1.

  Workaround: Do not poll or trap IPsec information via SNMP.

- CSCtx74342

  Symptoms: After interface goes down or is OIRed, in a routing table you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next hop interface set to the interface that is down.

  Conditions: The symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 sec default).

  Workaround: Configuring SPF throttle timer can change the interval.

  Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

  ```
  Router show ipv6 route
  IPv6 Routing Table - default - 2 entries
  Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
         B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
         IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
         ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
  ```

```
       l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/64 [110/10]
     via Ethernet0/0, directly connected
```

- CSCtx77750

  Symptoms: Crosstalk may be heard by PSTN callers when a call is placed on hold and Music on Hold (MMOH) is enabled.

  Conditions: CUCM is configured to do Multicast MoH.

  Workaround: (1) Disable H.323 Multicast MoH functionality in IOS or use SIP Multicast MoH. (2) Use Unicast MoH.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:ND/RC:C

  CVE ID CVE-2012-1361 has been assigned to document this issue.

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

- CSCtx79318

  Symptoms: OGW fails to send 200 OK response for OPTION.

  Conditions: The symptom is observed with 200 OK response for OPTION in Cisco IOS interim Release 15.2(02.16)T.

  Workaround: There is no workaround.

- CSCtx82775

  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.

  Conditions: The symptom is observed when MTP is invoked for calls.

  Workaround: Reload the router or perform a no sccp/sccp.

- CSCtx84059

  Symptoms: Forwarded calls in the SIP network experience one-way audio on calls from FXS to SIP.

  Conditions: This symptom is observed on a Cisco router that uses route-map for routing to the SIP network.

  Workaround: Add static route to the CFU party IP address.

- CSCtx86116

  Symptoms: Active router crashes when HA configuration is removed.

  Conditions: The symptom is observed when HA and RG configurations are present and traffic is flowing through the ACTIVE router.

  Workaround: There is no workaround.

- CSCtx86539

  Symptoms: NAT breaks SIP communication with addition of media attributes.

  Conditions: The symptom is observed with NAT of SIP packets.

  Workaround: There is no workaround.

- CSCtx86674

  Symptoms: ATM VPI/VCI does not come up after upgrading to Cisco IOS Release 15.1(4)M4.

  Conditions: This symptom is observed when upgrading to Cisco IOS Release 15.1(4)M4, which was an engineering build given for addressing CSCtx09973.

  Workaround: ATM port shut/no shut resolves the issue. However, it refers to about 5000+ nodes here or "config dsl-group 0 pairs 0" instead of dsl-group auto under controller SHDSL.

- CSCtx87939

  Symptoms: When the **Mediatrace Poll** command is invoked using WSMA interface, the "hops response received notifications" message is displayed. This message corrupts the WSMA output for the command.

  Conditions: This symptom is observed when Mediatrace poll is used in a WSMA interface.

  Workaround: There is no workaround.

- CSCtx90408

  Symptoms: A Cisco router will see a spurious access or a crash. ISR-G1 routers such as a 1800/2800/3800 will see a spurious access. ISR-G2 routers such as the 2900/3900 routers that use a Power PC processor will crash because they do not handle spurious accesses.

  Conditions: This issue is seen after enabling a crypto map on an HSRP-enabled interface. The exact conditions are still being investigated.

  Workaround: There is no workaround.

- CSCtx90703

  Symptoms: The CM tone is squelched when SG3 spoofing enabled.

  Conditions: SG3 spoofing should only apply to fax calls. SG3 spoofing should be ignored during modem calls. When the originating modem provides a calling menu the gateway should forward it when SG3-to-G3 is enabled.

  Workaround: Disabling SG3 spoofing may help:

  ```
  !
  voice service voip
   no fax-relay sg3-to-g3
  !
  ```

- CSCtx92665

  Symptoms: Executing the **show mediatrace session stat** command causes a crash at *__be_sla_mt_route_data_print*.

  Conditions: This symptom is observed when **show mediatrace session stat** or **show mediatrace session data** is used.

  Workaround: There is no workaround.

- CSCtx92802

  Symptoms: IP fragmented traffic destined for crypto tunnel is dropped.

  Conditions: The symptom is observed under the following conditions:

  - Cisco IOS Release 15.0(1)M7 on a Cisco 1841.
  - VRF enabled.
  - CEF enabled.
  - VPN tunnel.

Workaround: Disable VFR or CEF.

- CSCtx93598

  Symptoms: An "ikev1 dpd" configuration erroneously affects IKEv2 flows.

  Conditions: The symptom is observed if we configured the IKEv1 DPD function with "crypto isakmp keepalive" while IKEv2 is enabled as well. The IKEv2 DPD function will be affected.

  Workaround: There is no workaround.

- CSCtx95339

  Symptoms: ID leak while flapping walkby converted sessions in radius_parse_respons. "Out of ID" error messages are displayed on the console.

  Conditions: The symptom is observed when flapping walkby converted sessions.

  Workaround: There is no workaround.

- CSCtx95840

  Symptoms: A Cisco voice gateway may unexpectedly reload.

  Conditions: The symptom is observed on a Cisco voice gateway running SIP protocol. In this case the issue was when sipSPIUfreeOneCCB() returns, the leftover event is still being processed after CCB is released from sipSPIUfreeOneCCB(). Based on sipSPIStartRemoveTransTimer(ccb), CCB should have been released later by a background timer.

  Workaround: There is no workaround.

- CSCtx96779

  Symptoms: Crash seen at __be_cont_scan_get_10_session.

  Conditions: The symptom is observed when the CLI output of **show content-scan session active** is stopped at the --More-- prompt. The CLI is then removed from the router and finally more output is requested from the CLI earlier stopped at --More--.

  Workaround: Remove the CLI when there is no output pending from any show command.

- CSCtx99544

  Symptoms: Exception occurs when using **no aaa accounting system default vrf** *VRF3* **start-stop group** *RADIUS-SG-VRF3*:

  ```
  router(config)# no ip vrf VRF3
  router(config)# no aaa accounting system default vrf VRF3 start-stop group
  RADIUS-SG-VRF3

  %Software-forced reload
  ```

  Conditions: The symptom is observed with the following conditions:

  - Hardware: Cisco ASR 1001.
  - Software: asr1001-universalk9.03.04.02.S.151-3.S2.

  Workaround: There is no workaround.

- CSCty01234

  Symptoms: A router running Cisco IOS may reload unexpectedly.

  Conditions: This symptom is observed only with low-end platforms using VDSL interfaces, such as a Cisco 887 router. It also requires that the **qos pre-classify** command be used in conjunction with IPsec and GRE, such as in a DMVPN configuration.

  Workaround: Do not use the **qos pre-classify** command.

- CSCty01237

  Symptoms: The router logs show:

  ```
  <timestamp> %OER_BR-5-NOTICE: Prefix Learning STARTED
  CMD: 'show run' <timestamp>
  ```

  This is followed by the router crashing.

  Conditions: This issue is seen under the following conditions:

  1. Configure PfR with a learn-list using a prefix-list as a filter and enable learn.
  2. Use a configuration tool, script or NMS that periodically executes **show run** on the MC over HTTP or some other means.

  Workaround 1: If you use PfR learn-list feature, do not execute **show run** periodically.

  Workaround 2: If you use a monitoring tool that executes **show run** periodically, avoid using a learn-list configuration in PfR.

- CSCty02403

  Symptoms: An EIGRP topology entry with bogus nexthop is created when more than one attribute is present in the route received from neighbors. It also tries to install one default route with bogus nexthop. So if you have a default route received from some neighbors, then that default route will also flap.

  Conditions: It can only occur when more then one attribute set in any route received from a neighbor.

  Workaround: Do not set more then one attribute in the route.

- CSCty03629

  Symptoms: Traffic from a client with a valid IP-SGT mapping is dropped by the firewall.

  Conditions: NAT is co-located with SGFWl.

  Workaround: There is no workaround.

- CSCty03745

  Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.

  Conditions: This symptom occurs when the IPv4 default route exists, that is:

  ```
  ip route 0.0.0.0 0.0.0.0 <next-hop>.
  ```

  Or a certain static/IGP route exists: For example:

  ```
  ip route 0.0.253.0 255.255.255.0 <next-hop>.
  ```

  Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family. For example:

  ```
  router bgp 65000
    address-family l2vpn vpls
     neighbor 10.10.10.10 next-hop-self
  ```

  Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

- CSCty04384

  Symptoms: IMA-DSLAPP crashes when doing interoperability testing with third- party DSLAMs.

  Conditions: Change line rates on CO sides with various loop lengths.

  Workaround: There is no workaround.

- CSCty04798

  Symptoms: A Cisco router may experience a memory leak approximately 24 bytes in the dead process. The **show memory dead** output shows mostly the "show_voice_call_status_task" process.

