Caveats for Cisco IOS Release 15.1(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 15.1(4)M7

Cisco IOS Release 15.1(4)M7 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M7 but may be open in previous Cisco IOS releases

- CSCsl18054

  Symptom: A local user created with a one-time keyword is removed after unsuccessful login attempts. A one-time user should be removed automatically after the first successful login and not after unsuccessful login attempts.

  Conditions: This symptom occurs on a router running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCtl90292

  Symptom: The following error messages are displayed:

  ```
  an 18 08:00:16.577 MET: %SYS-2-MALLOCFAIL: Memory allocation of 9420 bytes failed from
  0x42446470, alignment 32 Pool: I/O Free: 11331600 Cause: Memory fragmentation
  Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "BGP I/O", ipl= 0,
  pid= 564 -Traceback= 417E8BEC 4180FA6C 42446478 42446B64 42443984 40FC18C8 40FCCB4C
  40FD1964 403BDBFC 403BCC34 40344508 403668AC
  Show buffers shows: 1. Increased miss counters on the EOBC buffers. 2. Medium buffer
  leak
  Router#sh buffers Buffer elements: 779 in free list (500 max allowed) 1582067902 hits,
  0 misses, 619 created
  Interface buffer pools: .... Medium buffers, 256 bytes (total 89647, permanent 3000,
  peak 89647 @ 00:01:17): 273 in free list (64 min, 3000 max allowed)
  EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400): 0 in free list (0 min, 2400
  max allowed) 2400 hits, 161836 fallbacks 1200 max cache size, 129 in cache ....
  ```

  Conditions: This symptom is observed when several hits and failures are seen for medium buffers. All are linktype IPC. For example: Buffer information for Medium buffer at 0x4660E964 ... linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0 if_input 0x481DEA50 (EOBC0/0), if_output 0x0 (None)

  Also, “show buffers old” shows some buffers hanging on EOBC buffers list for a really long time like a few weeks or more.

  Workaround: There is no workaround.

- CSCtn10698

  Symptom: CUBE crashes at sipSPI_ipip_free_channel_info_data.

  Conditions: This symptom occurs during a glare condition between UPDATE and ReINVITE, that is, Received UPDATE on one leg and Received INVITE on the other leg.

  Workaround: There is no workaround.

- CSCtn72925

  Symptom: PFR fails to get notified about interface state changes.

  Conditions: The issue is seen specifically when using Frame Relay and Multilink Frame Relay subinterfaces as PFR external exits and the main interface flaps.

  Workaround: Use the following command:

  clear pfr master *.

- CSCtq91305

  Symptom: Standby cannot reach HOT sync state with active. The standby RP keeps resetting. The following message is displayed:

```
*Apr 18 15:38:47.704: %SYS-3-CPUHOG: Task is running for (3305)msecs, more than
(2000)msecs (1/1),process = IPC Dynamic Cache.
```

Conditions: This symptom occurs with SSO mode, when the Cisco ASR1k is configured with ISG as dhcp server and with a low dhcp lease timer.

Workaround: There is no workaround.

- CSCtr10577

  Symptom: The following error message may be seen:

  ```
  OCE-3-OCE_FWD_STATE_HANDLE limit reached.
  ```

  Conditions: This symptom is observed under high traffic.

  Workaround: There is no workaround.

- 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.

- CSCts11166

  Symptom: 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.

- CSCtw74339

  Symptom: Blocked MRIB and SNMP IPC send time outs with no issues in the platform layer.

  Conditions: This symptom occurs in a control session when RPC replies using the seat ID as the dest_port and other normal control messages use IPC_SEAT | IPC_CONTROL_PORT_ID as the dest_port. Because of this, 2 messages from the same control session do not match when we receive an acknowledgement for one of them.

  Workaround: There is no workaround.

- CSCtx23534

  Symptom: 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.

- CSCtx31177

  Symptom: A watchdog crash is seen in avl_search.

  Conditions: This symptom is observed under the following conditions:

  1. When BFD/REP [pseudo-preemptive processes] is configured in the box.
  2. When an interrupt returns a buffer.

  Workaround: There is no workaround.

  More-Info: The AVL tree of our concern is used to account memory, cpu, buffer usage.

  1. A new process is created and we try to add a new entry into the avl tree for accounting.

2. When we are in the middle of inserting an entry into the avl tree, interrupt/pseudo-preemption[PP] happens.
3. Interrupt/PP returns a buffer/allocates memory and then we try to account the buffer usage.
4. To account the buffer, we traverse the AVL tree and end up looping , as the tree is not stable.

- 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 symptom occurs when Websense URL filtering is enabled and long URLs are accessed.

  Workaround 1: Disable URL filtering.

  Workaround 2: Do not invoke long URLs.

- 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.

- CSCty80553

  Symptom: 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.

- CSCtz01126

  Symptom: With 2xT1s in an IMA bundle, when a single T1 physical interface receives a hit, unexpectedly the IMA interface flaps even when the second T1 interface is running clean.

  Conditions: This symptom occurs in several Cisco 2800 routers which use VWIC2-2MFT-T1/E1 cards and AIM-ATM modules. The routers run on different IOS versions such as Cisco IOS Release 12.4(24)T3, Cisco IOS Release 12.4(15)T13b and Cisco IOS Release 15.1(3)T3.

  Workaround: There is no workaround.

- CSCtz12714

  Symptom: 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.

- CSCtz13023

  Symptom: A crash occurs during registration in SRST mode.

  Conditions: This symptom occurs during registration in SRST mode.

Workaround: This issue is fixed and committed.

- 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).

- CSCua14640

  Symptom: The router configuration order changes after the router reloads.

```
BEFORE ------------
ntp server 223.168.150.10 ntp server 223.168.151.10
AFTER -------------
ntp server 223.168.151.10 ntp server 223.168.150.10
```

  Conditions: There are no specific conditions for this symptom.

  Workaround: There is no workaround.

- CSCua45206

  Symptom: 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 because this is an unsupported configuration.

- 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.

- CSCua70065

  Symptom: 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.

- CSCua71038

  Symptom: A Cisco router crashes.

  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

- 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

- CSCub12694

  Symptom: Interrupt scheduler tracebacks seen.

  Conditions: The following are 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.

  Further Problem Description:

- CSCub30381

  Symptom: 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.

- 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.

- 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 <<<
  ```

- CSCub82495

  Symptom: Serial Interface associated with a Channel-group goes down after a router reload or reboot.

  Conditions: This symptom occurs after reload and is applicable to the following:

  - HWIC-1CE1T1-PRI
  - HWIC-2CE1T1-PRI
  - NM-8CE1T1-PRI Line Cards.

  Workaround: Do a “shutdown” and “no shutdown” of the corresponding Serial Interface of the channel-group.

- CSCuc09483

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

  Conditions: This symptom occurs when a privilege 15 user may run TCL commands.

  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

- CSCuc10966

  Symptom: A router crashes at Process = UNICAST REKEY.

  Conditions: This symptom occurs a COOP split and merge.

  Workaround: There is no workaround.

- CSCuc41531

  Symptom: Forwarding loop is observed for some PfR-controlled traffic.

  Conditions: This symptom is observed with the following conditions:

  - Traffic Classes (TCs) are controlled via PBR.
  - The parent route is withdrawn on selected BR/exit.

  Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class ...** command (this fixes the issue until the next occurrence).

- CSCuc45115

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

  Conditions: This symptom is observed in the case where there are two Overlay addresses of a different Address Family on the same NBMA (such as IPv4 and IPv6 over Ipv4). This issue 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.

- CSCuc82551

  Symptom: 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 While trying to obtain
  the data from IP SLAs Path-Echo (rttMonStatsCollectTable) by SNMP polling operation.
  ```

  Workaround: Remove the SNMP configuration from the router or schedule the probe before polling via SNMP.

- CSCuc95160

  Symptom: 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.

- 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.

- 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
  ```

- CSCud65796

  Symptom: Encryption stops with VSA upon removing and reapplying tunnel protection on any one of the tunnel interfaces.

  Conditions: This symptom occurs in DMVPN with shared IPsec profiles (shared keyword - atleast two m-gre tunnels).

  Workaround: Perform shut/no-shut on the tunnel interface.

- 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 both the physical and tunnel interface are flapping.

  Workaround: There is no workaround.

- 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: Users may experience “no audio” when the router is supposed to be playing IVR (prompt play).

  Conditions: This symptom occurs on the Cisco 3925E and Cisco 3945E platforms when there are more than 350 concurrent prompt plays.

  Workaround: There is no workaround.

- 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.

  Workaround 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”.

- CSCud93758

  Symptom: A router crashes due to the following messages:

  - SYS-3-CPUHOG
  - SYS-2-WATCHDOG

  Conditions: This symptom occurs on the ISDN L2 process.

  Workaround: There is no workaround.

- CSCue04841

  Symptom: When the SM module is removed, a %DXMRVL_FLTMG-7-INTERNAL_ERR output occurs with a traceback and when the SM module is reinserted, and the “switchport mode trunk” command is entered, a crash occurs.

  Conditions: This symptom occurs in Cisco IOS Release 15.1(4)M5.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCue36360

  Symptom: The following error message is seen followed by a software forced reload:

  ```
  CMD: 'wr mem' 12:42:12 MST Wed Jan 30 2013 Jan 30 19:42:18.245: %SYS-6-STACKLOW: Stack
  for process FTP Write Process running low, 0/6000
  ```

  Conditions: This symptom occurs on a router running Cisco IOS while auto archiving the configuration to a file server.

  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*.

- CSCue43669

  Symptom: There is a 2-10% packet loss to hypervisor and VM.

  Conditions: This symptom occurs in phase III DMVPN where the spoke contains a UCSE.

  Workaround: Use the external interface and remove QoS preclassify from the tunnel. Also, if you use the mod/1 port, this problem will be resolved. In this example ucse4/1 works, but ucse4/0 has drops.

- CSCue48419

  Symptom: 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.

- 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. Another symptom is that when a Serial interface has HDLC32 hardware, packet drop is observed in another interface such as GigabitEthernet, when output

queueing policies are applied to both of these interfaces: Serial and GigabitEthernet. The dropped packets can include keepalives for routing protocols such as OSPF, EIGRP, or BGP, and this will result in routing protocol flaps.

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.

- 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.

- CSCue56272

  Symptom: The Cisco ISR crashes due to watchdog timeout after SYS-3-CPUHOG errors with a traceback.

  Conditions: This symptom is observed with voice traffic through the router.

  Workaround: There is no workaround.

- CSCue59775

  Symptom: The device crashes.

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

  Workaround: There is no workaround.

- 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.

- 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.

- CSCue68318

  Symptom: 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.

- 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
------------------ 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
Enter hex value: 0x22CF95C4 0x22CF95C4:ip_mforward(0x22ce9448)+0x51c Enter hex value:
0x22CF0044 0x22CF0044:ip_mforward(0x22ce9448)+0x51c
```

  Conditions: This symptom is observed with the Cisco 2911 running Cisco IOS Release 15.1(4)M3. When IP Multicast is used with NAT, in certain scenarios when NAT functionality returns error, multicast code does not free duplicate packet buffers eventually leading to exhaustion of packet buffer pool in the router.

  Workaround: There is no real workaround except to disable NAT.

- 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.

- 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).

- 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.

- 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.

- CSCuf51357

  Symptom: An SSLVPN-enabled router crashes repeatedly and TCP process leaks are observed with the following messages:

  ```
  Nov 8 2012 15:23:53: SYS-2-MALLOCFAIL Memory allocation of 1740 bytes failed from
  0x2152A990, alignment 128
  Pool: I/O Free: 55984 Cause: Memory fragmentation Alternate Pool: None Free: 0 Cause:
  No Alternate pool -Process= "encrypt proc", ipl= 3, pid= 301
  -Traceback= 23B95D80z 21526538z 21526C70z 21529D10z 23158AE4z 26989D68z 2698B4E4z
  2697C780z 2697CD60z 24233A58z 2424D6C8z 2424A25Cz 23B829BCz 23B829A0z
  ```

  Conditions: This symptom occurs due to memory corruption at tcp_ha_sync_estab_connection().

  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.

- CSCuf89865

  Symptom: MAC addresses are being learnt from the STP blocking port.

  Conditions: This symptom occurs when the STP topology is changed and the FWD port goes to BLK state.

  Workaround: Manually refresh the MAC address table through a CLI command.

- 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.

- CSCuf93471

  Symptom: After a brief unavailability of LDAP CRL, no new CRL fetches can be performed. The following messages are seen on the interface:

  ```
  ---- Mar 28 08:23:37.988: CRYPTO_PKI: Retreive CRL using LDAP DIRNAME Mar 28
  08:23:37.988: CRYPTO_PKI: Failed to send the request. There is another request in
  progress. -----
  ```

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

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

- CSCug25383

  Symptom: A memory corruption crash occurs on a router running Cisco IOS Release 15.1(4)M6 or later versions. Crashinfo would contain errors similar to following:

  ```
  %SYS-3-BADMAGIC: Corrupt block at 4B47BC14 (magic EF4321CD) -Traceback= [Omitted]
  %SYS-6-MTRACE: mallocfree: addr, pc 4D7D4F0C,41EAA79C 4D7D4F0C,40000294
  4D59FAD8,41EAA780 4D59FAD8,4000020A 4B47BC44,44D38F78 4D7D3E3C,44D3B290
  4D7D3E3C,4000001E 4D7D1B84,44D3B290 %SYS-6-MTRACE: mallocfree: addr, pc
  4D7D1B84,30000042 4D5A2130,60000028 4D5A1F8C,419747BC 4D7D3C00,419855E0
  4D7D3C00,40000106 48B2CAF4,41974508 48B2CAF4,400000BA 4D5A0A20,419FDAB4
  %SYS-6-BLKINFO: Corrupted magic value in in-use block blk 4B47BC14, words 0, alloc
  B0D0B0D, Free, dealloc B0D0B0D, rfcnt 44D3B2FC -Traceback= [Omitted] %SYS-6-MEMDUMP:
  0x4B47BC14: 0xEF4321CD 0x41974734 0xB0D0B0D 0xB0D0B0D %SYS-6-MEMDUMP: 0x4B47BC24:
  0xB0D0B0D 0xB0D0B0D 0x15A3C78B 0x0 %SYS-6-MEMDUMP: 0x4B47BC34: 0x44D3B2FC 0x4B470408
  0xEF4321CD 0x44D38E08
  ```

  Conditions: This symptom occurs in a router running Cisco IOS Release 15.1(4)M6.

  Workaround: Downgrade to Cisco IOS Release 15.1(4)M5 or earlier versions.