  Conditions: The following configuration is present:

  pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 1

  If nfas is not configured there is no leak. This has been experienced on a Cisco 3825 router that is running Cisco IOS Release 12.4(15)T17 configured as a voice gateway.

  Workaround: There is no workaround.

- CSCty05092

  Symptoms: EIGRP advertises the connected route of an interface which is shut down.

  Conditions: This symptom is observed under the following conditions:

  1. Configure EIGRP on an interface.
  2. Configure an IP address with a supernet mask on the above interface.
  3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.

  Workaround 1: Remove and add INTERFACE VLAN xx. Workaround 2: Clear ip eigrp topology x.x.x.x/y.

- CSCty05150

  Symptoms: After SSO, an ABR fails to generate summary LSAs (including a default route) into a stub area.

  Conditions: This symptom occurs when the stub ABR is configured in a VRF without "capability vrf-lite" configured, generating either a summary or default route into the stub area. The issue will only be seen after a supervisor SSO.

  Workaround: Remove and reconfigure "area x stub".

- CSCty07771

  Symptoms: CSCts55654 may cause extensive performance degradation

  Conditions: This symptom is observed when normal QoS policy is applied on egress direction

  Workaround: There is no workaround.

- CSCty08070

  Symptoms: Router may print error message and traceback similar to the following example:

  ```
  %SCHED-STBY-3-THRASHING: Process thrashing on watched boolean 'OSPFv3 Router boolean'.
  -Process= "OSPFv3R-10/4/2", ipl= 5, pid= 830router ospf -Traceback= 7235C3Cz 7235F1Cz
  6A5F7A8z 6A6168Cz 50DA290z 50D3B44zv
  ```

  Conditions: The symptom is observed when the affected OSPFv3 router is configured, but the process does not run because it has no router-id configured. Further, an area command is configured, for example "area X stub".

  Workaround: Configure "router-id" so the process can run.

- CSCty12083

  Symptoms: A Cisco 819 router with the C819HG+7 SKU reloads.

  Conditions: This symptom is observed on a Cisco 819 router with the C819HG+7 SKU reloads while running Cisco IOS Release 15.1(4)M3.8.

  Workaround: There is no workaround.

- CSCty12524

  Symptoms: BRI packet from LMA is not handled properly on MAG and also MAG is not sending the APN and SSMO option in PBRA.

  Conditions: The symptom is observed on the originating or old MAG while clearing sessions in LMA in response to mobile node roaming to a new MAG.

  Workaround: There is no workaround.

- CSCty13747

  Symptoms: Cisco Network Based Application Recognition (NBAR) applications with "engine-id=13" not shown or exported.

  Conditions: This symptom is observed while executing the **show flow exporter option application table** command.

  Workaround: The issue has been fixed.

- CSCty14375

  Symptoms: There is a false temperature alarm on a Cisco 2911 in a production environment:

  ```
  %ENVMON-1-WARN_HDD_HIGH_TEMP: Critical Warning: sensor temperature (65535 C) exceeds
  40 C. System is experiencing excessive ambient temperatures and/or airflow blockage.
  SM-SRE-700-K9 hard disk drive may become unusable if continuously operated at this
  temperature. Please resolve system cooling to prevent system damage.
  ```

  Conditions: This has been seen on a Cisco 2900 router that is running Cisco IOS Release 15.1(4)M, when air intake temperature goes below 0C.

  Workaround: There is no workaround.

- CSCty15615

  Symptoms: Policy in direction A may disappear after removing policy from direction B. The policies no longer show up under the interface in **sh policy-map int** or **show running**.

  Conditions: The symptom is observed with policies on both input and output directions, and then you remove from one of the directions. Happens on Cisco 7200/7600 platforms.

  Workaround: There is no workaround.

- CSCty17288

  Symptoms: MIB walk returns looping OID.

  Conditions: The symptom is observed when a media mon policy is configured.

  Workaround: Walk around CiscoMgmt.9999.

- CSCty18156

  Symptoms: One Cisco Unified 9971 SIP video phone is registered with Cisco Unified Communications Manager Express (CUCME) and the "Extension Mobility" button is clicked on the phone. The CUCME crashes.

  Conditions: The symptom is observed only when you have SIP CUCME configurations alone. If you have telephony service configured on the same CUCME, the issue is not observed.

  Workaround: Configure telephony services command on same router.

- CSCty22840

  Symptoms: A router can crash due to a Watchdog timeout on the NTP process as it fails to unpeer from an NTP peer that had already been removed. In addition, the following error might be seen in the system log:

  ```
  NTP Core (ERROR): peer struct for X.X.X.X not in association table
  ```

Conditions: This symptom is observed when active changes occur in NTP, that is, new peers or servers are added at boot time as part of the existing configuration or during normal operation as part of a new configuration.

Workaround: Configure NTP to use the ACL with the **ntp access-group peer** command to explicitly define which hosts can function as an NTP peer.

- CSCty23094

  Symptoms: Responder crashes when running many video sessions.

  Conditions: The symptom is observed with a high responder CPU load.

  Workaround: Reduce the number of video sessions.

- CSCty24606

  Symptoms: Under certain circumstances, the Cisco ASR 1000 series router's ASR CUBE can exhibit stale call legs on the new active after switchover even though media inactivity is configured properly.

  Conditions: This symptom is observed during High Availability and box to box redundancy, and after a failover condition. Some call legs stay in an active state even though no media is flowing on the new active. The call legs can not be removed manually unless by a manual software restart of the whole chassis. The call legs do not impact normal call processing.

  Workaround: There is no workaround.

- CSCty24707

  Symptoms: Standby RP continually reboots and never recovers.

  Conditions: The symptom is observed during an RP standby switchover with QoS applied to ISG sessions.

  Workaround: Shut down the virtual template interface and do a switchover.

- CSCty25810

  Symptoms: Tracebacks are observed on PAN module in auth_feature_critical_get_authorized_domain_any()/dot1x_matm_mac_addr_learned () functions.

  Conditions: This symptom occurs due to an invalid HWIDB pointer. HWIDB is NULL for the mac-addresses learned over the CPU_PORT in case of L2VPN.

  Workaround: There is no workaround.

- CSCty25963

  Symptoms: CME reloads on configuring "no mode cme" under voice register global.

  Conditions: The symptom is observed when running Cisco IOS interim Release 15.2(3.1)T.

  Workaround: There is no workaround.

- CSCty26126

  Symptoms: Plain IP traffic gets a label when it should not. It bounces across the IPsec VPN network.

  Conditions: The symptom is observed with the following conditions:

  - "ip address negotiated" configured on the flexVPN spoke.
  - /32 address directly configured on the tunnel interface of the flexVPN spoke.

  Workaround: Use a /31 or bigger.

- CSCty29122

  Symptoms: TCP TLS handshake fails for secure RTP calls.

Conditions: The symptom is observed with Cisco IOS interim Release 15.2(03.1)T.

Workaround: There is no workaround.

- CSCty30886

  Symptoms: A standby RP reloads.

  Conditions: This symptom is observed when bringing up PPPoE sessions with configured invalid local IP address pool under virtual-template profile and “aaa authorization network default group radius” on the box with no radius present. No IP address is assigned to PPPoE Client.

  Workaround: There is no workaround.

- CSCty32232

  Symptoms: BRI interface is not showing as monitored.

  Conditions: The issue occurs after performing an on-line insertion/removal of an NM-16ESW module.

  Workaround: Reload the router.

- CSCty32463

  Symptoms: When you boot an ASR-1002-X or an ASR-1001 in dual IOSd mode (SSO), the standby process comes up and SSO gets executed but the configuration is unable to sync up between the two processes:

```
%REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
(raw-event=PEER_FOUND(4))
%REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
(raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

%LICENSE-3-BULK_SYNC_FAILED: License bulk sync operation Priority Sync for
feature adventerprise 1.0 failed on standby rc=Remote tty failed
%ISSU-3-INCOMPATIBLE_PEER_UID: Setting image (X86_64_LINUX_IOSD-UNIVERSALK9-
M),
version (15.2(20120222:153818)156) on peer uid (49) as incompatible
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:
crypto pki certificate chain root-tank.com
 ! <submode> "crypto-ca-cert-chain"

Cannot finish user input data read from fd 17
%RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
kp_perf1>
```

  When this part of the configuration is removed, the issue is not seen:

```
crypto pki certificate chain root-tank.com
! <submode> "crypto-ca-cert-chain"
- ^C
! </submode> "crypto-ca-cert-chain"
```

  Conditions: The position of the ^C is causing the issue.

  Workaround: The starting “^C” should be placed at the same line as “certificate ca”. For example:

```
certificate ca ^C
44AFB080D6A327BA893039862EF8406B
 ......
quit^C
```

- CSCty32851

  Symptoms: A Cisco router may unexpectedly reload due to software forced crash exception when changing the encapsulation on a serial interface to “multilink ppp”.