- CSCug34485

  Symptom: Multiple Cisco products are affected by a vulnerability involving the Open Shortest Path First (OSPF) Routing Protocol Link State Advertisement (LSA) database. This vulnerability could allow an unauthenticated attacker to take full control of the OSPF Autonomous System (AS) domain routing table, blackhole traffic, and intercept traffic.

  Conditions: The attacker could trigger this vulnerability by injecting crafted OSPF packets. Successful exploitation could cause flushing of the routing table on a targeted router, as well as propagation of the crafted OSPF LSA type 1 update throughout the OSPF AS domain.

  To exploit this vulnerability, an attacker must accurately determine certain parameters within the LSA database on the target router. This vulnerability can only be triggered by sending crafted unicast or multicast LSA type 1 packets. No other LSA type packets can trigger this vulnerability.

  OSPFv3 is not affected by this vulnerability. Fabric Shortest Path First (FSPF) protocol is not affected by this vulnerability.

  Workaround: 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-20130801-lsaospf

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 5.8/5.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:P/E:H/RL:U/RC:C

CVE ID CVE-2013-0149 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

- CSCug36075

  Symptom: Layer 1 on the ISDN PRI does not come up after a reload.

  Conditions: This symptom occurs after a reload.

  Workaround: Perform a shut/no shut.

- 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.

- CSCug59650

  Symptom: There is an intermittent issue where users will successfully authenticate via Auth-Proxy and download the proxy-acls, but the ACEs do not get applied to the interface ACL resulting in user traffic getting blocked.

  Conditions: This symptom occurs when IOS Auth-Proxy is configured on a Cisco 2911 router running Cisco IOS Release 15.1(4)M2. This is an intermittent issue.

  Workaround: Clear the auth-proxy session manually or wait for the Auth-Proxy idle timeout to expire.

- CSCug71832

  Symptom: I/O memory leaks occur with the following error messages:

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

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

  Workaround: There is no workaround.

- 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.

- 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.

Resolved Caveats—Cisco IOS Release 15.1(4)M6

Cisco IOS Release 15.1(4)M6 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M6 but may be open in previous Cisco IOS releases

- CSCso88138

  Symptoms: When there is a link flap or a reload, RSVP shows that the interface is down while actually the interface is up. Because of this, the tunnel may take a backup path even when the interface is up.

  Conditions: The conditions for this symptom are unknown at this time.

  Workaround: Perform a shut/no shut on the interface.

- CSCsz30049

  Symptoms: A router may crash with memory corruption or with one of the two following messages:

  ```
  %SYS-6-STACKLOW: Stack for process HQF Shaper Background running low, 0/6000
    %SYS-6-STACKLOW: Stack for process PPP Events running low, 0/12000
  ```

  In the case of memory corruption, a corrupted block will be in an address range very close to process or interrupt level 1 stack (this information is available in the crashinfo file).

  Conditions: This symptom is observed on routers running Cisco IOS Release 12.2SB when all of the following conditions are met:

  – The router is configured for VPDN/L2TP.

  – There is a mixture of PPPoVPDN and “MLP Bundle” users.

  – QoS service policy with queuing actions (bandwidth guarantee or shaper) is applied to virtual access interfaces for both types of users.

  Here is a way to find out if there are normal PPP users or MLP users:

  ```
  PPP User via CLI:
   Router#sh user | inc PPP.*00 [1-9]
     Vi4          user#wl-cp03-7k2#4 PPPoVPDN     00:00:00 30.3.0.47

   MLP via CLI:
   Router#sh user | inc MLP.*00 [1-9]
     Vi8          user#wl-cp04-7k2#5 MLP Bundle   00:00:00 30.4.0.54
  ```

  Workaround 1: Allow only PPPoVPDN (i.e.: prevent “MLP Bundle” creation).

  Workaround 2: Disable QoS for “MLP Bundle” users or all users.

- CSCtd67668

  Symptoms: A router running Cisco IOS may crash.

  Conditions: This symptom is observed with netflow configured on a virtual-template interface.

  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.

- CSCti51196

  Symptoms: SSH to any IPv6 link-local address connects to itself.

  Conditions: This symptom is observed when you configure SSH and try to connect to any link-local address using SSH.

  Workaround: There is no workaround.

- CSCtj95182

  Symptoms: Scanning for security vulnerabilities may cause a High CPU condition on the Cisco Catalyst 3750.

  Conditions: This symptom occurs when a network scanner runs against the Cisco Catalyst 3750 running Cisco IOS Release 12.2.55.SE.

  Workaround: There is no workaround.

  Additional Information: Vulnerable versions:

  - Cisco IOS Release 12.2(52)EX through Cisco IOS Release 12.2(55)SE4.
  - Cisco IOS Release 15.1(3)T through Cisco IOS Release 15.1(4)XB8a.
  - Cisco IOS Release 15.2(1)GC through Cisco IOS Release 15.2(3)XA.

  First fixed in: Cisco IOS Release 12.2(55)SE5, Cisco IOS Release 15.0(1)EX, Cisco IOS Release 15.1(1)SG, Cisco IOS Release 15.2(1)E, Cisco IOS Release 15.2(4)M, and Cisco IOS Release15.3(1)T.

  In the meantime, Cisco published several security advisories for Smart Install vulnerabilities:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-smart-install

- CSCtl88673

  Symptoms: Enhancements to GDOI processing.

  Conditions: The conditions for this symptom are unknown at this time.

  Workaround: There is no workaround.

- CSCtl99174

  Cisco IOS Software contains a memory leak vulnerability that could be triggered through the processing of malformed Session Initiation Protocol (SIP) messages. Exploitation of this vulnerability could cause an interruption of services. Only devices that are configured for SIP inspection are affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP inspection.

This advisory is available at the following link:

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

- CSCtn08613

  Symptoms: A Cisco router crashes when interfacing with UCCX.

  Conditions: This symptom has been experienced on a UC560 running Cisco IOS Release 15.1(2)T2 when making consult transfer calls.

  Workaround: There is no workaround.

- 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 Cisco IOS Release12.4(24)T4.

  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.

- CSCtn81231

  Symptoms: Multicast traffic is not forwarded out of the RBE interface due to incomplete multicast adjacency.

  Conditions: This symptom is seen on an ATM DCHP host that is running IGMPv2 that is established over RBE interface to router. Multicast group join is successful. However, multicast adjacency is incomplete and therefore cannot forward multicast traffic.

  Workaround: Use the **shutdown** command followed by the **no shutdown** command on the ATM main interface.

- CSCto87436

  Symptoms: In certain conditions, an 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: This symptom occurs if an SSH connection to the Cisco IOS device is slow or idle.

  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

- CSCtq14253

  Symptoms: Joins/registers not forwarded to the RP when first configured.

  Conditions: This symptom is observed when the router is first configured.

  Workaround: Reload all routers in the setup.

- 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.

- 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: This symptom is observed with a Cisco ISRG2 3900 series platform using PPC architecture.

  Workaround: There is no workaround.

- CSCtq41512

  Symptoms: After reload, the 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.

- CSCtq51039

  Symptoms: Traffic is dropped with VFR + Cisco Wide Area Application Services (WAAS).

  Conditions: This symptom 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 the following interface:

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t4/feature/guide/ft_admss.html

- CSCtq91063

  Symptoms: A Cisco router may unexpectedly reload due to bus error or generate a spurious access.

Conditions: This symptom occurs when fragmentation of a tunneled packet fails due to the F/S particle pool running out of free particles. The F/S pool is used for fragmentation, so exhaustion of this pool will occur when there is a large amount of traffic flowing for which fragmentation is required. By default, path MTU discovery is enabled for tunnels which means that fragmentation is done at the tunnel interface, rather than the underlying interface and this issue is not hit. If the MTU is overridden, then it may become exposed to this issue. Assuming the tunnel is over an Ethernet interface with MTU of 1500, this will happen by setting the tunnel MTU to greater than 1476 bytes.

Workaround 1: Remove MTU override from the tunnel interface.

Workaround 2: Configure “service disable-ip-fast-frag”.

Workaround 3: Reduce hold queue sizes such that the total size of the queues for all active interfaces in the system does not exceed 512.

- CSCtr79748

  Symptoms: Memory leak occurs with the “ip tcp header-compression” configuration on the Virtual-Template interface.

  Conditions: This symptom is observed when “ip tcp header-compression” is configured on the Virtual-Template interface.

  Workaround: Delete “ip tcp header-compression”.

- CSCts65564

  Symptoms: In a large-scale DMVPN environment, a DMVPN hub router may crash in the Cisco IOS process under high-scale conditions.

  Conditions: This symptom only occurs if CRL caching is disabled (with the **crl cache none** command under the pki trustpoint configuration).

  Workaround: Enable CRL caching (this is the configured default).

- 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: This 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.

- CSCtu08373

  Symptoms: The router crashes at various decodes including fw_dp_base_process_pregen and cce_add_super_7_tuple_db_entry_common.

  Conditions: This symptom occurs when the Cisco IOS firewall is configured and traffic flows through the router.

  Workaround: There is no workaround.

- CSCtu23195

  Symptoms: The SNMP ifIndex for serial interfaces (PA-4T/8T) becomes inactive after PA OIR.

  Conditions: This symptom is observed with a PA OIR.

  Workaround: Unconfigure and reconfigure the channel-groups of the controller and reload the router.

- CSCtw79510

  Symptoms: VPN client users cannot be forced to change their passwords in the next login.

  Conditions: This symptom is observed with an authentication problem while using the password change option.

  Workaround: There is no workaround.

- CSCtw89123

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

  Conditions: This 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 a multilink interface.

- CSCtx56174

  Symptoms: A 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 symptom is seen with websense URL filtering enabled and with zone based firewalls.

  Workaround: Disable URL-based filtering.

- CSCtx86539

  Symptoms: NAT breaks SIP communication with addition of media attributes.

  Conditions: This symptom is observed with NAT of SIP packets.

  Workaround: There is no workaround.

- CSCty51453

  Symptoms: Certificate validation using OCSP may fail, with OCSP server returning an “HTTP 400 - Bad Request” error.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T2 and later releases.

  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.

- CSCty56850

  Symptoms: Routers are not updating the cnpdAllStatsTable with traffic from all expected protocols.

  Conditions: This symptom is observed with routers that are running Cisco IOS 15.x (tested in 15.0, 15.1, and 15.2(2)T).

  Workaround 1: Use the following CLI to get the stats for all the protocols:

  show IP NBAR protocol-discovery

  Workaround 2: Perform a snmpget against objects in cnpdAllStatsTable.

- CSCty61216

  Symptoms: CCSIP_SPI_Control causes leak with a Cisco AS5350.

  Conditions: This 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 the gateway (ISDN PRI --> AS5350 --> SIP --> Provider SIP gateway).

Workaround: There is no 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: This symptom is observed when CEF is enabled.

  Workaround: Disable CEF.

- 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: This symptom is observed when an HTTP packet with the “HttpOnly” field set is received.

  Workaround: There is no workaround.

- CSCtz23020

  Symptoms: The EZVPN client running a Cisco IOS Release 15.x code shows a corrupted ISAKMP lifetime value due to which the rekey is not triggered and can cause an outage.

  Conditions: This symptom is observed when IKE uses certificate-based authentication.

  Workaround: Use pre-shared keys.

- CSCtz33622

  Symptoms: Multiple crashes on a Cisco ISR that is running latest IOS versions with x25 encapsulation due to managed timer corruption.

  Conditions: This symptom is observed on a Cisco ISR using x25 routing.

  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

- CSCtz40460

  Symptoms: A router running Cisco IOS may crash or hang.

  Conditions: This symptom may be seen when SSLVPN is configured with NTLM authentication. NTLM authentication is configured by default.

Workaround: There is no workaround.

- CSCtz47595

  Symptoms: Dial string sends digits at incorrect times.

  Conditions: This symptom is 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 2 seconds, three commas = 3 seconds, and so on.

  - 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, that is: 919195551212x,22 or 1212x,,,22.
  - With no comma in the dial string, the digits are sent immediately after being generated without waiting for a connection, that is: 919195551212x22.

  Dialing directly to a number with no extension or extra digits works as expected.

  Workaround: There is no workaround.

- 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.

- 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 symptom can be seen on distributed platforms running Cisco IOS Release 12.4T or a later code.

  Workaround: Use Cisco IOS 12.4 mainline code, such as Cisco IOS Release 12.4(25f), which is not susceptible.

- 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.

Workaround: Hard clear.

- CSCtz78943

  Symptoms: A Cisco router experiences a spurious access or a crash. Cisco ISR-G1 routers such as 1800/2800/3800 experience a spurious access. Cisco 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.

- 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.

- 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:

  – The ACL definition should have service OG ACE.
  – Reconfigure the service OG ACE or delete it.
  – 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 a configuration change is needed.

  Workaround 2: Remove ACL checks on the interface when changing the configuration (“no ip access-group”).

- 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: This symptom occurs 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.

- 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: This symptom can occur in the following situations:

  - CUBE receives 180 ringing with SDP session.
  - "media transcoder high-density" is enabled.

  Workaround: Disable "media transcoder high-density".

- CSCua19294

  Symptoms: IPSLA intermittently reports wrong minimum RTT of 1 millisecond or below.

  Conditions: This symptom is observed on microsecond precision setting sending multiple number-packets at 100msec intervals.

  Workaround: There is no workaround.

- CSCua24689

  Symptoms: Fragments are sent without label resulting in packet drops on the other side.

  Conditions: This symptom is observed under the following conditions:

  - MPLS enabled DMVPN tunnel on egress.
  - VFR on ingress.

  Workaround: Disable VFR if possible.