  Conditions: The symptom is observed when the interface is configured with a VRF.

  Workaround: Shut down the interface before making the encap configuration change.

- CSCty34020

  Symptoms: A Cisco 7201 router’s GigabitEthernet0/3 port may randomly stop forwarding traffic.

  Conditions: This only occurs on Gig0/3 and possibly Fa0/0 as they both are based on different hardware separate from the first three built-in gig ports.

  Workaround: Use ports Gig0/0-Gig 0/2.

- CSCty37020

  Symptoms: Learned inside BGP prefixes are not getting added into MC database.

  Conditions: The symptom is observed with learned inside BGP prefixes.

  Workaround: There is no workaround.

- CSCty37445

  Symptoms: A DMVPN hub router with a spoke which is an EIGRP neighbor. The spoke receives a subnet from hub and then advertises it back to the hub, bypassing split horizon.

  Conditions: The symptom is observed when on the spoke you have a **distribute list route-map** command setting tags.

  Workaround: Once you remove that command EIGRP works normally.

- CSCty41067

  Symptoms: Router crashes while doing an SSO without any configurations.

  Conditions: The symptom is observed while doing an SSO.

  Workaround: There is no workaround.

  CSCty41850

  Symptoms: MGCP gateway with PVDM3 advertises G723 to CUCM upon registration which it cannot support. Then, if the G723 is successfully negotiated for a call through a PRI on the MGCP gateway, all subsequent calls via that PRI will send CRCX of G723 to the gateway and fail immediately. The PRI needs to reregister in order to clear the issue.

  Error seen in gateway log each time a call fails as G723:

```
%FLEXDSPRM-3-UNSUPPORTED_CODEC: codec g723r63 is not supported on dsp 0/0

CUCM receives AUEP 200 OK messages from GW upon PRI registration which includes
G723 as a capability.

09:34:55.713 |MGCPHandler received msg from: XXX.XXX.XXX.XXX
200 178370
I:
X: 0
L: p:10-20, a:PCMU;PCMA;G.nX64, b:64, e:on, gc:1, s:on, t:10, r:g, nt:IN;LOCAL,
v:T;G;D;L;H;R;ATM;SST;PRE
L: p:10-220, a:G.729;G.729a;G.729b, b:8, e:on, gc:1, s:on, t:10, r:g,
nt:IN;LOCAL, v:T;G;D;L;H;R;ATM;SST;PRE
L: p:10-110, a:G.726-16;G.728, b:16, e:on, gc:1, s:on, t:10, r:g, nt:IN;LOCAL,
v:T;G;D;L;H;R;ATM;SST;PRE
L: p:10-70, a:G.726-24, b:24, e:on, gc:1, s:on, t:10, r:g, nt:IN;LOCAL,
v:T;G;D;L;H;R;ATM;SST;PRE
L: p:10-50, a:G.726-32, b:32, e:on, gc:1, s:on, t:10, r:g, nt:IN;LOCAL,
v:T;G;D;L;H;R;ATM;SST;PRE
L: p:30-270, a:G.723.1-H;G.723;G.723.1a-H, b:6, e:on, gc:1, s:on, t:10, r:g,
nt:IN;LOCAL, v:T;G;D;L;H;R;ATM;SST;PRE
L: p:30-330, a:G.723.1-L;G.723.1a-L, b:5, e:on, gc:1, s:on, t:10, r:g,
nt:IN;LOCAL, v:T;G;D;L;H;R;ATM;SST;PRE
M: sendonly, recvonly, sendrecv, inactive, loopback, conttest, data, netwloop,
netwtest
|4,100,152,1.565243^
```

Conditions: The symptom is observed with an MGCP gateway with PVDM3 that advertises G723 to CUCM upon registration. Then, if the G723 is successfully negotiated for a call through a PRI on the MGCP gateway, all subsequent calls via that PRI will send CRCX of G723 to the gateway and fail immediately.

Workaround: There is no workaround.

- CSCty42626

  Symptoms: Certificate enrollment fails for some of the Cisco routers due to digital signature failure.

  Conditions: This symptom was initially observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.

  This issue potentially impacts those platforms with HW crypto engine. Affected platforms include (this is not a complete/exhaustive list)

  – c3925E, c3945E
  – c2951, c3925, c3945
  – c7200/VAM2+/VSA,
  – possibly VPNSPA on c7600/cat6
  – K 819H ISR G2 routers with ISM IPSec VPN accelerator

  Workaround: There is no workaround.

- CSCty43587

  Symptoms: Crash observed with memory corruption similar to the following:

  ```
  %SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
  dealloc XXXXXXXX
  ```

  Conditions: The symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.

  Workaround: There is no workaround.

- CSCty44281

  Symptoms: Compile errors seen as the shim file crypto_shim_act_1_rng.h is missing

  Conditions: The symptom is observed with the missing shim file crypto_shim_act_1_rng.h.

  Workaround: There is no workaround.

- CSCty46273

  Symptoms: A router configured with the Locator ID Separation Protocol (LISP) may crash when the connected routes in the RIB flap.

  Conditions: This symptom is observed when LISP tracks the reachability of routing locators (RLOCs) in the RIB. For the crash to occur, a locator being watched by LISP must be covered by a route that is itself covered by a connected route. If both these routes are removed from the RIB in close succession, there is a small possibility that the race-condition resulting in this crash may be hit.

Workaround: There is no workaround.

- CSCty48870

  Symptoms: Router crash due to a bus error.

  Conditions: This has been observed in router that is running Cisco IOS Release 15.2(2)T and 15.2(3)T with NBAR enabled on a crypto-enabled interface. NBAR can be enabled through NAT, QoS, or NBAR protocol discovery.

  Workaround: Using **no ip nat service nbar** will help where NBAR is enabled through NAT.

- CSCty49656

  Symptoms: A crash is observed when executing the **no ip routing** command.

  Conditions: This symptom is observed under the following conditions:

  1. Use a Cisco IOS image that has fix for CSCtg94470.
  2. Configure OSPF.
  3. Enable multicast.
  4. Create several (>6000) routes in the network to be learned by OSPF.
  5. Wait for OSPF to learn all the (>6000) routes from the network.

  Finally, executing the **no ip routing** command may crash the box.

  Workaround: There is no workaround.

- CSCty51453

  Symptoms: Certificate validation using OCSP may fail, with OCSP server returning an "HTTP 400 - Bad Request" error.

  Conditions: The symptom is observed with Cisco IOS Release 15.2(1)T2 and later.

  Workaround 1: Add the following commands to change the TCP segmentation on the router:

  ```
  router(config)# ip tcp mss 1400
  router(config)# ip tcp path-mtu-discovery
  ```

  Workaround 2: Use a different validation method (CRL) when possible.

- CSCty52047

  Symptoms: IKE SAs are not getting deleted by DPD (crypto isakmp keepalive).

  Conditions: This symptom is observed on a Cisco ASR 1000 router with DPD enabled.

  Workaround: Manually delete the stuck isakmp session:

  ```
  clear crypto isakmp conn-id
  ```

  You can get the conn-id from the output of the **show crypto isakmp sa** command.

- CSCty53243

  Symptoms: Video call fails in the latest mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has the uc_infra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.

  Conditions: This symptom is observed when CUBE changes the video port to "0" in 200 OK sent to the UAC.

  Workaround: There is no workaround.

- CSCty54434

  Symptoms: ISRG2 with ISM VPN is not bringing up more than one tunnel in a crypto map-based scenario with large certificates (4096 bit).

  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T and Cisco IOS Release 15.2(2)T.

  Workaround: Configure IKEv2 fragmentation so that the fragmentation/reassembly is handled by IKE code rather than by IPsec.

- CSCty54446

  Symptoms: CPU can sometimes shoot up to 99% when initiating an HTTP session from the client. This makes router unresponsive and typically leads to crash.

  Conditions: The symptom is observed with WebAuth, NTLM, or HTTP-basic authentication enabled. More specifically, the problem is triggered when the router intercepts a large, longer than 2KB, HTTP message from client. The problem affects both HTTP (port 80) and HTTPS (port 443) connections.

  Workaround: There is no workaround.

- CSCty54728

  Symptoms: The **media-proxy** {**rsvp** | **metadata**} *name* command and its subcommands are not applied when a Cisco router reloads.

  Conditions: This symptom is observed when the **media-proxy** {**rsvp** | **metadata**} *name* command does not generate correct **show running-config** output.

  Workaround: Reload the router, and then configure the **media-proxy** {**rsvp** | **metadata**} *name* command and its subcommands.

- CSCty55449

  Symptoms: The device crashes after registering an Embedded Event Manager TCL policy.

  Conditions: If the policy uses the multiple event feature and the trigger portion is registered without curly braces ("{}"), then the device will crash. For example, this policy will trigger a crash:

  ```
  ::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
  ::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
  ::cisco::eem::trigger
  ::cisco::eem::correlate event 1 or event 2

  namespace import ::cisco::eem::*
  namespace import ::cisco::lib::*

  action_syslog priority crit msg " triggered "
  ```

  Note how "::cisco::eem::trigger" is not followed by an opening curly brace.

  Workaround: Ensure that the trigger portion (i.e.: the correlate statement) is enclosed within curly braces. Given the example above, the proper syntax is:

  ```
  ::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
  ::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
  ::cisco::eem::trigger {
      ::cisco::eem::correlate event 1 or event 2
  }

  namespace import ::cisco::eem::*
  namespace import ::cisco::lib::*

  action_syslog priority crit msg " triggered "
  ```

- CSCty56801

  Symptoms: Bus error at __be_cisp_client_match on an ASW.

  Conditions: The symptom is observed on an ASW upon issuing **clear auth sess int** *int_id*.

  Workaround: There is no workaround.

- CSCty58241

  Symptoms: The following symptoms are observed:

  Symptom 1. You may receive the following error when you enable radius debugs:

  ```
  RADIUS: Response for non-existent request ident
  ```
  Symptom 2. The radius alias functionality may not work.

  Conditions:

  For symptom 1: You move from the alias-based configuration to non-alias based configuration and you remove the host first and alias next. In the new configuration if one of the alias becomes the primary host address this will lead to symptom 1.

  For symptom 2: If the reply comes from the alias IP address the functionality may not work.

  Workarounds:

  For symptom 1:

  - Reload the router; or
  - Unconfigure the alias first before unconfiguring the host.

  For symptom 2:

  - Do not use the alias on the NAS.

- CSCty58300

  Symptoms: BGP Processing Enhancements.

  Conditions: None.

  Workaround: There is no workaround.

- CSCty58992

  Symptoms: One-way audio is observed after transfer to a SIP POTS Phone.

  Conditions: This symptom is observed under the following conditions:

  - Cluster is in v6 mode.
  - A call is made from Phone1 to Phone2, and then Phone2 transfers the call to Phone3(SIP POTS), which is when the issue occurs.

  Workaround: There is no workaround.

- CSCty59692

  Symptoms: CME crashes.

  Conditions: The symptom is observed with SIP SNR + CFNA on SNR mobile.

  Workaround: There is no workaround.

- CSCty61212

  Symptoms: The removal of crypto map hangs the router.

  Conditions: This symptom is observed with the removal of GDOI crypto map from interface.

  Workaround: There is no workaround.

- CSCty61216

  Symptoms: CCSIP_SPI_Control causes leak with a Cisco AS5350.

  Conditions: The symptom is observed with the following IOS image: c5350-jk9su2_ivs-mz.151-4.M2.bin.

  It is seen with an outgoing SIP call from gateway (ISDN PRI --> AS5350 --> SIP --> Provider SIP gateway).

  Workaround: There is no workaround.

- CSCty63868

  Symptoms: CUBE crashes at sipSPICheckHeaderSupport.

  Conditions: CUBE crashes while running the codenomicon suite.

  Workaround: There is no workaround.

- CSCty64721

  Symptoms: Improper memory allocation by CTI process crashes the CME.

  Conditions: The CTI front end process is using up huge memory causing the CME to crash eventually. When the crash occurs:

  ```
  Processor Pool Total:140331892    Used:  140150164    Free:     181728
        I/O Pool Total:  27262976    Used:    5508816    Free:   21754160
  ```

  Workaround: There is no workaround.

- CSCty65334

  Symptoms: Unconfigured crypto ACL causes the Cisco 3900 router to crash.

  Conditions: This symptom is observed with a Cisco 3900 image with ISM crypto engine installed and enabled. This may also affect the Cisco 2900 and Cisco 1900 routers with ISM crypto engine installed and enabled.

  Workaround: When changing the crypto ACL configuration, disable the ISM crypto engine first using the **no crypto engine** *slot 0* command, and then change the ACL. After changing the ACL, reload the router with ISM enabled.

- CSCty68348

  Symptoms: If the OSPF v2 process is configured with the **nsr** command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

  Conditions: This symptom is observed under the following conditions:

  - The OSPF router is configured for “nsr”.
  - Shutdown/no shutdown of the OSPF process.

  Workaround: Flapping of the neighbor will fix the issue.

- CSCty68402

  Symptoms: NTT model 4 configurations are not taking effect.

  Conditions: This symptom occurs under the following conditions:

  ```
  policy-map sub-interface-account
   class prec1
  ```

```
  police cir 4000000 conform-action transmit  exceed-action drop
  account
 class prec2
  police cir 3500000 conform-action transmit  exceed-action drop
  account
 class prec3
  account
  class class-default fragment prec4
  bandwidth remaining ratio 1
  account


policy-map main-interface
 class prec1
  priority level 1
  queue-limit 86 packets
 class prec2
  priority level 2
  queue-limit 78 packets
 class prec3
  bandwidth remaining ratio 1
  random-detect
  queue-limit 70 packets
  class prec4 service-fragment prec4
  shape average 200000
  bandwidth remaining ratio 1
  queue-limit 62 packets
 class class-default
  queue-limit 80 packets
```

Workaround: There is no workaround.

- CSCty69981

  Symptoms: Crash observed in HTTP server Codenomicon testing.

  Conditions: The symptom is observed with HTTP server Codenomicon testing.

  Workaround: There is no workaround.

- CSCty71843

  Symptoms: Tracebacks observed at lfd_sm_start and lfd_sm_handle_event_state_stopped APIs during router bootup.

  Conditions: The symptom is observed with L2VPN (Xconnect with MPLS encapsulation) functionality on a Cisco 1941 router (acting as edge) running Cisco IOS interim Release 15.2(3.3)T. This is observed when a router is reloaded with the L2VPN configurations.

  Workaround: There is no workaround.

- CSCty73817

  Symptoms: In large-scale PPPoE sessions with QoS, the Standby RP might reboot continuously (until the workaround is applied) after switchover. This issue is seen when the QoS Policy Accounting feature is used. When the issue occurs, the Active RP remains operational and the Standby RP reboots with the following message: %PLATFORM-6-EVENT_LOG: 43 3145575308: *Mar 16 13:47:23.482: %QOS-6-RELOAD: Index addition failed, reloading self

  Conditions: This symptom occurs when all the following conditions are met:

  1. There is a large amount of sessions.
  2. The QoS Policy Accounting feature is used.
  3. Switchover is done.

Workaround: Bring down sessions before switchover. For example, shut down the physical interfaces that the sessions go through, or issue the Cisco IOS command **clear pppoe all**.

- CSCty76106

  Symptoms: Crash is seen after two days of soaking with traffic.

  Conditions: This symptom occurs with node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, constant frequent polling of SNMP, RCMD, full scale of routes and bidirectional traffic.

  Workaround: There is no workaround.

- CSCty77190

  Symptoms: DTLS is switched back to TLS after reconnect.

  Conditions: This symptom is observed with the following conditions:

  - Test image c3845-advsecurityk9-mz.152-2.T1.InternalUseOnly
  - Test version - Cisco IOS Release 15.2(01)T

  Workaround: Restart the AnyConnect client.

- CSCty78435

  Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

  Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

  Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- CSCty79277

  Symptoms: Line protocol stays down after Authz success and traffic is allowed.

  Conditions: The symptom is observed with Cisco IOS Release 15.2(2)T, running on a Cisco 1900 platform, doing **default inter Fa0/1/0** with 802.1x configurations and re-applying will authenticate the connected MAB supplicant. However, the interface’s line protocol remains in DOWN state and traffic will be allowed.

  Workaround: Do a **shut** and **no shut** and authenticate the connected supplicant.

- CSCty80553

  Symptoms: Multicast router crashes.

  Conditions: The symptom is observed when multicast traffic is routed through an IPsec tunnel and multicast packets are big causing fragmentation.

  Workaround: Make sure that multicast packet sizes do not exceed tunnel transport MTU.

- CSCty80566

  Symptoms: Cisco IOS crashes.

  Conditions: This symptom is observed with Cisco IOS during normal usage.

  Workaround: There is no workaround.

- CSCty83520

  Symptoms: IP Phone -- CUCM --- H323 -- 3845 - PSTN

  1. A call is originated from the IP phone to a PSTN number and it gets connected.
  2. The IP phone puts the call on hold.
  3. The CUCM instructs GW to listen to the Multicast MoH stream.
  4. The Cisco IOS Gateway sends the RTCP packet to Multicast MoH.