- 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, the following traceback is seen:

```
%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: This symptom is observed with Cisco IOS Release 15.1(3)T and Cisco IOS Release 15.1(4)M4 after reload. The issue does not occur in Cisco IOS Release 12.4(24)T6 or earlier releases.

Workaround: Reapply the configuration after the router comes back up.

- CSCua40273

  Symptoms: The Cisco ASR 1000 router crashes when displaying MPLS VPN MIB information.

  Conditions: This symptom occurs on the the Cisco ASR 1000 with Cisco IOS Release 15.1(02)S software.

  Workaround: Avoid changing the VRF while querying for MIB information.

- CSCua50697

  Symptoms: After unplugging and reconnecting a T1 cable, the T1 controller remains down or reports 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
  – GRWIC-xCE1T1-PRI

  The T1 signal must also be 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 **show memory debug leaks** command 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.

- CSCua55785

  Symptoms: Build breakage due to the fix of CSCtx34823.

  Conditions: This symptom occurs with the 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 the device is reloaded, the device will not fully boot until the configurations are bypassed.

  Conditions: This symptom occurs after the **privilege exec level 0 show glbp brief** command is entered and saved.

  Workaround: Reload the router before saving the configurations.

- CSCua61201

  Symptoms: Unexpected reload with BFD configured.

  Conditions: This symptom occurs when a device is configured with BFD.

  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.

- 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.

- 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 the startup-configuration.

- 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.

- CSCub13317

  Symptoms: The Cisco 2900 with VWIC2-2MFT-T1/E1 in TDM/HDLC mode does not forward any traffic across the serial interface after a certain amount of time.

  Conditions: This symptom occurs when you 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

- CSCub18682

  Symptoms: The phone number is missing in the Sent INVITE from CUBE when testing OutBound Dial-Peer Matching using the phone number and context under destination-uri.

  Conditions: This symptom occurs when running Cisco IOS Release 15.2(2)T1.12.

  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.

- CSCub41748

  Symptoms: The router displays high CPU usage due to NBAR.

  Conditions: This symptom occurs due to RTP traffic.

  Workaround: Replace “protocol rtp” with ACL in match statement.

- CSCub45303

  Symptoms: H323 to SIP interworking calls fail.

  Conditions: This symptom is observed with the following topology:

  ```
  callgen----ogw------cube1------cube2-----tgw----callgen
  ```

  The following call combinations fail:

  HHHS,HSSH,SHHS,HSSS.

  Workaround:

  1. Configure voice CLIs on the router.
  2. Save the configurations.
  3. Reload the router and rerun the calls.

- 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

  Symptoms: Spurious errors are observed on the Cisco AS5400.

  Conditions: This symptom is observed on the Cisco AS5400.

  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.

- 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 *”.

- CSCub80491

  Symptoms: A Cisco router may experience alignment errors. These alignment errors may then cause high CPU.

  Conditions: This symptom occurs as the alignment errors require using Get VPN. It is currently believed to be related to having the Get VPN running on a multilink interface, but this is not yet confirmed.

  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.

- 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.

- CSCub91111

  Symptoms: Outgoing packet drop on the HSPA+R7 cellular interface with SWI MC8705 firmware T3.5.x (not released).

  Conditions: This 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.

- CSCub98623

  Symptoms: 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.

- 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.

- CSCuc12685

  Symptoms: Address Error exception is observed with ccTDUtilValidateDataInstance.

  Conditions: This symptom is observed with ccTDUtilValidateDataInstance.

  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 an 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.

- 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 Flexible NetFlow.

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

- 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: This symptom is observed when you configure the **bandwidth** command.

  Workaround: There is no workaround.

- CSCuc38253

  Symptoms: The Cisco C3900 router crashes due to “Unexpected exception to CPU: vector 1400”.

  Conditions: The exact conditions are still being investigated.

  Workaround: There is no workaround.

- CSCuc39963

  Symptoms: Spurious memory access/crash is seen at mdb_tree_classify.

  Conditions: This symptom occurs when the egress QoS policy is configured.

  Workaround: There is no workaround.

- CSCuc42518

  Symptoms: Cisco IOS Unified Border Element (CUBE) contains a vulnerability that allows 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: This symptom occurs when Cisco IOS CUBE may experience an input queue wedge condition on an interface configured for media negotiation using SIP when a 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

- CSCuc42558

  Symptoms: A Cisco router configured as the VXML gateway may experience a leak in the processor memory pool in CCSIP_SPI_CONTROL in the function url_parseTelUrl.

  Conditions: This symptom occurs when a Cisco router is configured as the VXML gateway. There could be other triggers as well.

  Workaround: Reload the router during a maintenance window to avoid an unexpected crash. You may also downgrade to Cisco IOS Release 15.1(4)M3, which is not affected.

- CSCuc47675

  Symptoms: Traffic blackhole when a single pair of 4-wire EFM bond connection is down on a Cisco 888E router.

  Conditions: This 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 symptom occurs 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.

- CSCuc59541

  Symptoms: Spoke fails to learn networks behind other spokes and EIGRP flapping occurs.

Conditions: This symptom is observed with a FlexVPN spoke-to-spoke setup.

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.

- CSCuc70472

  Symptoms: 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.

- 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.

- CSCuc91717

  Symptoms: The router crashes when making a basic x25 configuration change.

  Conditions: This symptom occurs when you remove the x25 translation statement from the running configuration when traffic is on.

  Workaround: Shut the interface before making the x25 configuration change.

- CSCud01502

  Symptoms: A crash occurs in CME while accessing a stream in sipSPIDtmfRelaySipNotifyConfigd.

  Conditions: This symptom occurs in CME.

  Workaround: There is no workaround.

- CSCud05636

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

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

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

- 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.

- CSCud22148

  Symptoms: The E1 (E&M) controller is down.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M2 or later releases. This issue is seen with the Cisco 3945.

  Workaround: There is no workaround.

- 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.

- CSCud46314

  Symptoms: The Cisco router crashes when polling ciscoEnvMonSupplyStatusDescr MIB.

  Conditions: This symptom is observed when 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.

- CSCud86954

  Symptoms: 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.

Workaround: 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.

Resolved Caveats—Cisco IOS Release 15.1(4)M5

Cisco IOS Release 15.1(4)M5 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M5 but may be open in previous Cisco IOS releases.

- CSCsg36725

  Symptoms: A memory leak and memory exhaustion may occur when QoS policies are updated on 40,000 sessions.

  Conditions: This symptom is observed on a Cisco 10000 series router, but may also affect other platforms.

  Workaround: There is no workaround.

- CSCth20872

  Symptoms: The following error message is seen accompanied by a reset of the Fast Ethernet:

  ```
  %C870_FE-3-TXERR: FastEthernet0: Fatal transmit error. Restarting...
  ```

  Conditions: This symptom is observed on a Cisco 877 router that is running Cisco OS Release 12.4(24)T3.

  Workaround: There is no workaround.

- CSCth43911

  Symptoms: The system may crash when performing the SNMP SET operation for CISCO-CALLHOME-MIB objects in callHomeDestEmailAddressTable, ccmSeverityAlertGrouptable, ccmPeriodicAlertGroupTable, ccmPatternAlertGroupTable, ccmEventAlertGroupTable, and ccmDestProfileTestTable.

  Conditions: This symptom does not occur under any specific conditions.

  Workaround: There is no workaround. The fix exists in Cisco IOS Release 12.2(33)SXJ and Cisco IOS Release 12.2(50)SY.

- CSCth56654

  Symptoms: When making calls in a CVP solution environment, the call is not established.

  Conditions: This symptom is observed when CUBE is enabled with the “connection-reuse” CLI, which supersedes handling of the VIA header for SIP response messages.

  Workaround: Disable the “connection-reuse” CLI.

- CSCth92828

  Symptoms: When viewing a device configuration, such as via a URL like https://tools.cisco.com/sch/reports/viewDeviceConfiguration.do<specific_item_quer y>, the TACACS server key, a type 7 reversible password, is still visible.

  Conditions: This symptom is observed when viewing a device configuration.

  Workaround: There is no workaround.

- CSCti87194

  Symptoms: The last fragment causes a crash because of an invalid zone value.

  Conditions: This symptom occurs when a Big IPC message is fragmented. Then, the last fragment causes the crash because of an invalid zone value.

  Workaround: There is no workaround.

- CSCtj10515

  Symptoms: A crash is seen in the IGMP input process.

  Conditions: This symptom is observed in a multi-VRF scenario with extranet MVPN.

  Workaround: There is no workaround.

- CSCtj14921

  Symptoms: Memory leak is seen in the crypto SS process.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M2.

  Workaround: If possible, reload the router periodically.

- 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 is enabled and sessions get DHCP information from a RADIUS server.

  Workaround: There is no workaround.

  Further Problem Description: This fix needs to be included in the Cisco ME 3400.

- 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: This symptom is observed on a Cisco 1803 that is running Cisco IOS Release 12.4(15)T12 or Cisco IOS Release 12.4(15)T14.

  Workaround: Remove CEF.

- CSCtl73132

  Symptoms: The router may crash and reset when the **show ipc hog-info** command or the **show tech-support ipc** command is run repetitively on either the switch processor or route processor.

  Conditions: The issue can be seen when when the **show ipc hog-info** command or the **show tech-support ipc** command is run repetitively on either the switch processor or route processor.

  Workaround: Do not use the **show ipc hog-info** command or the **show tech-support ipc** command.

- CSCtn55070

  Symptoms: Call-home http messages can hang and not be sent out.

  Conditions: This symptom is observed when call home is enabled and an http transport method is used. This symptom is timing-dependent and cannot be hit every time. In addition, this symptom is observed in telnet sessions.

  Workaround: Log in to the console port if a telnet session was used to send call-home http messages. Because the console is waiting on user-supplied information (--More--), enter something into the console; the call-home process can then continue to execute.

- CSCto09059

  Symptoms: CPUHOG at IPC Check Queue Time Process results in IOSD crash.

  Conditions: This symptom occurs with multiple RP switchovers with ISG PPPoE sessions.

  Workaround: There is no workaround.

- CSCto71671

  Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

  Workaround: There is no workaround.

- CSCtq21258

  Symptoms: When a user uses a password larger than 32 bytes in size, the authentication for COA will pass if the password matches the settings on the RADIUS server. When this password is reduced in size to exactly 32 bytes, including the setting on the RADIUS server, the authentication for the COA will fail as the ISG appends excess data to the password sent to the RADIUS for authentication.

  Conditions: This symptom is seen when the user password is larger then 32 bytes and is being reduced to exactly 32 bytes.

  Workaround: Do not use 32 bytes as the size for the user password. In case the error occurs, the only method to solve the issue is to reload the device.

- CSCtr87070

  Symptoms: Enable login fails with the error “% Error in authentication”.

  Conditions: This symptom is observed with TACACS single-connection.

  Workaround: Remove TACACS single-connection.

- CSCts03251

  Symptoms: A Cisco 2921 router running Cisco IOS Release 15.1(4)M with the “logging persistent” feature configured may crash.

  Conditions: This symptom is observed with the “logging persistent” feature.

  Workaround: Disable the “logging persistent” feature.

- CSCts32708

  Symptoms: Similar to CSCth80642, the Cisco IOS SSLVPN router fails to accept new sessions. Users will not be able to load the WebVPN login page. If debug sdps is enabled, the following error message may be displayed:

```
Sev 4:sdps_get_pak_from_tcp(),line 1080:tcp_getpacket returned error 2, tcb=0x6A9EFFEC
```

Conditions: This symptom occurs when the router remains reachable; otherwise, (that is, you can ping the WebVPN IP) the SSL process is running and listening on the right port. The **show tcp tcb** and **show tcp brief all numeric** command output 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: \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

- CSCts33018

  Symptoms: The Cisco UC500 crashes at Dot11 subsystem after being upgraded from SWP 8.1.0 (15.1(2)T2) to SWP 8.2.0 (15.1(2)T4)

  Conditions: This symptom is observed when a Cisco 2900 PoE switch is connected to the Cisco UC540 with Cisco phones and an iMac is connected to the switch. An Apple laptop is also connected using wireless.

  Workaround: There is no workaround.

- CSCts56044

  Symptoms: A Cisco router crashes while executing a complex command. For example:

  ```
  show flow monitor access_v4_in cache aggregate
  ipv4 precedence sort highest ipv4 precedence top 1000
  ```

  Conditions: This symptom is observed while executing the **show flow monitor top** top-talkers command.

  Workaround: Do not execute complex flow monitor top-talkers commands.

- CSCts68626

  Symptoms: PPPoE discovery packets causes packet drop.

  Conditions: This symptom is observed when you bring up a PPPoE session and then clear the session.

  Workaround: There is no workaround.

- CSCts69204

  Symptoms: PPPoE sessions do not get recreated on the standby RP.

  Conditions: This symptom occurs on the standby RP.

  Workaround: There is no workaround.

- CSCts72911

  Symptoms: In case of a GR/NSF peering, after an SSO, the restarting router (PE, in this case) does not advertise RT constrain filters to the nonrestarting peer (RR, in this case).

Conditions: This symptom is observed after an SSO 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.

- 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

- 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: The conditions are not known at this time.

  Workaround: There is no workaround.

- CSCtt26692

  Symptoms: The 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: This symptom occurs when the 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.

- CSCtt61762

  Symptoms: IPv6 hosts connected to EHWIC-*ESG Layer 2 ports are not able to communicate to each other locally (at Layer 2).

  Conditions: This symptom was first noticed on a Cisco ISR G2 with EHWIC-*ESG and directly connected IPv6.

  Workaround: There is no workaround.

- CSCtv36812

  Symptoms: Incorrect crashInfo file name is displayed during crash.

  Conditions: This symptom is observed whenever a crash occurs.

  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.

- CSCtw46229

  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.

  Conditions: This symptom is observed with PPP negotiations and the session involving PPPoA.

  Workaround: Ensure all your PPP connections stay stable.

- CSCtw61872

  Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.

  Conditions: This 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.

- CSCtw87132

  Symptoms: A Cisco router may crash when clearing a TCP session:

  ```
  router120#clear tcp tcb 08C5F4F8 [confirm]
  SIGBUS (0xFF1BD460) : Bus Error ( [0xD0D0D39] invalid address alignment)
  ```

  Conditions: This has been experienced on a Cisco 2921 router that is running Cisco IOS Release 15.1(4)M through to Cisco IOS Release 15.1(4)M3.

  Workaround: There is no workaround.

- CSCtx06018

  Symptoms: Interface queue wedge is seen when performing the WAAS performance test.

  Conditions: This symptom is observed when performing the WAAS performance test.

  Workaround: Increase the interface input queue hold size.

- CSCtx22322

  Symptoms: If an over-temperature interrupt occurs when the CPU utilization is high, the system may crash.

  Conditions: This symptom is observed when CPU utilization of the system is high in Cisco 880 series routers.

  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.

- 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: This symptom is observed with the following conditions:

  - “ppp lcp delay 0” is configured.
  - Cisco IOS Release 15.0(1)M5.

  Workaround: Set delay timer without 0.

- CSCtx71185

  Symptoms: The router crashes due to corrupted program counter.

  Conditions: This symptom is observed with packets being switched across the dialer interface.

  Workaround: There is no workaround.

- CSCtx74342

  Symptoms: After the 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: This 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

- 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.

- CSCtx92802

  Symptoms: IP fragmented traffic destined for crypto tunnel is dropped.

  Conditions: This 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.

- CSCtx95840

  Symptoms: A Cisco voice gateway may unexpectedly reload.

  Conditions: This 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.

- 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.

- 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.

- 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.

- CSCty32232

  Symptoms: BRI interface is not showing as monitored.

  Conditions: This symptomoccurs after performing an on-line insertion/removal of an NM-16ESW module.

  Workaround: Reload the router.

- CSCty33945

  Symptoms: When a SIP gateway tears down video and later sets it up again after a midcall invite for the same call, it reuses the same source RTP port as before. Unfortunately, it does not check if this RTP port is in use for a different call, and therefore crosstalk can occur.