  Conditions: This symptom is observed when the H.323 Gateway is configured and the Multicast MoH and MoH stream is sent across an IP Multicast network.

  Workaround 1: Disable the H.323 Multicast MoH functionality in Cisco IOS.

  Workaround 2: Use Unicast MoH.

- CSCty84989

  Symptoms: IKEv2 pushed routes are not installed in the IPv6 inner VRF routing table.

  Conditions: This symptom occurs when using IKEv2 on pure IPV6 tunnels with tunnel protection IPsec and a VRF on the tunnel.

  Workaround: There is no workaround.

- CSCty85634

  Symptoms: A router configured with the Locator ID Separation Protocol (LISP) without an EID-table for the default VRF fails to maintain its LISP map-cache during an RP switchover. After the switchover, the existing remote EID entries in CEF eventually expire and new data packet signals result in repopulation of the LISP map-cache, thus resuming normal operation.

  Conditions: This symptom occurs in a LISP configuration that contains EID-tables for VRFs other than the default and does not contain an EID-table for the default VRF.

  Workaround: Configure an EID-table for the default VRF before the switchover with some lisp configuration such as “ipv4 itr”.

- CSCty86111

  Symptoms: The Cisco ISR G2 router crashes after “no ccm-manager fallback-mgcp” is configured.

  Conditions: This symptom is observed with Cisco ISR G2 router.

  Workaround: There is no workaround.

- CSCty90223

  Symptoms: A crash occurs at nhrp_nhs_recovery_co_destroy during setup and configuration.

  Conditions: This symptom is observed under the following conditions:

  1. Add and remove the ip nhrp configuration over the tunnel interface on the spoke multiple times.
  2. Do shut/no shut on the tunnel interface.
  3. Rapidly change IPv6 addresses over the tunnel interface on the spoke side and on the hub side multiple times.
  4. Replace the original (correct) IPv6 addresses on both the spoke and the hub.
  5. Wait for the registration timer to start.

  The crash, while not consistently observed, is seen fairly often with the same steps.

  Workaround: There is no known workaround.

- CSCty90293

  Symptoms: Router does not encrypt GREv6 packets and send is as clear text.

  Conditions:

  - Configure GREv6 over IPSec IPv6 using Crypto Map.
  - IPv6 CEF is enabled.
  - The GRE packet are encapsulating traversing packet.

  Workaround: Implementing using Tunnel Protection works as workaround.

- CSCty91465

  Symptoms: Ping to a global IP address (interface not part of any VRF) received via a VRF interface does not work even when “vrf receive” and the policy maps are configured correctly to receive the packets from the VRF interface.

  Conditions: The symptom is observed when CEF is enabled.

  Workaround: Disable CEF.

- CSCty92182

  Symptoms: Router crashes with SIGTRAP exception. The cifs_browse_share_sync function alone is consuming a lot of stack memory.

  Conditions: The device crashes because the stack is completely depleted. This shows that there is 0 bytes left out of 6000:

  ```
  %SYS-6-STACKLOW: Stack for process CIFS API Process running low, 0/6000
  ```

  Workaround: There is no workaround.

- CSCty94289

  Symptoms: The drop rate is nearly 1 Mbps with priority configuration.

  Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.

  Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

- CSCty96049

  Symptoms: Several 3750X switches in a stack crash. The crashinfo shows vector 0x200 and stack corruption:

  ```
  C3750E Software (C3750E-UNIVERSALK9-M), Version 15.0(1)SE2, RELEASE SOFTWARE
  (fc3)
     Technical Support: http://www.cisco.com/techsupport
     Compiled Thu 22-Dec-11 00:05 by prod_rel_team
     Signal = 10, Vector = 0x200, Uptime = E
     .
     .
     ========= Stack Dump ========================

     Stack Frame Pointer in Context is 0x46DCB0C, at process level
     : INVALID STACK ADDRESS
  ```

  Conditions: The issue is seen when the switch receives a DHCP using a TLV with a length of 256 or longer. This is not platform specific.

  Workaround: As a workaround, an administrator can disable the DHCP device classifier using the “device-sensor filter- spec dhcp exclude all” command, as shown in the following example:

```
hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
hostname(config)# device-sensor filter-spec dhcp exclude all
hostname(config)# end
```

- CSCty96052

  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

  Conditions: It is an extreme corner case/timing issue. Has been observed only once on release image.

  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty97784

  Symptoms: The router crashes.

  Conditions: This symptom is observed when NBAR is enabled, that is, "match protocol" actions in the QoS configuration, or "ip nbar protocol-discovery" on an interface or NAT is enabled and "ip nat service nbar" has not been disabled.

  Workaround: There is no workaround.

- CSCty98365

  Symptoms: A crash in RF MIB code is seen when B2B remote domain comes up.

  Conditions: The symptom is observed when B2B peers (application redundancy) are configured and come to the redundancy state.

  Workaround: Do not configure B2B peers.

- CSCty98834

  Symptoms: The Cisco c2900, c3900, and c1900 IOS with the ISM VPN crypto engine might crash after some time when you run out of memory on the ISM VPN engine as there are memory leaks during rekey.

  Conditions: This symptom occurs when the ISM VPN crypto engine is enabled.

  Workaround: Disable the ISM VPN module using the **no crypto engine** *slot 0* command.

- CSCtz00431

  Symptoms: Device crashes and tracebacks are seen in syslog process.

  Conditions: The symptom is observed with the following steps:

  1. Configure a capture point and start it.
  2. Remove the policy map associated with the capture point. First time it throws error but second time it accepts. After that, remove the class-map.
  3. Stop the capture point. 4. Restart the capture point.

  Workaround: Do not remove the policy map associated with capture point while capture is active.

- CSCtz02182

  Symptoms: Tracebacks are seen on a flexVPN hub.

  Conditions: The symptom is observed when adding a virtual-template interface type tunnel.

  Workaround: There is no workaround.

- CSCtz02622

  Symptoms: FlexVPN spoke crashed while passing spoke to spoke traffic.

  Conditions: Passing traffic from spoke to spoke or clearing IKE SA on the spoke.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:M/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-3893 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtz03779

  Symptoms: The standby RSP crashes during ISSU.

  Conditions: Occurs when you perform an ISSU downgrade from Release 3.6 to 3.5.

  Workaround: There is no workaround.

- CSCtz04599

  Symptoms: On a Cisco Catalyst 4500/SUP6-E setup on both Cisco IOS Release 15.0(2)SG3 and Release 15.0(2)SG4 you see high CPU and the switchport stuck in a dot1x authentication loop, causing intense RADIUS traffic toward the AAA server. Under these conditions the processes "Dot1x Mgr" and "Auth Manager" will use high CPU and the switch will eventually reload.

  Conditions: The symptom is observed under the following conditions:

  - Cisco Catalyst 4500/SUP6-E.
  - Cisco IOS Release 15.0(2)SG3 and Release 15.0(2)SG4.
  - Port configured in multidomain with dot1x and MAB.
  - Phone configured to use dot1x (phone supplicant).
  - RADIUS server immediately rejects (access-reject) the dot1x auth before the actual dot1x authentication takes place.

  Sequence:

  - Dot1x auth fails (access-reject following the first access-request).
  - The port falls back to MAB.
  - MAB succeeds and the RADIUS server returns the device-traffic-class=voice VSA.
  - The phone sends a new EAPoL frame.

  Workaround: The following workarounds are available:

  1. Configure "authentication priority mab dot1x".
  2. Configure the radius server to reject at a later decision stage to slow the response.

- CSCtz05090

  Symptoms: This is a proactive software enhancement to implement secure best practice procedures into the code.

  Conditions: Cisco ASA with default configuration.

  Workaround: There is no workaround.

- CSCtz07394

  Symptoms: You are not able to ping with a packet size larger than 1494 bytes across the Cisco 887VA router configured for MLP LFI with PPPoA.

Conditions: The symptom is observed when a ping is issued. The PPP fragment gets dropped due to incorrect FFFF padding in the data portion of the fragment.

Workaround: Use a packet size smaller than or equal to 1494 bytes.

- CSCtz08037

  Symptoms: The router fails to pass any traffic after receiving the "%OCE-3-OCE_FWD_STATE_HANDLE: Limit of oce forward state handle allocation reached; maximum allowable number is 50000" error message.

  Conditions: This symptom is observed MPLS L2VPN is configured with EoMPLSoGRE with IPSec encryption on top of the VTI tunnel with IPSec encryption (double encryption).

  Workaround: Reload the router.

- CSCtz08388

  Symptoms: 86x VAE platform DSL line cannot train up with ADSL2/ADSL2+ profile after you manually shut/no shut the DSLAM port.

  Conditions:

  1. Connect 86x VAE DSL WAN port to DSLAM port (either ADSL2/ADSL2+ profile).
  2. Disable/enable the port and the line will not train up again.

  Workaround: There is no workaround.

- CSCtz12714

  Symptoms: A Cisco router configured for voice functions may crash.

  Conditions: The exact conditions to trigger the crash are unknown at this time.

  Workaround: There is no workaround.

- CSCtz13818

  Symptoms: In a rare situation when route-map (export-map) is updated, IOS is not sending refreshed updates to the peer.

  Conditions: The symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.

  Workaround 1: Refresh the updated route-target to use **clear ip route vrf** *vrf-name net mask*.

  Workaround 2: Hard clear the BGP session with the peer.

- CSCtz14980

  Symptoms: When you perform the RP switch, the standby RP (original active one) will keep rebooting.

  Conditions: The symptom is observed when you have "crypto map GETVPN_MAP gdoi fail-close" configured and image is Cisco IOS XE Release 3.6 or 3.7.

  Workaround: There is no workaround.

- CSCtz15211

  Symptoms: The ISM card does not encrypt packets through a double encrypted tunnel.

  Conditions: This symptom is observed with ISR g2 with the ISM module and crypto configured for GRE over IPsec packets to be encrypted through a VTI (double encryption).

  Workaround: Use onboard encryption.

- CSCtz21456

  Symptoms: A router has an unexpected reload due to CCSIP_SPI_CONTROL process.

  Conditions: This issue has been seen in Cisco IOS Release 15.2(3)T.

  Workaround: There is no workaround.

- CSCtz22112

  Symptoms: A VXML gateway may crash while parsing through an HTTP packet that contains the "HttpOnly" field:

  ```
  //324809//HTTPC:/httpc_cookie_parse: * cookie_tag=' HttpOnly'
  //324809//HTTPC:/httpc_cookie_parse: ignore unknown attribute: HttpOnly
  Unexpected exception to CPU: vector D, PC = 0x41357F8
  ```

  Note: The above log was captured with "debug http client all" enabled to generate additional debugging output relevant to HTTP packet handling.

  Conditions: The symptom is observed when an HTTP packet with the "HttpOnly" field set is received.

  Workaround: There is no workaround.

- CSCtz24280

  Symptoms: MSP flows are not identified.

  Conditions: This symptom is observed when "proxy-call-id" is present in the "Route" header of SIP packets.

  Workaround: Remove proxy servers from the topology.

- CSCtz25364

  Symptoms: GM to GM communication between ISM VPN and the Cisco ASR 1000 series router with TBAR enabled is broken.

  Conditions: This symptom occurs when ISM VPN and the Cisco ASR 1000 series router are GMs and TBAR is enabled.

  Workaround: Disable ISM VPN or disable TBAR and switch to counter-based anti-replay.

- CSCtz25953

  Symptoms: "LFD CORRUPT PKT" error message is dumped and certain length packets are getting dropped.

  Conditions: The symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

  Workaround: There is no workaround.

- CSCtz26683

  Symptoms: An unsupported "ip verify unicast ..." configuration applied to an interface may still be shown in **show running-config** after being rejected. Output similar to the following will appear when applying the configuration:

  ```
  % ip verify configuration not supported on interface Tu100
    - verification not supported by hardware
  % ip verify configuration not supported on interface Tu100
    - verification not supported by hardware
  %Restoring the original configuration failed on Tunnel100 - Interface Support
  Failure
  ```

  Conditions: This occurs when there is no prior "ip verify unicast ..." configuration on the interface and when the interface and/or platform do not support the given RPF configuration.

Workaround: In some cases it may be possible to get back to the previous configuration by using a **no** form of the command. In other cases, it will be necessary to reload the device without saving the configuration, or editing the configuration manually if already saved.

- CSCtz27137

  Symptoms: An upgrade to the S640 signature package may cause a Cisco IOS router to crash.

  Conditions: This symptom is observed in a Cisco 1841, 1941, and 2911 router running one of the following Cisco IOS versions:

  - Cisco IOS Release 12.4(24)T4
  - Cisco IOS Release 15.0(1)M4
  - Cisco IOS Release 15.0(1)M8
  - Cisco IOS Release 15.2(3)T

  Workaround: Update the signature package to anything less than S639. If already updated with any package larger than or equal to S639, follow the below steps to disable IPS:

  - Access the router via the console.
  - Enter break sequence to access ROMmon mode.
  - Change the config-register value to 0x2412.
  - Boot the router to bypass the startup-configuration.
  - Configure the basic IP parameters.
  - TFTP a modified configuration to the router's running-configuration with Cisco IOS IPS disabled.
  - Reset the config-register to 0x2102.
  - Enter the **write memory** command and reload.

- CSCtz32521

  Symptoms: In interop scenarios between Cisco CPT and Cisco ASR 9000 platforms, in order to support transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Conditions: This symptom occurs in interop scenarios between Cisco CPT and Cisco ASR 9000 platform. In order to support transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Workaround: There is no workaround.

- CSCtz33536

  Symptoms: SIP KPML subscription fails with:

  ```
  ?xml version="1.0" encoding="UTF-8"?><kpml-response version="1.0" code="533"
  text="Multiple Subscriptions on a Dialog Not Supported"/
  ```

  This happens on a CUBE when the call is transferred on CUCM.

  Conditions: The symptom is observed with SIP to SIP CUBE running Cisco IOS Release 15.1(3)T2.

  Workaround: Use a different DTMF method.

- CSCtz33622

  Symptoms: Multiple crashes on a Cisco ISR that is running latest IOS versions with x25 encapsulation due to managed timer corruption.

  Conditions: The symptom is observed on a Cisco ISR using x25 routing.

Workaround: There is no workaround.

- CSCtz34228

  Symptoms: When NTLM (passive/active) is configured on a Cisco ISR, the user authentication process can generate authentication failure messages.

  Conditions: The symptom is observed when user authentication sees multiple GETs from the browser.

  Workaround: Increase the max-login attempts from a default of five to a larger number.

- CSCtz37863

  Symptoms: IPCP is not in an open state and it does not seem to be calling the This-Layer-Down (TLD) vector.

  Conditions: The symptom is observed if IPv4 saving is enabled and IPCP negotiation failed because of a TermReq received from peer.

  Workaround: There is no workaround.

- CSCtz40621

  Symptoms: Router crash observed.

  Conditions: The symptom is observed when GetVPN GM tries to register to keyserver and keyserver issues a rekey simultaneously.

  Workaround: There is no workaround.

- CSCtz41048

  Symptoms: The **trace mpls ipv4** command is unsuccessful.

  Conditions: The symptom is observed with the **trace mpls ipv4** command.

  Workaround: There is no workaround.

- CSCtz45901

  Symptoms: The **show runn** or **format xml** output for an ATM interface is not displayed in the correct order.

  Conditions: The symptom is observed if there are multiple subinterfaces for an ATM interface and PVC is configured under these.

  Workaround: There is no workaround.

- CSCtz47873

  Symptoms: The command **show crypto ikev2 client flex** does not work as expected.

  Conditions: The symptom is observed with a client/server flexVPN setup.

  Workaround: Execute either **show crypto IKEv2 sa** or **show crypto session detail**.

- CSCtz48615

  Symptoms: AES encryption may cause high CPU utilization at crypto engine process.

  Conditions: The symptom is observed with AES encryption configuration in ISAKMP policy. The issue is seen only when one of the negotiating routers is a non-Cisco device where the key size attribute is not sent in ISAKMP proposal.

  Workaround: Remove ISAKMP policy with AES encryption.

- CSCtz51773

  Symptoms: High CPU seen on routers equipped with an ISM-VPN module. The output of **show process cpu** shows that the process "REVT Background" is using around 70% of the CPU cycles.

  The ISM-VPN module is not visible in **show diag**, and the output of **show crypto engine configuration** indicates that the module status is DEAD.

  Conditions: The symptom is observed with an ISM VPN with a few IPSec tunnels. This can take between a day and a week.

  Workaround 1: Reload the router.

  Workaround 2: For a longer-run workaround and if the traffic volume is not too high, switch to the onboard crypto hardware using the configuration **no crypto engine slot 0**.

- CSCtz59429

  Symptoms: Packets do not match a flow with the attribute "application category voice-video".

  Conditions: This symptom occurs when a flow with the attribute "application category voice-video" is matched for the same attribute.

  Workaround: There is no workaround.