  ```
  4310820: Feb 27 17:56:08.910: //3017060/BF76175BB294/SIP/Media/sipSPIAddStream:
  Reusing old src_port(16384)
  ```

  Conditions: This symptom is observed when a SIP gateway tears down video and later sets it up again after a midcall invite for the same call.

  Workaround: There is no workaround.

- CSCty34020

  Symptoms: A Cisco 7201 router's GigabitEthernet0/3 port may randomly stop forwarding traffic.

  Conditions: This symptom only occurs on Gig0/3 and possibly Fa0/0 as both are based on different hardware separate from the first three built-in gig ports.

  Workaround: Use ports Gig0/0-Gig 0/2.

- 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/cat6K
819H
ISR G2 routers with ISM IPSec VPN accelerator
```

Workaround: There is no workaround.

- CSCty43587

  Symptoms: A crash is observed with memory corruption similar to the following:

  ```
  %SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
  dealloc XXXXXXXX
  ```

  Conditions: This symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.

  Workaround: There is no workaround.

- 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.

- CSCty54718

  Symptoms: A Cisco 3945 router crashes with configuration greater than 40k DN numbers of SAF/EIGRP.

  Conditions: This symptom is seen with the reset of CUCM several times. The router crashes, and a memory leak is seen.

  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.

- CSCty64721

  Symptoms: Improper memory allocation by CTI process crashes the CME.

  Conditions: This symptom occurs when 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.

- CSCty65189

  Symptoms: Incoming register packets are dropped at the RP when zone-based firewall (ZBFW) is configured on the RP.

  Conditions: This symptom is observed when ZBFW is configured.

  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.

- CSCty80074

  Symptoms: A Cisco 3800 router running Cisco IOS Release 15.0(1)m7, with only Multilink or Serials, shows aborts and input errors during normal traffic conditions.

  Conditions: This symptom is observed with normal traffic load. In addition, when a ping sweep is done, aborts and input errors are seen more frequently.

  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.

- CSCty84512

  Symptoms: All Wi-Fi phones are stuck in “Connecting...”.

Conditions: This symptom is observed with Wi-Fi phones connected to Cisco UC540W/UC520W AP.

Workaround: Power cycle the phone.

- 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.

- CSCty90293

  Symptoms: Processing improvements for GREv6 over IPv6 currenlty require IP CEFv6 to be disabled.

  Conditions: This symptom is observed with GREv6 over IPv6.

  Workaround: Use “tunnel protection” instead.

- 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: This symptom is an extreme corner case/timing issue. This issue has been observed only once on a release image.

  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty97255

  Symptoms: High CPU is seen under “rf task” after a reload or an upgrade.

  Conditions: This symptom is observed on Cisco ISR routers configured with “crypto map redundancy”.

  Workaround: Remove “crypto map redundancy”.

- CSCtz13818

  Symptoms: In a rare situation when route-map (export-map) is updated, Cisco IOS is not sending refreshed updates to the peer.

  Conditions: This symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then, Cisco 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.

- CSCtz27137

  Symptoms: An upgrade to the S639 or later 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.

- CSCtz41130

  Symptoms: The build failed for the Cisco 7200 platform after committing changes for CSCtj14921 to the v151_4_m_throttle.

  Conditions: This symptom occurs when monolith changes are not committed.

  Workaround: Commit the monolith changes to the v151_4_m_throttle.

- 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: This symptom is observed with IPv6 link-local next-hop. When the EIGRP route is redistributed to BGP VRF, it clears the next-hop 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.

- CSCtz48615

  Symptoms: AES encryption may cause high CPU utilization at crypto engine process.

  Conditions: This 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.

- 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.

- 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.

- 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: This symptom is timing-dependent; therefore, the problem is not systematic.

  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.

- CSCua06598

  Symptoms: The router may crash with breakpoint exception.

  Conditions: This 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.

- 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: This symptom was first seen in Cisco IOS Release 15.1(4)M4, but it has also been found to be in Cisco IOS Release 15.2(3)T.

  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: This symptom is observed on a Cisco ISR G2.

  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?action=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.

- 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.

- CSCtw58664

  Symptoms: SSL VPN for SCCP causes a crash when clearing a WebVPN session.

  Conditions: This 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.

- CSCtu29881

  Symptoms: A router may crash while using double authentication for IPsec (ESP + AH) and certain types of traffic. The following message is seen in the crashinfo file:

  ```
  validblock_diagnose, code = 1

  current memory block, bp = 0xZZZZZZZZ,
  memorypool type is I/O
  data check, ptr = 0xZZZZZZZZ

  next memory block, bp = 0xZZZZZZZZ,
  memorypool type is I/O
  ```

```
data check, ptr = 0xZZZZZZZ

previous memory block, bp = 0xZZZZZZZZ,
memorypool type is I/O
data check, ptr = 0xZZZZZZZZ
```

The router crashes due to I/O memory corruption - block overrun.

Conditions: This symptom is observed with double authentication (AH + ESP) and certain type of packets.

Workaround 1: Do not use double authentication (AH + ESP). Use ESP instead.

Workaround 2: Use an IOS version that does not have the fix for CSCtc40806.

- CSCtk74632

  Symptoms: In some rare scenarios, closed IPC connections may be still detected as active, and cause some IPC message pass to fail.

  Conditions: This symptom is observed in rare scenarios in which IPC connections are being set up and torn down frequently.

  Workaround: There is no workaround.

- 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.

- CSCty54695

  Symptoms: RRI routes are missing when IPsec SA is up after peer IP change.

  Conditions: This symptom is observed under the following conditions:

  - Cisco ASR 1002 router running Cisco IOS XE Release 3.4.2S.
  - Dynamic crypto map with RRI.
  - Peer changes the IP address frequently.

  Workaround: Clear the crypto session with the peer.

- CSCty97961

  Symptoms: A device configured with SSLVPN crashes.

  Conditions: This symptom is observed when a device configured is with SSLVPN and **functions svc-enabled** or **functions svc-required** and **svc dtls**, and has an outbound ACL on one of the device's interface.

  This vulnerability has only been observed when the outbound ACL is tied to either a NAT or ZBFW interface in the outbound direction and is not the interface that the SSLVPN session is terminated against.

  This vulnerability has only been observed when the SSLVPN sessions terminate over PPP over ATM interface.

  This vulnerability was not able to be reproduced over SSLVPN sessions terminating over Ethernet or Serial interfaces.

  Workaround: Remove the outbound ACL, or **no svc dtls** if running Cisco IOS software that has a fix for CSCte41827.

- CSCty99846

  Symptoms: Cisco IOS software includes a version of OpenSSL that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

  CVE-2009-1386

  This bug was opened to address the potential impact on this product.

  Conditions: This symptom is observed when a device is configured with SSLVPN and **svc dtls**.

  Workaround: Disable DTSL with **no svc dtls**.

  Further Problem Description: This problem would only be seen in Cisco IOS when using Anyconnect client with Cisco IOS SSLVPNs, after the initial session has been authenticated and established. Exploitation would result in Cisco IOS reloading.

  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 6.3/5.2:

  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:F/RL:OF/RC:C

  CVE ID CVE-2009-1386 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

- CSCua31157

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

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

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

  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.

- CSCub39997

  Symptoms: SIP TNP phones failed to register with CME.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M4.14.

  Workaround: There is no known 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.

- CSCtl05570

  Symptoms: SNMP does not work on the ppc/mips/x86 PI image.

  Conditions: This symptom does not occur every time. When this issue is seen, SNMP will stop working even after reload/power cycle of the router.

  Workaround: The only way to make SNMP work again is manually start [nova-k5-7:~]$ /usr/binos/bin/snmp_subagent.

Resolved Caveats—Cisco IOS Release 15.1(4)M4

Cisco IOS Release 15.1(4)M4 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M4 but may be open in previous Cisco IOS releases.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, 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.

- CSCtl53576

  Symptoms: A Cisco router freezes while executing the **show run** command.

  Conditions: This symptom is observed if “auto ip sla schedule” is configured on the router.

  Workaround: There is no workaround.

- CSCtn07696

  Symptoms: The Cisco 6506-E/SUP720 may crash while redirecting the **show tech-support** command output using the **ftp** command due to TCP-2-INVALIDTCB.

  Conditions: This symptom is observed with the following CLI:

  ```
  show tech-support | redirect
  ftp://cisco:cisco@10.0.255.14/Cisco/tech-support_swan21.pl.txt
  ```

  During the FTP operation, if the interface fails or shuts down, it could trigger this crash.

Workaround: This is an FTP-specific issue. Redirect the output by TFTP or other protocols.

- CSCtn36227

  Symptoms: Alignment errors or ‘C’ response may occur in response to IPv6 pings.

  Conditions: These symptoms may be observed while sending an IPv6 ping.

  Workaround: There is no workaround.

- CSCtn56006

  Symptoms: The SNMP value is not matching with the output value of the **show** command.

  Conditions: This symptom is observed under no specific condition.

  Workaround: There is no workaround.

- CSCtn65116

  Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.

  Conditions: The symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Cisco IOS Release 12.2(33)SRB or later. Earlier versions are not affected. This occurs with the same prefixes with different mask lengths, e.g.: 10.0.0.0/24 and 10.0.0.0/26 (but not for 10.0.0.0/24 and 10.0.0.1/32, because 10.0.0.0 is not the same prefix as 10.0.0.1). It is seen with the following process:

  1. Assume the prefix, 10.0.0.0/24, is imported from VPNv4 to VRF. It has been allocated a label of 16.
  2. The allocated label changes from 16 to 17, e.g.: due to interface flapping or BGP attribute change.
  3. However, before the BGP import happens, a more specific prefix (e.g.: 10.0.0.0/26) is added to the BGP radix tree, but it is denied for importing due to, say, RT policy.

  Workaround: Remove RT or import map and add it back. Note, however, that if the above conditions occur again, the issue could reappear.

- CSCto59459

  Symptoms: Connections that are optimized by WAAS are reset. Malformed TCP options are added to the packet that is created and sent by WAAS-Express over the WAN, causing the peer WAE to reset connections.

  Conditions: Any TCP connection will suffer from this defect.

  Workaround: There is no workaround.

- CSCto90912

  Symptoms: A crash is seen with the DHCPv6 client process.

  Conditions: The symptom is observed when **ipv6 address dhcp** is run on an “auto-template” interface, and then the interface is removed with a **no int auto-temp**.

  Workaround: There is no workaround.

- CSCto93880

  Symptoms: Enable authentication fails when user is configured with TACACS server group.

  Conditions: This symptom occurs when TACACS server is configured with user defined group and configured for enable authentication. User is unable to authenticate when he tries to switch to privilege executive mode (enable) and gets the following error that indicates that there is no address for defined servers.

```
%TAC+: no address for get_server
%TAC+: no address for get_server
```

Workaround: Configure the TACACS server group with the default group name.

- CSCtq59923

  Symptoms: OSPF routes in RIB point to an interface that is down/down.

  Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

  Workaround: Configure the **ip routing protocol purge interface** command.

- CSCtq74389

  Symptoms: While using a Switch Virtual Interface (SVI) as a Layer 2 Tunnel Protocol Version 3 (L2TPv3) termination, the SVI interface floods an unknown unicast packet unexpectedly.

  Conditions: This symptom is observed while using an SVI interface as an L2TPv3 termination.

  Workaround: Use a routed port instead of an SVI.

- CSCtq77024

  Symptoms: Metrics collection fails on hop0 if route change event occurs.

  Conditions: This symptom is observed when the mediatrace is not passing up an interface type that is acceptable to DVMC when a route change occurs on the node which has the initiator and responder enabled.

  Workaround 1: Remove and reschedule mediatrace session.

  Workaround 2: Remove and reconfigure mediatrace responder.

- CSCtq92650

  Symptoms: DMVPN tunnel is not selecting the right source interface.

  Conditions: The symptom is observed when multi-link frame relay creates more than one sub-interface with the same name.

  Workaround: There is no workaround.

  Further Problem Description: This bug resolves the issue reported in CSCth08338 for Cisco IOS Release 15.1M.

- CSCtr18985

  Symptoms: The CEF adjacency for a Frame Relay point-to-point circuit is incomplete causing the traffic passing through the Cisco router to drop.

  Conditions: This symptom is observed after the Cisco router reloads.

  Workaround 1: Flap the Serial interface.

  Workaround 2: Disable CEF either on the serial interface or globally.

- CSCtr25734

  Symptoms: A router crashes.

  Conditions: This symptom is observed when the router is reloaded with a BRI interface brought up in startup configuration.

  Workaround: There is no workaround.

- CSCtr86077

  Symptoms: MGCP call drops 10 seconds after IP phone puts call on hold.

  Conditions: The symptom is observed under the following conditions:

  - IP phone -- CUCM -- MGCP -- GW -- PRI.
  - **mgcp rtp unreachable timeout** *10000* is configured on gateway.
  - **no MOH** is configured for the IP phone so Tone on Hold (TOH) is used.
  - IP phone make calls to PSTN and is answered.
  - IP phone puts call on hold.
  - PSTN user hears TOH.
  - 10 seconds after hold is initiated, the call is dropped.

  Workaround: Remove **mgcp rtp unreachable timeout** from the MGCP gateway.

- CSCtr86149

  Symptoms: A router crashes if placing a call from an ISDN phone to an IP phone. The call is a secure SIP call (TLS); the phone is also using secure SCCP.

  Conditions: The router is in secure SRST mode due to a WAN outage.

  Workaround: There is no workaround.

- CSCtr88739

  Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

  Symptom 2: The routes in BGP may not get installed to RIB.

  Conditions: The symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

  For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

  For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

  Workaround for symptom 1: Remove **import-route target** and reconfigure route-target.

  Workaround for symptom 2: Clear **ip route** *x.x.x.x* to resolve the issue.

- CSCts46578

  Symptoms: Firewall may drop a packet with log similar to:

  ```
  %FW-6-DROP_PKT: Dropping ftp-data session 10.7.7.99:1449 10.7.8.100:20  due
  to  Invalid Seq# with ip ident 6621 tcpflags 0x8018 seq.no 3558493868 ack
  1386495675
  ```

  Retransmitted packet is allowed through.

  Conditions: CBAC configured.