- CSCtz62766

  Symptoms: One or more linecards may be reset. Persistent in the logs:

  ```
  %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  (608/2),process = CEF LC Stats.
  ```

  until:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = CEF LC Stats.
  ```

  Conditions: This issue can be seen on distributed platforms running Cisco IOS Release 12.4T or later code.

  Workaround: Use Cisco IOS 12.4 mainline code, such as 12.4(25f), which is not susceptible.

- CSCtz63438

  Symptoms: In a GETVPN environment, the group member continuously registers to keyserver.

  Conditions: The symptom is observed when the onboard crypto engine is disabled on a Cisco 1900 series platform.

  Workaround: There is no workaround.

- CSCtz67726

  Symptoms: 1. Single probe ID is not permitted on the **ip sla group schedule...** command. For example: **ip sla group schedule** *group id* **schedule-period 5 start now** gives following error messages:

  ```
  %Group Scheduler: probe list wrong syntax %Group schedule string of probe ID's
  incorrect
  ```

  2. Entering the same probe ID under **ip sla group schedule** in the format of "id,id" is accepted but it will display on the running configuration as just single probe ID. For example: **ip sla group schedule** *group* **id,id schedule-period 5 start now**. The running configuration will show **ip sla group schedule** *group* **id schedule-period 5 start now**.

  Conditions: Observed if using single probe ID under **ip sla group schedule...** command.

  Workaround: Use the command **ip sla schedule** for single probe ID.

- CSCtz70623

  Symptoms: A Cisco router may experience a software-forced crash.

Conditions: Crash may occur when a 2-wire cable is unplugged from the G.SHDSL interface.

Workaround: There is no workaround.

- CSCtz70938

  Symptoms: When the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are “service-module” CLI in the configuration, the router crashes.

  Conditions: This symptom occurs when the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are “service-module” CLI in the configuration, the router crashes.

  Workaround: Do not use boot configuration files other than startup-configuration when there are “service-module” CLI in the configuration.

- CSCtz72044

  Symptoms: EzVPN client router is failing to renew ISAKMP security association, causing the tunnel to go down.

  Conditions: The issue is timing-dependent, therefore the problem is not systematic.

  Workaround: There is no workaround.

  CSCtz73157

  Symptoms: CUBE sends 0.0.0.0 when 9971 has video enabled for hold/resume/conference from PSTN caller. CUBE sends correct IP address when 9971 has video disabled for hold/resume/conference from PSTN caller.

  Conditions: The symptom is observed with the following conditions:

  - Cisco IOS Release 15.2(2)T1.
  - Current phone load sip99719.2.4-19.
  - Current CUCM version: 8.5.1.13900-5.
  - MCS7825I4-K9-CMD2A.
  - On the SIP trunk, the box “Retry Video Call as Audio” was checked.

  For the calls with video disabled, the CUBE is sending the 200OK with the C=IN

```
ipX x.x.x.x address.
```

```
Sent:
SIP/2.0 200 OK
Via: SIP/2.0/TCP x.x.x.x:5060;branch=z9hG4bK7322e28fb58f2
From: "name"
<sip:2127153896@x.x.x.x>;tag=1171271~17954349-bc2a-4081-adb4-34491012bb45-24984725
To: <sip:16464831236@x.x.x.x>;tag=D99A474-A1A
Date: Tue, 24 Apr 2012 18:26:17 GMT
Call-ID: f9e43000-f961f049-61593-a28050a@x.x.x.x
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:16464831236@x.x.x.x>;party=called;screen=no;privacy=off
Contact: <sip:16464831236@x.x.x.x:5060;transport=tcp>
Supported: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.2.T1
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
```

```
Content-Length: 241

v=0
o=CiscoSystemsSIP-GW-UserAgent 9798 5431 IN IPX x.x.x.x
s=SIP Call
c=IN IPX x.x.x.x
t=0 0
m=audio 25014 RTP/AVP 0 101
c=IN IPX x.x.x.x
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

For the calls with video enabled, the CUBE is not sending the IP address correctly, as seen here:

```
Sent:
SIP/2.0 200 OK
Via: SIP/2.0/TCP x.x.x.x:5060;branch=z9hG4bK734ab4c88ccb9
From: "name"
<sip:2127153896@x.x.x.x>;tag=1171897~17954349-bc2a-4081-adb4-34491012bb45-24984949
To: <sip:16464831236@x.x.x.x>;tag=DA1D53C-2232
Date: Tue, 24 Apr 2012 18:35:25 GMT
Call-ID: 39f7e280-f961f262-616f4-a28050a@x.x.x.x
CSeq: 102 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:16464831236@x.x.x.x>;party=called;screen=no;privacy=off
Contact: <sip:16464831236@x.x.x.x:5060;transport=tcp>
Supported: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.2.T1
Supported: timer
Content-Type: application/sdp
Content-Length: 278

v=0
o=CiscoSystemsSIP-GW-UserAgent 144 2583 IN IPX x.x.x.x
s=SIP Call
c=IN IPX 0.0.0.0
t=0 0
m=audio 16654 RTP/AVP 0 101
c=IN IPX 0.0.0.0
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
m=video 0 RTP/AVP 126
c=IN IPX 10.5.40.14
```

Workaround: Disable video from CUCM phone page under the 9971.

- CSCtz73263

  Symptoms: MSP is not getting packets on SVI interface and MSP profile is not getting attached to the flow.

  Conditions: The symptom is observed when the **profile flow** command is configured globally and an MSP profile is applied using **media-proxy services** *profile-name*.

  Workaround: Disable MSP using **no profile flow** and enable it again using **profile flow**.

- CSCtz75380

  Symptoms: A Cisco ASR 1000 series router sends malformed radius packets during retransmission or failover to a secondary radius server, e.g.: Cisco CAR.

ISG log if secondary radius server is installed in the network:

```
%RADIUS-4-RADIUS_DEAD: RADIUS server <ip-secondary-Radius-Server>:1645,1646 is
not responding.
%RADIUS-4-RADIUS_ALIVE: RADIUS server <ip-secondary-Radius-Server>:1645,1646 is
being marked alive.

Radius-Server Log:
13:23:01.011: P78: Packet received from 10.0.0.1
13:23:01.011: P78: Packet successfully added
13:23:01.011: P78: Parse Failed: Invalid length field - 63739 is greater than 288
13:23:01.011: Log: Packet from 10.0.0.1: parse failed <unknown user>
13:23:01.011: P78: Rejecting Request: packet failed to parse
13:23:01.011: P78: Trace of Access-Reject packet
13:23:01.011: P78:    identifier = 40
13:23:01.011: P78:    length = 21
13:23:01.011: P78:    reqauth = 23:<snip....>
13:23:01.011: P78: Sending response to 10.0.0.1
13:23:01.011: Log: Request from 10.0.0.1: User <unknown user> rejected
(MalformedRequest).
13:23:01.011: P78: Packet successfully removed
```

Conditions: The issue can occur during retransmission of radius access requests or if radius packets are sent to a secondary radius server.

Workaround: There is no workaround.

- CSCtz76650

  Symptoms: In phase 2 IPv6 DMVPN deployment, traffic for IPv6 hosts behind spokes goes via the hub.

  Conditions: This symptom is observed in IPv6 DMVPN network when using phase 2 configuration and routing protocols with link-local nexthop.

  Workaround: Do not use link-local nexthop routing, instead use unicast nexthops (e.g.: BGP as the routing protocol).

- CSCtz78194

  Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.

  Conditions: The symptom is observed with the Cisco ASR configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.

  Workaround: Shorten the ISAKMP profile name to less than 31.

- CSCtz78868

  Symptoms: Fax issue.

  Conditions: The symptom is observed with poor line condition.

  Workaround: Use modem passthrough.

- CSCtz79991

  Symptoms: Router crashes @ lic_install_notify_and_print_output.

  Conditions: The symptom is observed when license files are copied to flash of the router. After checking for EULA, the router crashes.

  Workaround: There is no workaround.

- CSCtz85134

  Symptoms: A manually generated self-signed trustpoint gets erased and a new trustpoint is auto-generated when SSL-Express Accelerator is enabled and the router's configuration is saved and it is reloaded.

  Conditions: This symptom is observed when the trustpoint is generated manually and SSL-Express Accelerator must be enabled. This issue is seen only when the configuration is saved and the router is reloaded.

  Workaround: Disable SSL-Express Accelerator.

- CSCtz86747

  Symptoms: Router crashes upon removing all the class-maps from policy-map.

  Conditions: This symptom is observed when a route crashes while removing all user defined class-maps with live traffic.

  Workaround: Shut the interface first before removing class-map.

- CSCtz88595

  Symptoms: NTLM VIP pop-up shows actual server URL, instead of VIP address.

  Conditions: The symptom is observed with NTLM authentication method and when virtual IP is configured. If GET request comes for the session already in INIT state, this issue will occur.

  Workaround: There is no workaround.

- CSCtz90154

  Symptoms: Rapid getVPN re-registration by GM when IPsec failure occurs during initial registration. Multiple ISAKMP SAs created and deleted per second.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.2(1)S or Release 15.2(1)S2 as a GM.

  Workaround: There is no workaround.

- CSCtz94964

  Symptoms: Sub-classification fails when protocol discovery is enabled.

  Conditions: The symptom is observed when sub-classification is configured first and then protocol discovery is configured.

  Workaround: There is no workaround.

- CSCtz95782

  Symptoms: When traffic streams are classified into multiple classes included with LLQ (with QoS preclassify on the tunnel interface and the crypto map applied to an interface) packets are dropped on crypto engine on the Cisco 890 series router with buffers unavailable.

  Conditions: This symptom is observed when IPsec and QoS are used when QoS preclassify is on the tunnel interface and a crypto map is on the main interface.

  Workaround: Use tunnel protection or VTI instead of the crypto map on the interface.

- CSCtz96167

  Symptoms: QoS DSCP cases failing.

  Conditions: The symptom is observed with a QoS profile (with DSCP as 31 configured under SBE) is being hit but DSCP bit is still sent as 0.

  Workaround: There is no workaround.

- CSCtz97244

  Symptoms: IPSLA Video Operation with VRF support sees no packets received at responder.

  Conditions: This symptom occurs when no emulate CLI is specified with the input interface.

  Workaround: Use the emulate CLI to specify the input interface that has access to the VRF.

- CSCtz99916

  Symptoms: The Cisco 3945 router does not respond to a reinvite from CVP.

  Conditions: This symptom occurs when call legs are not handled in a proper IWF container.

  Workaround: There is no workaround.

- CSCua06629

  Symptoms: The **sh ipv6 mobile pmipv6 mag globals** command does not show any output.

  Conditions: The symptom is observed only when domain and MAG configurations are present.

  Workaround: If MAG configuration is complete (all requisite access interfaces and peers are configured) then this issue will not be seen.

- CSCua08876

  Symptoms: IPv6 LCP fails to negotiate on PPP over VDSL connections on Cisco 867VAE routers. (If you have “ppp negotiation” debug enabled, you will see a “LCP: O PROTREJ’ message displayed”.)

  Conditions: First seen in Cisco IOS Release 15.1(4)M4 but it has found to be in Cisco IOS Release 15.2(3)T.

  Workaround: There is no workaround.

- CSCua15292

  Symptoms: Router may report unexpected exception with overnight stress traffic.

  Conditions: The symptom is observed with the following conditions:

  - Cisco ISR 3925E is deployed as DMVPN hub router and about 100Mbps traffic is controlled by PfR MC with dynamic PBR.
  - Router logs with

  ```
  %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
  destaddr=172.8.9.8, prot=50, spi=0xE8FB045F(3908764767), srcaddr=10.0.100.1, input
  interface=GigabitEthernet0/0
  ```

  Workaround: There is no workaround.

- CSCua16561

  Symptoms: Jumbo-frame packets sent over IPsec VPN from a Cisco 800 series router are dropped on the receiving VPN peer.

  Conditions: The symptom is observed when the packet size is above the standard FastEthernet MTU size (the problem was observed for any packet more than 1512 bytes), and the path MTU is such that no fragmentation is needed.

  Workaround: Disable the onboard crypto accelerator:

  ```
  no crypto engine onboard 0
  ```

- CSCua17746

  Symptoms: IKEv2 with RSA-Sig as auth session will fail.

  Conditions: The symptom is observed with:

  - IKEv2 + RSA-Sig auth + ISM VPN; or

  - IKEv2 + RSA-Sig auth + 7200 with VSA.

  Workaround: Disable ISM VPN or VSA or do not use IKEv2 RSA-Sig as auth.

- CSCua18138

  Symptoms: If you enable the mobile IP function, a Cisco 819 will crash after a cable is removed.

  Conditions: The symptom is observed when redundancy group is configured under "ip mobile router".

  Workaround: There is no workaround.

- CSCua19294

  Symptoms: IPSLA intermittently reports wrong minimum RTT of 1 millisecond or below.

  Conditions: Observed on microsecond precision setting sending multiple number-packets at 100msec intervals.

  Workaround: There is no workaround.

- CSCua22313

  Symptoms: SSLv3.0- and TLSv1.0-based data transfer using certain older client applications (like IE6) fails.

  Conditions: This symptom is observed when the HTTPS page is fetched by a client application that does not have a fix for the BEAST vulnerability (http://blogs.cisco.com/security/beat-the-beast-with-tls/) and the connection is optimized by SSL-Express Accelerator in WAAS-Express.

  Workaround: Upgrade the client application to the latest version or at least a version that has a fix for BEAST in case of Internet Explorer version 8 or higher.

- CSCua29428

  Symptoms: When you try to configure **router rip**, the "version" sub-command does not exist.

  Conditions: The symptom is observed with the **router rip** command.

  Workaround: There is no workaround.

- CSCua31934

  Symptoms: Crash seen at __be_address_is_unspecified.

  Conditions: The symptom is observed with the following conditions:

  1. It occurs one out of three times and it is a timing issue.
  2. DMVPN tunnel setup between Cisco 2901 as spoke and Cisco ASR 1000 as hub.
  3. Pass IPv4 and IPv6 traffic between the hub and the spoke for 5-10 minutes.
  4. It can occur with v6 traffic alone.
  5. If you remove the tunnel interface on the ASR and add it again using **conf replace nvram:startup-config** the crash will occur.

  Workaround: Use CLI to change configuration instead of the rollback feature.

- CSCua33527

  Symptoms: Traceback seen after second or third switchover:

  ```
  %LFD-SW2-3-SMBADEVENT: Unexpected event CO_WAIT_TIMEOUT for state RUNNING -Traceback=
  7908E9Cz 7909848z 79099CCz 7909B9Cz 78DBF20z 523292Cz 522C1D4z
  ```

  Conditions: The symptom is observed with a quad-sup scenario/setup. This traceback is seen on the new active RP after second switchover onwards.

Workaround: There is no workaround.

- CSCua33821

  Symptoms: CPU utilization shoots up to 99% after configuring crypto maps.

  Conditions: The symptom is observed after applying crypto maps.

  Workaround: There is no workaround.

- CSCua35884

  Symptoms: The **ipv6 cef** option is missing from serial and ATM interface commands.

  Conditions: The symptom is observed with the following CLI:

  conf t int s0/2/0 ipv6 c?

  Returns

  Workaround: There is no workaround.

- CSCua38881

  Symptoms: Router reloads at clear_dspm_counter_per_bay.

  Conditions: This issue is observed from Cisco IOS interim Release 15.2(3.16)M0.1 on Cisco 5350 and Cisco 5400 routers.

  Workaround: There is no workaround.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

  Conditions: The issue is seen on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua44462

  Symptoms: DNS reply is not cached.

  Conditions: DNS based X25 routing. DNS server is reachable via IPsec over Gig link and SHDSL links. There are Cisco devices at different locations. Few of them are communicating to DNS server via IPsec over Gig link and few of them are communicating via IPsec over ATM (EHWIC-4SHDSL-EA and HWIC-4SHDSL). It is seen that the UDP reply contains the x25 address to IP address resolution but it is not being used by the router causing X25 calls to fail.

  Workaround: There is no workaround.

- CSCua45548

  Symptoms: Router crashes with **show ip sla summary** on longevity testing.

  Conditions: The symptom is observed with Cisco 2900, 1900, and 3945 routers configured with IPSLA operations. The router which was idle for one day crashes on issuing the command **show ip sla summary**.

  Workaround: There is no workaround.

- CSCua45685

  Symptoms: A Cisco 2951, 3925, or 3945 crashes during rekey when GetVPN is configured and rekey packet size > MTU.

  Conditions: The symptom is observed if a rekey is coming through the interface where a crypto map is applied.

Workaround: There is no workaround.

- CSCua50490

  Symptoms: Parts of the IOS configuration for the interface UCSE are not automatically applied onto the UCSE after a module OIR.

  Conditions: The symptom is observed after a module OIR or when a UCSE interface configuration is being changed while the module is not fully up and running.

  Workaround: Repeat the interface UCSE configuration in IOS after the module comes up completely.

- CSCua60785

  Symptoms: Metadata class-map matches only the first of the following filter, if present, in a class map (the other media-type matches are skipped):

  match application attribute [category, sub-category, media-type, device-class] *value-string*
  match application application-group *value-string*

  Conditions: Seen in a case where the class map has the aforementioned filters.

  Workaround: There is no workaround.

- CSCua64100

  Symptoms: SCTP receives message fails.

  Conditions: None.

  Workaround: There is no workaround.

- CSCua78782

  Symptoms: Authentication of EzVPN fails.

  Conditions: The symptom is observed with BR-->ISP-->HQ.

  Workaround: There is no workaround.

- CSCua84879

  Symptoms: Crash at slaVideoOperationPrint_ios.

  Conditions: The symptom is observed when IPSLA video operations are configured and **show running-config** is issued.

  Workaround: There is no workaround.