  Workaround: There is no workaround.

- CSCts67465

  Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.

  Conditions: The symptom is observed always, if the standby is configured as an SSO.

  Workaround: Remove enhanced history interval configuration before resetting the frequency.

- CSCts70790

  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via **neighbor default-originate** to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

  Workaround: Remove and re-add the **neighbor default-originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCtt05910

  Symptoms: Router crashes.

  Conditions: The symptom is observed when running the **show sum** command. It is seen with the Cisco 3900e platform.

  Workaround: Do not use the **show sum** command.

- CSCtt16051

  Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall

- CSCtt17879

  Symptoms: The **bgp network backdoor** command does not have any effect.

  Conditions: This symptom occurs:

  - On 64-bit platform systems.
  - When the network is learned after the backdoor has been configured.

  Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt21228

  Symptoms: Router crashes while trying to configure Tcl script via SSH connection.

  Conditions: SSH to the router and then try to configure Tcl script.

  Workaround: There is no workaround.

- CSCtt26721

  Symptoms: A Cisco router may see increased CPU utilization when NBAR is used.

Conditions: This has been experienced on a Cisco 3925 router running Cisco IOS Release 15.1(3)T2.

Workaround: There is no workaround.

- CSCtt43552

  Symptoms: A Cisco router reloads with the **warm-reboot** command.

  Conditions: This symptom is observed on the Cisco router while running Cisco IOS Release 15.2(2.2)T.

  Workaround: There is no workaround. Remove warm-reboot from configuration (router will not be able to use the warm reboot feature).

- CSCtu00488

  Symptoms: The traffic stops in the transmit direction of GE0 (configured as WAN) interface for traffic coming from FE8 (configured as LAN) interface.

  Conditions: This symptom is observed when **batch** commands are configured on GE0 and FA8 interfaces.

  Workaround: Do not use **batch** commands as they are intended for performance improvement in the case of higher cache misses.

- CSCtu02542

  Symptoms: T.38 OnRamp consistently fails for every call with the following error:

  ```
  %LAPP_ON_MSGS-6-LAPP_ON_CAUSE_NO_MEMORY: No memory available
  ```

  The debugs indicate negative free process memory while displaying the following message:

  ```
  %LAPP_ON_MSGS-6-LAPP_ON_CAUSE_NO_MEMORY: No memory available
  //1093/4DE38C71808E/FOIP_ON/lapp_on_call_handoff:
     SOFTWARE_ERROR; Not enough memory; Free Process Memory Bytes=-1922868956
  ```

  However, while monitoring memory, no issues appear with the available memory resources:

  ```
  Router#show memory stat
                  Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
  Processor   2AC0BEE0   2436776224    59890020   2376886204   2113970464 1034143696
        I/O    C000000    67108864    20001528    47107336    46989820 46943484
  ```

  Conditions: The conditions under which these symptoms are observed are unknown.

  Workaround: Apply a logging buffer large enough to bring the free memory below 2147483648 (b). For example, **logging buffered** *500000000*.

- CSCtu02833

  Symptoms: ISR G2 with IVR crashes due to bus error exception.

  Conditions: The symptom is observed with a Cisco ISR G2 that is running Cisco IOS Release 15.1(1)T2.

  Workaround: There is no workaround.

- CSCtu57226

  Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.

  Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.

  An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

- CSCtu06894

  Symptoms: Cisco UBE crashes when the **show sip-ua calls** command is executed while there is an active SIP call through system.

  Conditions: This symptom is present on Cisco 2821 routers. The router crashes only when Cisco UBE receives an SDP length greater than 9000 bytes as part of a SIP message. And at the same time, if the show command is executed, the crash occurs. Otherwise, the crash is not seen.

  Workaround: There is no workaround.

- CSCtu08717

  Symptoms: A Cisco router experiences a watchdog timeout while executing tw_timer_replenish.

  Conditions: This symptom is observed on the Cisco router if the IP SLA and Performance Agent features are configured on it. This timeout may also be observed if traffic is sent for a long time through a router configured with these features.

  Workaround: There is no workaround.

- CSCtu11140

  Symptoms: When there is no reachability cache on a DLSw router, the DLSw router sends CUR_EX unexpectedly if receiving XID_F.

  Conditions: The symptom is observed if a DLSw router receives XID_F when there is no reachability cache.

  Workaround: There is no workaround.

- CSCtu11677

  Symptoms: A Cisco router may unexpectedly reload due to bus error or segV exception or generate a spurious error when the *cSipStatsSuccessOkTable snmp* object is polled.

  Conditions: This is seen on a voice gateway when the cSipStatsSuccessOkTable snmp object is polled.

  Workaround: Create an SNMP view and then block the oid for cSipStatsSuccessOkTable and then apply it to all SNMP communities on the device:

  ```
  snmp-server view blockmib iso include
  snmp-server view blockmib 1.3.6.1.4.1.9.9.152.1.2.2.5 exclude
  ```

and then apply it to the community:

```
snmp-server community <community> view blockmib ro
```

- CSCtu12445

  Symptoms: Traffic breaks off for a long time even though STP topology is converged on a Cisco 2921 router.

  Conditions: There are two Ethernet links between two Cisco 2921 routers, one is a forwarding link, and the other one is a blocking link. This symptom is observed when the forwarding link is broken, and the blocking link takes over as the forwarding link. This causes a break in traffic.

  Workaround: There is no workaround.

- CSCtu16433

  Symptoms: A Cisco 3725 running Cisco IOS Release 12.4(15)T may crash in GETVPN with the following bus error. It appears to crash just after registration:

  ```
  %GDOI-5-GM_REGS_COMPL: Registration to KS <snip> complete for
  group <snip> using address <snip>

  Address Error (load or instruction fetch) exception, CPU signal 10, PC =
  <snip>
  ```

  Conditions: The symptom is observed on Cisco IOS Release 12.4(15)T14.

  Workaround: There is no workaround.

- CSCtu17228

  Symptoms: DHCPv6 relay does not work on an EHWIC.

  Conditions: This symptom is observed when one of the following modules is used:

  - EHWIC-4ESG
  - EHWIC-4ESG-P
  - EHWIC-D-8ESG
  - EHWIC-D-8ESG-P

  Workaround: There is no workaround.

- CSCtu18786

  Symptoms: Device may crash showing “VOIP” error messages. Decodes point to voice functions.

  Conditions: The symptom is observed when SIP is enabled on the device.

  Workaround: There is no workaround.

- CSCtu21636

  Symptoms: Sometime calls are dropped if there are active calls on the DSP. The following errors are displayed in the logs:

  ```
  Power alarm on DSP channel ch=1 is ON
  0001 0001 **

  Power alarm on DSP channel ch=1 is OFF
  0001 0000 **
  ```

```
Power alarm on DSP channel ch=1 is ON
0001 0001 **

Power alarm on DSP channel ch=1 is OFF
0001 0000 **
```

Conditions: This symptom is seen with all conditions.

Workaround: There is no workaround.

- CSCtu21967

  Symptoms: A router configured to be an IP voice gateway may crash.

  Conditions: The exact conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtu29107

  Symptoms: While using the "Reuse MAC address" feature on an ATM RBE, the router uses the MAC address of the main interface rather than the configured MAC address of the subinterface.

  Conditions: This symptom is observed when ATM route bridge encapsulation is used with the "Reuse MAC address" feature.

  Workaround: There is no workaround.

- CSCtu36224

  Symptoms: A Cisco router reboots unexpectedly at intermittent intervals.

  Conditions: This symptom is observed on a Cisco router that is used for SSLVPN.

  Workaround: There is no workaround.

- CSCtv21900

  Symptoms: Intermittent one-way audio occurs from an MGCP gateway to a Cisco IP phone.

  Conditions: This symptom is observed under the following conditions:

  - Encrypted call with SRTP
  - MGCP Controlled Gateway
  - Cisco IOS Release 15.1(4)M or later releases

  Phone logs show the following message:

```
6622: DBG 23:29:50.256330 DSP: RTP RX: srtp_unprotect() again
6623: DBG 23:29:50.257139 DSP: RTP RX: srtp_unprotect() failed with error
code 7
6624: DBG 23:29:50.276390 DSP: RTP RX: srtp_unprotect() failed with auth func
3
```

  The "Rcvr Lost Packet" counter on the Cisco IP phone begins to increment as soon as the call connects.

  Workaround 1: Downgrade the software to Cisco IOS Release 15.1(3)T or earlier releases.

  Workaround 2: Perform a hold/resume on the one-way audio call. This mitigates the problem.

- CSCtw45055

  Symptoms: A Cisco ASR series router may experience a crash in the BGP Scheduler due to a segmentation fault if BGP dynamic neighbors have been recently deleted due to link flap. For example:

```
Nov 10 08:09:00.238: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
Nov 10 08:10:20.944: %BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold
time expired) x bytes
Nov 10 08:10:20.944: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification
received
Nov 10 08:10:20.945: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session  Neighbor deleted
Nov 10 08:10:34.328: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session  Neighbor deleted
Nov 10 08:10:51.816: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up

Exception to IOS Thread:
Frame pointer 0x3BE784F8, PC = 0x104109AC

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler
```

  The scheduler process will attempt to reference a freed data structure, causing the system to crash.

  Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

  Workaround: There is no workaround.

- CSCtw45592

  Symptoms: The **ntp server** *DNS-name* command is not synced to the standby device. When the **no ntp server** *hostname* command is issued later on the active device, the standby device reloads because the config was not added.

  Conditions: This symptom is observed when the device is reloaded or when the DNS name is not resolved. Due to this, the config is not added. After the standby SYNC failure, then issue the **no ntp server** *hostname* command.

  Workaround: Use IP/IPv6 addresses instead of the hostname for NTP configurations.

- CSCtw48553

  Symptoms: When MPLS-IP is configured on a Cisco router and QoS policy-map actions are applied, classification fails and packets are dropped. This prevents the committed information rate (CIR) from getting updated on the output interfaces.

  Conditions: This symptom is observed on any Cisco router that is running either Cisco IOS Release 15.0(1)M7.10 or later releases, or Cisco IOS Release 15.1(4) M2.5 or later releases.

  Workaround: There is no workaround.

- CSCtw56439

  Symptoms: The **ip mtu** command that is configured on an IPsec tunnel disappears after a router reload.

  Conditions: The symptom is observed with IPsec and the **ip mtu** over a tunnel interface.

Workaround: There is no workaround.

- CSCtw59086

  Symptoms: Unable to connect via Cisco AnyConnect or the WebVPN portal on a Cisco IOS router.

  The following message is seen in the Syslog:

  ```
  %SSLVPN-6-LICENSE_NO_FREE_COUNT: All avaiable SSLVPN session licenses are in use
  ```

  Conditions: This symptom is observed when the WebVPN License counter incorrectly reads 4294967295. Also, no connections are visible while executing the **show webvpn session context all** command.

  For example:

  ```
  sh webvpn session context all
  show webvpn license
    Max platform license count : 1500
    Available license count    : 100
    Reserved license count     : 100
  * In-use count               : 4294967295*
  ```

  Workaround: Reload the Cisco router.

- CSCtw62213

  Symptoms: When two Cisco 3945E routers are connected to each other and perform IPSLA operations, the responder experiences a drop in packets coinciding with the license update process.

  Conditions: This symptom is observed when two Cisco 3945E routers are connected back to back while performing IPSLA UDP-jitter operation.

  Workaround: Increase both the input queue length on the interface and the SPD queue length.

- CSCtw66863

  Symptoms: A Cisco router may crash when using VXML script with Cisco proprietary tag *Cisco-data*.

  Conditions: This symptom is observed when the *Cisco-data* tag uses memory beyond allocated memory, which causes the router to crash intermittently.

  Workaround: There is no workaround.

- CSCtw73544

  Symptoms: A leak is observed in the header pool with “ppp multilink”.

  Conditions: This symptom is observed with PPP over ATM.

  Workaround: There is no workaround.

- 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.

- CSCtw99290

  Symptoms: The source or destination group-address gets replaced by another valid group-address.

  Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

  Workaround: There is no workaround.

- CSCtx06747

  Symptoms: Device crashes at boot and never reaches CLI.

  Conditions: This symptom will happen even with no configuration. This issue is only seen with Cisco IOS Release 15.1(4)M3 due to a bad code fix integrated. The following platforms with k9 images are impacted by this bug: Cisco AS5300, Cisco AS5400, Cisco 7200, Cisco 7200p, Cisco 7301, Cisco VGD 1T3.

  Workaround: There is no workaround. Downgrade to Cisco IOS Release 15.1(4)M2, or upgrade to Cisco IOS Release 15.1(4)M3a.

- CSCtx09973

  Symptoms: Voice quality on the network deteriorates after 10 minutes.

  Conditions: This symptom is observed when voice traffic is not classified properly and is classified as web or other kind of traffic.

  Workaround: There is no workaround. However, use ACL to correctly tag the traffic.

- CSCtx19332

  Symptoms: A Cisco router crashes when ‘remote mep’ is unlearned while auto EOAM operations are executing.

  Conditions: This symptom is observed if ‘remote mep’ is unlearned from the auto database (shutdown on interface or remote mep reload) while the ‘IP SLA ethernet-monitor jitter’ operation is still running. The crash occurs if the initial control message times out.

  Workaround: There is no workaround.

- CSCtx27813

  Symptoms: Evaluation license cannot be used on a Cisco router.

  Conditions: This symptom is observed on a Cisco router when the evaluation license has high priority and the router is reloaded.

  Workaround: There is no workaround.

- CSCtx29543

  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the **show ip route** command.

  Conditions: This symptom occurs under the following conditions:

  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

  The router may now crash when doing **show ip route** command or when default route is updated.

Workaround: There are two possible workarounds:

1. Ensure that not all 23 supernet mask lengths are populated by doing route filtering.
2. If the previous workaround does not work, then ensure that at least one supernet route exists at all times for all possible mask lengths. For example by configuring summary routes that do not interfere with normal operation.

- CSCtx32628

  Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.

  Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

  – BGP full mesh is configured.
  – BGP cluster-id is configured.
  – **address family vpnv4** is enabled.
  – **address family ipv4 mdt** is enabled.
  – The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

  Workaround: Remove the cluster-id configuration or hard-reset the bgp session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx38806

  Symptoms: SSL VPN users lose connectivity as soon as Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.

  This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)

  The problem affects Firefox also (version 10.0.1) displaying the following message:

  ```
  "The page isn't redirecting properly"
  ```

  Conditions: This symptom is observed in Cisco IOS software that is acting as head end for SSL VPN connections.

  Workaround: Any of the following workarounds will work:

  1. Use the clientless portal to start the client. This only works in some versions of Cisco IOS software.
  2. Uninstall the update.
  3. Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

     ```
     webvpn gateway gateway name
        ssl encryption rc4-md5
     ```

  4. Use AC 2.5.3046 or 3.0.3054.
  5. Use older versions of Firefox (9.0.1).

  Further Problem Description: For AnyConnect users, the following user error message is seen:

```
"Connection attempt has failed due to server communication errors. Please retry the
connection"
```

The AnyConnect event log will show the following error message snippet:

```
Function: ConnectIfc::connect
Invoked Function: ConnectIfc::handleRedirects
Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED
```

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

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

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

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

- 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.

- CSCtx51935

  Symptoms: Router crashes after configuring **mpls traffic-eng tunnels**.

  Conditions: The symptom is observed with the following steps:

```
interface gi1/2
mpls traffic-eng tunnels
no shut

router OSPF 1
mpls traffic-eng area 100
mpls traffic-eng router-id lo0
end

show mpls traffic-eng link-management summary
```

  Workaround: There is no workaround.

- 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.

- CSCtx87646

  Symptoms: Firmware behavior options can only be used if "service internal" is activated.

  Conditions: The condition under which this symptom is observed is unknown.

Workaround: There is no workaround.

- CSCtx88093

  Symptoms: A dialer idle timeout is not initiated after the watched route is installed back in the routing table while using a dialer watch list, causing the watch disconnect timer to not start.

  Conditions: This symptom occurs while using the **dialer-list x protocol ip deny** command to define interesting/uninteresting traffic and while there is traffic flowing over the dialer interface.

  Workaround: Use the method that follows to define interesting traffic instead of **dialer-list x protocol ip deny**:

```
access-list x protocol ip deny
dialer-list 1 protocol ip list x
```

- 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.

Resolved Caveats—Cisco IOS Release 15.1(4)M3a

Cisco IOS Release 15.1(4)M3a is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M3a but may be open in previous Cisco IOS releases.

- CSCtx06747

  Symptoms: Device crashes at boot and never reaches CLI.

  Conditions: This symptom will happen even with no configuration. This issue is only seen with Cisco IOS Release 15.1(4)M3 due to a bad code fix integrated. The following platforms with k9 images are impacted by this bug: Cisco AS5300, Cisco AS5400, Cisco 7200, Cisco 7200p, Cisco 7301, Cisco VGD 1T3.

  Workaround: There is no workaround. Downgrade to Cisco IOS Release 15.1(4)M2, or upgrade to Cisco IOS Release 15.1(4)M3a.

Resolved Caveats—Cisco IOS Release 15.1(4)M3

Cisco IOS Release 15.1(4)M3 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M3 but may be open in previous Cisco IOS releases.

- CSCsh39289

  Symptoms: A router may crash under a certain specific set of events.

  Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.

  Workaround: There is no obvious workaround, but the problem is unlikely to occur.

- CSCsk94026

  Symptoms: AuthProxy sessions on a Cisco 871 router can be deleted immediately after completing the authentication.

Conditions: This issue is seen only on a Cisco 871 router. It occurs with a basic AuthProxy configuration on a BVI interface.

Workaround: There is no workaround.

- CSCso41274

  Symptoms: A router crashes or shows the following traceback:

  ```
  % Not enough DSP resources available to configure ds0-group 1 on controller T1 1/0 %
  The remaining dsp resources are enough for 14 time slots. % For current codec
  complexity, 1 extra dsp(s) are required to create this voice port.
  sip-cme(config-controller)# %ALIGN-3-SPURIOUS: Spurious memory access made at
  0x40C627A8 reading 0x4 %ALIGN-3-TRACE: -Traceback= 0x40C627A8 0x40D6769C 0x40D7281C
  0x40D72E74 0x4036B0E4 0x4036D4B4 0x414C78EC 0x414EB3FC
  ```

  Conditions: The symptom is observed on a router that has enough DSP resources to set up 14 signaling channels. When trying to configure a ds0-group for the 16 time-slot, you may get an error message that not enough DSP resources are available. Immediately after that the router shows the traceback or may crash.

  Example:

  ```
  sip-cme(config)#controller t1 1/0 sip-cme(config-controller)#ds0-gr 1 time 1-16 type
  e&m-imm sip-cme(config-controller)#ds0-gr 1 time 1-16 type e&m-immediate-start
  ```

  Workaround: Ensure there are more DSPs in the router than signalling channels.

- CSCta22221

  Symptoms: Frame relay client triggers reload of standby router.

  Conditions: This symptom occurs if many frame relay related configurations are present.

  Workaround: There is no workaround.

- CSCtg06045

  Symptoms: A Cisco router may reload with traceback from a crypto ACL configuration.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.4(15)T12 and experiencing a high CPU stress load while the ACEs are being changed periodically. This symptom is specific to the ACE entries in crypto ACL downloaded from KS.

  Workaround: Simplify and consolidate the ACE entries in the crypto ACL. In addition, reducing the CPU stress level may help.

- CSCth84370

  Symptoms: The Standby Supervisor gets reloaded when **write memory** is run from one VTY, and then later, **show configuration** is run from another VTY. No particular configuration needs to be done prior to **write memory**.

  Conditions: This symptom occurs when the Dual Supervisor is used and the configuration file is quite long.

  Workaround: Do not run the **write memory** and **show configuration** commands simultaneously.

- CSCti13493

  Symptoms: A router crashes and the following traceback is seen:

  ```
  ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
  ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
  %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 47523D58. - Process= "DSMP",
  ipl= 0, pid= 226, -Traceback=
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x430853EC
  ```

Conditions: The symptom is observed with the DSMP process.

Workaround: There is no workaround.

- CSCtj21237

  Symptoms: %SYS-2-LINKED: Bad enqueue, Bad dequeue messages are received, which might result an in unexpected reboot due to SegV Exception.

  Conditions: The symptom is observed on a router configured with control plane policing and protection feature.

  Workaround: Disable the feature in order to prevent any further crash.

- CSCtj79476

  Symptoms: Traffic loss and VLAN related errors seen when the traffic is sent for a prolonged duration on an HWIC-4ESW.

  Conditions: The symptom is observed when traffic is sent for a prolonged duration (>12hrs) on an HWIC-4ESW.

  Workaround: There is no workaround.

- CSCtk18404

  Symptoms: Per-user route is not installed after IPCP renegotiation.

  Conditions: The symptom is observed with the following conditions:

  1. PPP session comes up, NAS installs static routes which are sent as attribute from RADIUS server.
  2. After a while, if CPE asks for IPCP renegotiation, IPCP is renegotiated but the static routes are lost.

  Workaround: There is no workaround.

- CSCtk66753

  Symptoms: On a Cisco UC560 with SSL VPN tunnel and running Cisco IOS Release 15.1(2)T2. Heavy UDP traffic through the tunnel sometimes causes the following message to be seen:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 18188 bytes failed from 0x80319FD0,
  alignment 32
  Pool: I/O  Free: 54368  Cause: Memory fragmentation
  Alternate Pool: None  Free: 0  Cause: No Alternate pool
   -Process= "encrypt proc", ipl= 4, pid= 249
  ```

  The same issue is observed with Cisco IOS Release 15.1(2)T2 on a Cisco 871. With heavy UDP traffic through the SSL VPN tunnel, sometimes the following message is seen:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 1708 bytes failed from 0x802F6A2C,
  alignment 32
  Pool: I/O  Free: 15856  Cause: Memory fragmentation
  Alternate Pool: None  Free: 0  Cause: No Alternate pool
  ```

  Conditions: The symptom is observed when you send UDP traffic (payload size=30 bytes) to SSL VPN clients through an SSL VPN tunnel.

  Workaround: There is no workaround.

- CSCtl87463

  Symptoms: Queue length becomes negative.

  Conditions: The symptom is observed when Cisco IOS-WAAS is configured on the interface.

  Workaround: There is no workaround.

- CSCtn16855

  Symptoms: The Cisco 7200 PA-A3 cannot ping across ATM PVC.

  Conditions: This symptom occurs due to a high traffic rate, and the output policy applied under PVC.

  Workaround: There is no workaround. Removing the policy will resolve this issue, but the QoS functionality will not be present in this case.

- CSCtn62287

  Symptoms: The standby router may crash while flapping the interface or while doing soft OIR of the SPA.

  Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flows across the multilink.

  Workaround: There is no workaround.

- CSCtn83520

  Symptoms: VOIP_RTCP related traceback is seen.

  Conditions: This symptom is observed when IPIP gateways are involved.

  Workaround: There is no workaround.

- CSCtn87155

  Symptoms: CoA sessions are not coming up.

  Conditions: This symptom is observed when some CLI commands that are called within shell function might fail if the shell programmatic APIs are used.

  Workaround: Manually use shell functions on the console.

- CSCto13338

  Symptoms: When a PSTN phone is calling an IP Phone that is forwarded to a PSTN destination, the call is placed but no audio is present. This is the same behavior with blind transfer to external destinations.

  Conditions: This symptom occurs when voice-class codec X offer all and transcoders are used with CUBE.

  Workaround 1: Use the **codec XXXX** command instead of voice-class codec X offer all.

  Workaround 2: Use consultative transfer instead of blind transfer.

- CSCto32044

  Symptoms: The interface hangs and fails to pass traffic. It will still show an “up/up” status but the input and output rates will go to 0. The following errors will be seen:

  ```
  %SBETH-3-ERRINT: GigabitEthernet0/0, error interrupt, mac_status = 0x0000040000000000
  %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to reset
  ```

  The interface number will vary.

  Conditions: The conditions are unknown.

  Workaround: There is no workaround.

- CSCto89536

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
  - Memory Leak in H.323 Inspection
  - Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

- CSCto98212

  Symptoms: When RIPng is removed from an interface from telnet and serial console sessions at the same time, it causes the routers to crash.

  Conditions: This symptom occurs when RIPng is configured on an interface and two users are connected using two different console sessions.

  Workaround: Do not configure the same RIPng through two different console sessions.

- CSCtq24614

  Symptoms: The commands to ignore S1 bytes are not supported on an ATM interface.

  Conditions: The symptom is observed with an ATM SPA.

  Workaround: There is no workaround.

- CSCtq24733

  Symptoms: VXML gateway crash with “Unexpected exception to CPU: vector C”.

  Conditions: The symptom is observed with MRCP is enabled.

  Workaround: There is no workaround.

- CSCtq45553

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
  - Memory Leak in H.323 Inspection
  - Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

- CSCtq61128

  Symptoms: Router is crashing with Segmentation fault(11)

  Conditions: It was observed on routers acting as IPSEC hub using certificates.

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 6.3/5.2: 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:F/RL:OF/RC:C CVE ID CVE-2011-4231 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

- CSCtq63625

  Symptoms: WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4 is not getting trained with some DSLAMs without "line rate" configured manually. It gets trained with a manual line rate configured.

  Conditions: WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4.

  Workaround: There is no workaround.

- CSCtq63838

  Symptoms: A Cisco 2921 router crashes, and the following traceback is seen:

```
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback=
0x24A19810z 0x24A5DC8Cz 0x24A4A560z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
0x233DEA40z 0x233DEA24z
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback=
0x24A19810z 0x24A5DC8Cz 0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
0x233DEA40z 0x233DEA24z
%SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 315556E0. -Process= "DSMP",
ipl= 0, pid= 306, -Traceback= 0x246EBB2Cz 0x24719984z 0x24A19810z 0x24A5DC8Cz
0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z
23:50:00 UTC Sun May 1 2011: TLB (load or instruction fetch) exception, CPU signal 10,
PC = 0x2581FB94
```

  Conditions: This symptom is observed with the DSMP process.

  Workaround: There is no workaround.

- CSCtq64987

  Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.

  Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.

  An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

- CSCtq88777

  Symptoms: VDSL controller and ATM interface remains up, however ATM PVC becomes inactive and virtual interface goes down.

Conditions: The symptom is observed when the ATM PVC becomes inactive causing the virtual interface to go down.

Workaround: Use a VBR-NRT value that is lower than trained upstream speed.

- CSCtq90054

  Symptoms: **ip nbar protocol-discovery** fails to recognize Skype application traffic.

  Conditions: The issue is seen after configuring PfR to control NBAR based application traffic.

  Workaround: There is no workaround.

- CSCtq91939

  Symptoms: Intermittent crash due to SegV Exception after a consult transfer of external SIP call to a local ephone extension.

  Conditions: The symptom is observed under the following conditions:

  - UC540 that is running Cisco IOS Release 15.1(2)T3.
  - CME 8.1.
  - SIP----UC540---switch--SCCP---IP phones.

  Workaround: There is no workaround.

- CSCtq97991

  Symptoms: ADSL interface fails to re-train when “dsl enable-training-log” is configured.

  Conditions:

  1. Observed in a Cisco 800, 1900, and 2900 chassis and could affect other software platforms.
  2. Observed in Cisco IOS Release 15.1(2)T, Release 15.1(2)T1, and Release 15.1 (3)T.
  3. It is not observed in Cisco IOS Release 15.0(1)M4.

  Deviation observed in the following manner:

  1. With “dsl enable-training log” not configured the HWIC trains up to the DSLAM OK. After unplugging cable and reconnecting it, the HWIC still comes up fine after.
  2. Configure “dsl enable-training log”. After unplugging cable and reconnecting it, the HWIC fails to come up. CD LED does not blink and the following error message appears: “No retrain. sleep 20 seconds”.

  Workaround: Remove “dsl enable-training-log.”

- CSCtr04829

  Symptoms: A device configured with “ip helper-address” drops packets because of a zero hardware address check.

  Conditions: This symptom occurs when the hardware address is zero.

  Workaround: There is no workaround.

- CSCtr06747

  Symptoms: ISIS neighborship remains in INIT state when MTU at both ends is changed to 4470.

  Conditions: The symptom is observed when a Cisco 2900 is used in the topology with MTU 4470 (any MTU >2000).

  Workaround: Replace the Cisco 2900 with a Cisco 2800 or reduce the MTU to <2000.

- CSCtr07142

  Symptoms: A memory leak is seen at crypto_ss_open.

Conditions: No special configuration is needed.

Workaround: There is no workaround.

Further Problem Description: At bootup, when the **show memory debug leaks** command is run, memory leak entries are seen for the crypto_ss_open process.

- CSCtr18574

  Symptoms: H323-H323 video calls fail with cause code 47.

  Conditions: The symptom is observed when an H323-H323 video call fails to establish an H245 media connection. The following errors are seen:

  ```
  Received event H225_EV_H245_FAILED while at state H225_WAIT_FOR_H245
  cch323_send_passthru_out: Send passthru message retcode 15
  ```

  Workaround: There is no workaround.

- CSCtr20762

  Symptoms: L3VPN tunnel is not coming up after the router is reloaded.

  Conditions: The symptom is observed with “aaa system accounting” configured and when the TACACS server is not reachable.

  Workaround 1: Disable “aaa system accounting”.

  Workaround 2: Ensure the TACACS server is reachable.

- CSCtr33856

  Symptoms: Traceback and/or watchdog crash, with decodes pointing to mace_monitor_waas_command@

  ```
  %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 218959117 for chunk 6527D73C, data
  D0D0D0D -Process= "Exec", ipl= 0, pid= 373 -Traceback= 23054C68z 2238121Cz 223877F0z
  22397A24z 2376B0FCz 2376B0E0z or %SYS-2-FREEBAD: Attempted to free memory at 4F, not
  part of buffer pool -Traceback= 24F4EA90z 23789608z 237758E4z 23054C68z 2238121Cz
  223877F0z 22397A24z 2376B0FCz 2376B0E0z %SYS-2-NOTQ: unqueue didn’t find 4F in queue
  28275D8C -Process= "Exec", ipl= 4, pid= 374
  ```

  Conditions: The symptom is observed with on the fly changes to mace policies and classes.

  Workaround: There is no workaround.

- CSCtr45978

  Symptoms: Cisco IOS WAAS has FTP connections hung in CONN_ABORT state.

  Conditions: Device configured with Cisco IOS WAAS, and crafted FTP packets are passed across the WAN link. Has only been observed on 15.2(1)T IOS Code. Once the connection limit is reached and the rest of the connections started going pass-through.

  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 5/4.1:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:P/A:N/E:F/RL:OF/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

- CSCtr46123

  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

- CSCtr50118

  Symptoms: The router crashes.

  Conditions: This symptom occurs when the presence feature is turned on.

  Workaround: There is no workaround.

- CSCtr51926

  Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

  Conditions: The symptom is observed when a service-policy is applied on the main interface.

  Workaround 1: Enable IPv6 explicitly on the main interface:

  interface x/y ipv6 enable

  Workaround 2: Reconfigure the IPv6 address on the subinterface:

  interface x/y.z no ipv6 address ipv6 address ...

- CSCtr52740

  Symptoms: Query on an SLA SNMP MIB object using an invalid index can cause the device to crash.

  Conditions: The symptom is observed when querying history information from rttMonHistoryCollectionCompletionTime object using invalid indices.

  Workaround: Instead of using “get”, use “getnext” to list valid indices for the MIB OID.

- CSCtr54327

  Symptoms: A Cisco router may crash due to a SegV exception or have a spurious access when a fax comes in.

  Conditions: The crash occurs on a voice gateway that is configured with transcoding and fax passthrough where a fax call comes in for a codec, but the fax is not configured for a codec, and the “a=silenceSupp:off” option is set in SDP.

  Workaround: There is no workaround.

- CSCtr58658

  Symptoms: VSA crypto engine reports “Deny Jump overflow” when packet match deny entries that are supposed to be sent clear.

  Conditions: This problem only occurs with a Cisco 7200 with a VSA crypto engine module, where there are many crypto maps. Many of them use deny ACL, and many permit/deny crypto ACL entries share either the same source or the same destination address.

  Workaround: Do not use deny entries. The traffic that does not match permit entries will automatically send clear.

- CSCtr59840

  Symptoms: Crypto tunnels may flap up and down constantly after issuing a **clear crypto session** or **clear crypto isakmp** and **clear crypto sa**.

```
RTR#clear cry sess RTR# %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer
10.10.1.1:500 Id: serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN,
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer 10.10.10.10:500 Id:
serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN, RTR#
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP . Peer 10.10.1.1:500 Id:
serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN, %CRYPTO-5-SESSION_STATUS:
Crypto tunnel is UP . Peer 10.10.10.10:500 Id:
serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN, ...
```

  Conditions: This issue is seen when using eToken and OCSP revocation check on Cisco 870, 881, 1812 and 1921 routers that are running Cisco IOS Release 15.1 (2)T3. Certificate-based authentication is also used.

  Workaround: Disabling OCSP revocation check, if configured, may alleviate this behavior.

- CSCtr66487

  Symptoms: Packet drops beyond 1492 MTU size with MPLS L2VPN Xconnect configuration.

  Conditions: The symptom is observed when you ping mpls pseudowire 10.0.0.1 101 size 1493 and above.

  Workaround: There is no workaround.

- CSCtr67852

  Symptoms: Invalid route entries injected by the RRI mechanism after an HSRP failover happens in a stateful IPSec HA setup.

  Conditions: The symptom is observed following a failover in a stateful IPSec HA setup and the use of RRI.

  Workaround: Clear all crypto sessions with **clear crypto session** or remove and add back the crypto map to the interface where it is applied.

- CSCtr72393

  Symptoms: Virtual-access goes down whenever you apply a service-policy to the dialer interface.

  Conditions: The symptom is observed when you apply a service-policy to the dialer interface.

  Workaround: There is no workaround.

- CSCtr72685

  Symptoms: Keyserver is sending rekey for all groups after a change.

  Conditions: Keyserver is configured for multiple GDOI groups. A change is made (e.g. ACL, sa receive only) triggering a rekey. The rekey is being sent to all the groups instead of the impacted one(s). This was observed on Cisco IOS Release 12.4(24)T, 15.0M, and 15.1M.

  Workaround: There is no workaround.

- CSCtr79347

  Symptoms: A Cisco ASR1006 crashes without a BGP configuration change or BGP neighbor up/down event.

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
Traceback summary
% 0x80e7b6 : __be_bgp_tx_walker_process
% 0x80e3bc : __be_bgp_tx_generate_updates_task
% 0x7f8891 : __be_bgp_task_scheduler
```

Conditions: No conditions but this is a rarely observed issue.

Workaround: There is no workaround.

- CSCtr83533

  Symptoms: When you check the message on a VM system and that triggers the SIP notify to turn off the MWI to IAD, IAD will turn off the MWI but, after that, DSP is not released for the port. If you make one more call, in the next call you will hear silence. After it is off hook, there is no ring tone.

  Conditions: The symptom is observed when MWI is configured for analog ports on IAD, and if MWI is ON and a call is made to clear the MWI.

  Workaround 1: Reload the router.

  Workaround 2: Remove the MWI configuration from the analog port configuration.

- CSCtr86437

  Symptoms: NAT-PT function does not work properly after an interface flap occurs.

  Conditions: The symptom is observed when you configure NAT-PT on the router.

  Workaround: Reconfigure “ipv6 nat prefix.”

- CSCtr86666

  Symptoms: EIGRP flap due to retry limit exceeded. On peer it is waiting for INIT ACK and complains of out of order sequence number.

  Conditions: DMVPN network with a spoke running Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCtr87413

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

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

  Workaround: Use **clear crypto sa**.

- CSCtr92779

  Symptoms: Call scenario is with Avaya CM6 over TLS/SIP trunks which causes the Cisco 3945 router (running Cisco IOS Release 15.1(4)M1) CUBE to crash.

  Conditions: The symptom is observed when a call is originated from Cisco Phone A via TLS/SIP Trunk to CUBE (3945 15.1(4)M1), to Avaya CM6 Phone A which is set to “call forward all” back to the original Cisco Phone A.

  Workaround: There is no workaround.

- CSCtr94471

  Symptoms: Carrier specific exec commands under cellular interface, such as profile configuration and activation commands, return an error.

  Conditions: The symptom is observed after the router boots up.

  Workaround: There is no workaround.

- CSCtr97248

  Symptoms: Router reloads with the following:

  ```
  Unexpected exception to CPU: vector 300, PC = 0xZZZZZZZZ , LR = 0xXXXXXXXX -Traceback=
  0xZZZZZZZZ
  ```

  Conditions: The symptom is observed with L4F (TCP Proxy) based NAT ALG processing of TCP DNS traffic.

  Workaround: Use the following configuration:

  ```
  Router(config)# no ip nat service tcp-alg
  ```

- 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.

- CSCts11594

  Symptoms: A mediatrace session is scheduled with an attached session-parameter. The session is unscheduled and the session-parameters removed so that the default session parameters should be used.

  On the first schedule, traceback is seen. The session is again unscheduled and scheduled for second time and a crash is seen.

  Conditions: The symptom is observed when using custom session-parameters for a session and then removing it. Then using the default session-parameters followed by scheduled and unscheduled twice.

  Workaround: Use either the default session-parameters or custom session-parameters. Do not toggle between both.

- CSCts11743

  Symptoms: A Cisco router acting as a Call Manager Express device may unexpectedly reboot due to stack corruption.

  Conditions: The symptom is observed if more than eight calls are being queued in a route point, and one agent transfers a call back to this route point's queue.

  Workaround: From UCCX, set the limit of calls in the queue to eight.

- CSCts12366

  Symptoms: Memory may not properly be freed when malformed SIP packets are received on the NAT interface.

  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 5/4.8:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C

CVE ID CVE-2011-2578 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

- CSCts16285

  Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time out. In the worst case, the line card may become disconnected if timeouts continue for a long period.

  Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.

  Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- CSCts18257

  Symptoms: MGCP modem passthru call is failing.

  Conditions: The issue is observed on a Cisco AS5400 that is running Cisco IOS Release 15.1(4)M.

  Workaround: Use Cisco IOS Release 15.0(1)M6, if possible.

- CSCts24348

  Symptoms: PBR "set vrf" feature can cause unnecessary ARP requests and packet drops if some other feature is configured on the same router interface and packets are punted to process-switching path. This issue slows down TCP traffic considerably as first SYN in a flow may always be dropped.

  Conditions: The symptom is observed with multi-VRF selection using the Policy Based Routing (PBR) feature. It was observed in all IOS versions with new CEF code (Cisco IOS Release 12.4(20)T and upwards). The issue was not seen in Cisco IOS Release 12.4(15)T and Release 12.4(25).

  Workaround: This issue can be alleviated by using proxy ARP on the upstream device. Otherwise, there is no workaround.

- CSCts27042

  Symptoms: PIM bidirectional traffic loops upon DF-election and RPF-change.

  Conditions: The symptom is observed with several hundred streams combined with a routing change (interface shutdown/no shutdown or metric increment/decrement).

  Workaround: There is no workaround.

- CSCts28315

  Symptoms: A DHCP PD request does not accept a specific server.

  Conditions: The symptom is observed because the router does not include any IA Prefix option in Request message. This is correct behavior of RFC:

  http://tools.ietf.org/html/rfc3633#section-10

  A requesting router may set the IPv6 prefix field to zero and a given value in the prefix-length field to indicate a preference for the size of the prefix to be delegated.

  Workaround: There is no workaround.

- CSCts30143

  Symptoms: CPE WAN Management Protocol (CWMP) function is not working on UC500 platforms.

  Conditions: The symptom is observed under normal operation.

  Workaround: There is no workaround.

- CSCts31111

  Symptoms: Coredump generation fails on the Cisco 800.

  Conditions: This symptom occurs when coredump is configured.

  Workaround: Go to ROMmon, and set a variable WATCHDOG_DISABLE before the coredump happens, as follows:

```
conf t
config-reg 0x0
end
wr
reload
yes
<rommon prompt>
DISABLE_WATCHDOG=yes
sync
set
conf-reg 0x2102
reset
```

- CSCts38291

  Symptoms: When configuring 6VPE, you may see prefix corruption. Advertised prefix is different than the one installed. RD value also changes as well.

  Conditions: The symptom is observed when configuring “vpnv6 address family”.

  Workaround: There is no workaround.

- CSCts38429

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

- 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 “no 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”.

- CSCts40771

  Symptoms: Device goes into a hang state and requires a power cycle. If “scheduler isr-watchdog” is configured, the device will crash and reload the system.

  Conditions: This issue has been seen with “ip nbar protocol-discovery” configured on tunnel interfaces.

  Workaround: Remove “ip nbar protocol-discovery” from the device.

- CSCts64539

  Symptoms: The BGP next hop is inaccessible. The **show ip route** command output in the global and VRF routing tables shows that the next hop is reachable. The **show ip bgp vpnv4** all attr next-hop command output shows max metric for the next hop.

  Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

Workaround 1: If “set ip next-hop” is not configured in import route map, this issue does not occur.

Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

Workaround 3: If “neighbor x.x.x.x diable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- CSCts76410

  Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

  Conditions: The symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.

  Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCts78348

  Symptoms: Packet drop will occur on a router when the interface is configured as 10/full.

  Conditions: It seems that when interface is configured as 10/full, with the traffic of 10 Mbps, this issue will occur. By performing a shut/no shut on the interface, this issue will recover but it will be seen again when you reload the device.

  This issue may be seen on a Cisco 19xx and a Cisco 29xx (except Cisco 2951) This issue may occur when manual set duplex on the affected platform.

  Workaround 1: Perform a shut/no shut on the interface and this issue will recover.

  Workaround 2: Use auto negotiation.

- CSCts80643

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  A workaround is available to mitigate this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp

- CSCts99818

  Symptoms: Traceback is seen.

  Conditions: The symptom is observed when multimode ADSL/VDSL CPE configuration is rapidly changed between VDSL and ADSL mode while using a VDSL2-only transmission mode profile on DSLAM.

  Workaround: There is no workaround.

- CSCtt07878

  Symptoms: A Cisco 7206 router running IPSec sees this message in syslog output:

  ```
  WARNING: start sending an incomplete HAPI bundle with errors
  ```

Conditions: The symptom is observed with a Cisco 7206 router that is running IPSec with Cisco IOS Release 15.0(1)M4.7 or higher.

Workaround: There is no workaround.

- CSCtt11210

  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt20215

  Symptoms: Controller goes down after reload.

  Conditions: The symptom is observed with a VWIC3-2MFT-T1E1 (in E1/CAS mode) connected to a PBX.

  Workaround: Unplug/plug the cable, or reset link from PBX side.

- CSCtt26074

  Symptoms: Memory leak with IP SLAs XOS Even process.

  Conditions: The symptom is observed with IP SLA configured.

  Workaround: There is no workaround.

- CSCtt28703

  Symptoms: VPN client with RSA-SIG can access a profile where the CA trustpoint is not anchored

  Conditions: Use of RSA-SIG.

  Workaround: Restrict access by using a certificate-map matching the right issuer.

  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 3.5/3:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:P/I:N/A:N/E:POC/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

- CSCtt36513

  Symptoms: Crash seen on a Cisco ASR for the process IPSec key engine.

  Conditions: The symptom is observed when you have more than 4K sessions up on the ASR.

  Workaround: There is no workaround.

- CSCtt47007

  Symptoms: Router is unstable and displays badshare error messages in the syslog:

  ```
  -Traceback= 60DE2A40z 60DE40C8z 602D1E30z 60F36DA4z 60F17894z *Oct 19 11:31:59.358:
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=69B9D3FC, count=
  ```

Conditions: Has been seen on a Cisco ISR 3845 with AIM-SSLV3. It may also show on other platforms as well.

Workaround: Disable WebVPN CEF and reload the router.

- 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.

- CSCtt97905

  Symptoms: Multiple demandNbrCallDetails traps generated.

  Conditions: Multiple demandNbrCallDetails traps are generated for connect under normal conditions.

  Workaround: There is no workaround.

- CSCtt98801

  Symptoms: Mobile router reports stale RRP received from HA.

  Conditions: The symptom is observed when the mobile router sends a RRQ to HA in CCOA mode.

  Workaround: There is no workaround.

- CSCtu02835

  Symptoms: Slow performance through the fastethernet WAN ports while running Cisco IOS Release 15.1(4)M2.

  Conditions: When the issue occurs the fastethernet WAN ports are showing a large number of throttles in the **show interface** command. The symptom only occurs when the **scheduler interval** command is configured.

  Workaround: Remove the **scheduler interval** command.

- CSCtu07626

  Symptoms: Router processing SIP traffic crashes.

  Conditions: The following error may be seen prior to the crash:

  ```
  %SDP-3-SDP_PTR_ERROR: Received invalid SDP pointer from application. Unable to
  process.
  ```

  Workaround: There is no workaround.

- CSCtu13446

  Symptoms: High CPU utilization will be seen on Cisco 39xxE platforms if an SM-2GE-SFP module is plugged in.

  Conditions: The symptom is observed when a SM-2GE-SFP module is plugged in.

  Workaround: There is no workaround.

- CSCtu36562

  Symptoms: cikeFailureReason and cipsecFailureReason from CISCO-IPSEC-FLOW-MONITOR MIB do not report the proper failure reasons for failed IKE negotiations (ph1 or ph2).

  Conditions: The symptom is observed with failed IKE negotiations (ph1 or ph2).

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(4)M2

Cisco IOS Release 15.1(4)M2 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M2 but may be open in previous Cisco IOS releases.

- CSCso46409

  Symptoms: mbrd_netio_isr and crypto_engine_hsp_hipri traceback log messages are produced.

  Conditions: This symptom is observed using WebVPN on a Cisco 3845 with an AIM-VPN/SSL-3.

  Workaround: There is no workaround.

- CSCta93316

  Symptoms: Memory leaks are seen.

  Conditions: The symptom is observed after the coop functionality test when using the **show memory debug incremental leaks** command.

  Workaround: There is no workaround.

- CSCtb55479

  Symptoms: A router may crash by the “BGP Router” process.

  Conditions: This symptom is observed if the memory is corrupted.

  Workaround: There is no workaround.

- CSCtd10735

  Symptoms: A router crashes with a Cisco 7200 platform image.

  Conditions: Configuring the sgbp test commands as given in the “Steps to reproduce” enclosure.

  Workaround: There is no workaround.

- CSCtd15853

  Symptoms: When removing VRF configuration on remote PE, local PE receives withdraw message from remote PE to purge its MDT entry. However, local PE does not delete the MDT entry.

  Conditions:

  - mVPN is configured on PE router.
  - Both Pre-MDT SAFI and MDT-SAFI IOS are running in a Multicast Domain.

  CCO : MDT SAFI
  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

  Workaround: There is no workaround.

- CSCtg42271

  Symptoms: A router that is running Cisco IOS Release 15.0(1)M1 may experience a series of spurious memory access errors and a bus error when configured for IPS:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0xXXXXXXXX reading 0xXXX
  %ALIGN-3-TRACE: -Traceback= 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX
  0xXXXXXXXX
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x70, pc=0x251A00CCz ,
  ra=0xFFFF3331z , sp=0x28F88EB0
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x70, pc=0x251A00CCz ,
  ra=0xFFFF3331z , sp=0x28F88EB0
  XX:XX:XX XXX XXX XXX XX XXXX: TLB (store) exception, CPU signal 10, PC = 0xXXXXXXXX
  ```

Conditions: The symptom is observed when the device is configured for IPS and is running Cisco IOS Release 15.0(1)M1.

Workaround: There is no workaround.

- CSCth11006

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCth80642

  Symptoms: IOS SSLVPN fails to accept new ssl connection. Sessions get stuck in Time Wait until TCP queue is full.

  Conditions: SSLVPN on IOS.

  Workaround: clear tcp tcb * will clear Time Wait sessions.

- CSCti33159

  Symptoms: The PBR topology sometimes chooses a one-hop neighbor to reach a border, as opposed to using the directly-connected link.

  Conditions: This is seen when the border has multiple internal interfaces and one of the internal interfaces is directly connected to a neighbor and the other interface is one hop away.

  Workaround: There is no workaround.

- CSCtj47822

  Symptoms: The standby RP is stuck in standby_issu_negotiation_late state after a switchover and does not come to SSO. Also, memory leaks are seen at tid_cmn_add_or_find_port_info.

  Conditions: This symptom occurs during the peer (standby RP) reset or switchover.

  Workaround: There is no workaround.

- CSCtj56551

  Symptoms: The Cisco 7600 crashes in a very rare case.

  Conditions: This symptom is observed very rarely when route-churn/sessions come up.

  Workaround: There is no workaround.

- CSCtj95685

  Symptoms: A router configured as a Voice Gateway may crash while processing calls.

  Conditions: This symptom is observed with a router configured as a Voice Gateway.

  Workaround: There is no workaround.

- CSCtk34885

  Symptoms: Crosstalk being heard intermittently on inbound calls.

Conditions: Inbound calls from PSTN to Ingress gateway hearing crosstalk on Rout call leg (DSP to PSTN) on AS5400XM.

Workaround: The following command in IOS can mitigate this for SIP:

voice service voip sip source filter

This eliminates the risk for crosstalk since the gateway blocks all rogue audio out to the PSTN with this command.

The above command only works for SIP, so H323, MGCP, and SCCP are still affected.

The following enhancement requests have been filed:

CSCtq47019 - support on H.323, SCCP, and MGCP. This will allow the command to be used in all VoIP environments.

CSCtq47431 - To get this feature added to IP phones.

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 1.8/1.6:

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

- CSCtk69114

  Symptoms: RP resets while doing ESP reload with crypto configuration.

  Conditions: This symptom is observed by unconfiguring and configuring interface configuration and reloading both ESPs. The RP crashes on the server.

  Workaround: There is no workaround.

- CSCtk98248

  Symptoms: An FA8 line protocol goes down after the connected device is reloaded.

  Conditions: The symptom is observed with the following conditions:

  - A Cisco 892 router that is running Cisco IOS Release 15.0(1)M3 or earlier.
  - The Cisco 892 is the only FA8 port and is set to 10/full.
  - A Cisco 3750/2960 router that is running a Cisco IOS Release other than Cisco IOS Release 12.2(37)SE.

  Workaround 1: Set the FA8 to 100/full or auto.

  Workaround 2: Use Cisco IOS Release 15.0(1)M4 on the Cisco 892.

  Workaround 3: Use Cisco IOS Release 12.2(37)SE on the Cisco 3750/2960 router.

- CSCtl00995

  Symptoms: Cisco ASR 1000 series routers with 1000 or more DVTIs may reboot when a shut/no shut operation is performed on the tunnel interfaces or the tunnel source interfaces.

  Conditions: This symptom occurs when all the DVTIs have a single physical interface as tunnel source.

  Workaround: Use different tunnel source for each of the DVTIs. You can configure multiple loopback interfaces and use them as tunnel source.

- CSCtl01141

  Symptoms: cswmMvrfStatsTable does not get populated.

  Conditions: This symptom occurs when the multicast vrf instance is configured on any switch running mtrose image and mibwalk is configured on cswmMvrfStatsTable.

  Workaround: There is no workaround.

- CSCtl23748

  Symptoms: EoMPLS over GRE (DMVPN) with IPSec protection is not working after a reboot.

  Conditions: The symptom is observed when there is a tunnel (Ethernet over MPLS over GRE over IPSec) between PE1 and PE2 and following a reload and when tunnel protection is configured.

  Workaround: There is no workaround.

- CSCtl50815

  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

  ```
  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
  Non-OER, OOP Reason <reason>
  ```

  Conditions: The symptom is observed under the following conditions:

  - Use ECMP.
  - Use **mode monitor passive**.

  Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

  Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl52854

  Symptoms: Client does not receive multicast traffic when it is connected to an EHWIC port in access mode.

  Conditions: This symptom is observed when a multicast server is connected to an EHWIC L2 interface.

  Workaround: Connect the multicast server to an on-board gig interface.

- CSCtl54975

  Symptoms: A small number of Cisco 1812 routers have been observed to unexpectedly restart due to software-forced crashes, repeatedly.

  Conditions: Unknown.

  Workaround: While the root cause is being investigated, units that are experiencing this problem should be replaced. Please replace the Cisco 1812 and send the unit for Failure Analysis, after contacting the Cisco TAC and referencing this bug ID.

- CSCtl55502

  Symptoms: Any parser command with a pipe option used in an HTTP URL is not working properly and giving the help option instead of the actual output.

  Conditions: The symptom is observed when a parser command uses a pipe option in an HTTP URL (for example, http://<ipadd>/level/15/exec/show/runn/|/i/http/CR).

  Workaround: There is no workaround.

- CSCtl74521

  Symptoms: Crackling voice is heard on the PSTN rx side.

  Conditions: This symptom occurs under the following conditions:

  - RTP comes from Multilink interface. There is no audible crackling in the RTP stream.
  - If used, codec g711ulaw with packetization > 80 bytes.

  Workaround: Set codec packetization to 80 bytes on dial-peer or voice-class codec.

- CSCtl82517

  Symptoms: For the Cisco ME3600 and Cisco ME3800, the following licensing errors are seen, leading to license manager failure at bootup:

  ```
  %SCHED-7-WATCH: Attempt to lock uninitialized watched semaphore (address 0). -Process=
  "Init", ipl= 4, pid=
  ```

  Conditions: This symptom is seen when a Cisco ME3600 or Cisco ME3800 license-based image is loaded off mcp_dev_nile.

  Workaround: Use whales-universal-mz.

- CSCtl90341

  Symptoms: A router crashes due to an NHRP stack overflow.

  Conditions: This symptom occurs very inconsistently.

  Workaround: There is no workaround.

- CSCtn04277

  Symptoms: Time-based WRED does not work.

  Conditions: The symptom is observed when time-based WRED is used in Cisco IOS Release 15.1(3)T.

  Workaround: There is no workaround.

- CSCtn04357

  Symptoms: When applying the following netflow configuration in the same sequence, the standby supervisor module continuously reloads:

  ```
  vlan configuration 161 ip flow monitor flowmonitor1 in ip flow monitor flowmonitor1
  input
  ```

  Conditions: The symptom is observed on a Sup7-E that is running Cisco IOS XE Release 3.1.0(SG). The router must have a redundant RP. The monitor must be using a flow record that does not conform to V5 export format while being used with V5 exporter and be running on a distributed platform. When the flow monitor is applied to an interface the config sync will fail and the standby will reload.

  Workaround 1: Remove the flow monitor configuration.

  Workaround 2: Use netflow-v9 export protocol.

  Workaround 3: Use a record format exportable by netflow-v5.

- CSCtn08673

  Symptoms: A Cisco device crashes with tracebacks:

  ```
  08:56:31 gmt Fri Jan 14 2011: Unexpected exception to CPU: vector D, PC = 0x3CD7565
  %Traceback= 3CD7565 29D255AC 3D5602E 3D3A510 3D69BC2 3CC49C8 3CC2266 3CCD42B 3CCC96D
  ```

  Conditions: This symptom is observed on a Cisco 3900 running Cisco IOS Release 15.1(1)T1.

  Workaround: There is no workaround.

- CSCtn10507

  Symptoms: Tracebacks at fw_dp_base_process_new_pak & fw_dp_state_object_init_obj IPv6 routing and mediatrace do not come up.

  Conditions: This symptom is observed when FW with self zones is configured on the router.

  Workaround: There is no workaround.

- CSCtn12119

  Symptoms: There is no change in functionality or behavior from a user perspective. This DDTS brings in changes to padding used during signing/verification from PKCS#1 v1.0 to PKCS #1v1.5.

  Conditions: This symptom is observed during signing/verification for releases prior to Cisco IOS Release 15.1(2)T4.

  Workaround: The Rommon is capable of verifying images signed using both v1.0 and v1.5. As such no workaround is necessary from a usability perspective, the image boots and runs as expected. However, it will not be in compliance with FIPS 140-3 requirements.

- CSCtn18784

  Symptoms: Interface Tunnel 0 constantly sends high-bandwidth alarms.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtn21198

  Symptoms: Placing fax calls through c5510 DSP (NM-HDV2, etc) using Voice over Frame Relay (VoFR) may trigger UNSUPPORTED CODEC messages on the console and possibly a WatchDog Timeout.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(2)T and Release 15.1(4)M.

  Workaround: Use Voice over IP (VoIP) instead of VoFR, or use an older IOS release.

- CSCtn21501

  Symptoms: A Cisco 2900 series router with switch modules (such as HWIC-4ESW-POE or HWIC-D-9ESW-POE) does not respond to SNMP queries on the BRIDGE-MIB.

  Conditions: The symptom is observed on a Cisco 2900 series router (with switch modules) that is running Cisco IOS Release 15.x.

  Workaround: There is no workaround.

  Further Problem Description: This issue is similar to CSCsb46470.

- CSCtn31333

  Symptoms: High CPU utilization is observed on the Cisco CMTS router due to the Net Background process.

  Conditions: This symptom is observed on a router used for L2TP network server (LNS) with an L2TP application.

Workaround: There is no workaround.

- CSCtn40571

  Symptoms: Issuing the **crypto pki server** *name* **rollover cancel** command can result in multiple rollover certificates installed on Sub-CA router.

  Conditions: This symptom is seen when the rollover certificate is already installed.

  Workaround:

  - Copy startup-configuration from router.
  - Remove the older rollover certificate from configuration under the **crypto pki cert chain** *ca* command.
  - Copy the new configuration back to startup-configuration and reload the router.

- CSCtn43589

  Symptoms: A crash is observed at process_run_degraded_or_crash.

  Conditions: The symptom is observed when SNMP bulkstat has been configured for periodic MIB collection.

  Workaround: There is no workaround.

- CSCtn47119

  Symptoms: Router crashes when sending IPv6 ping packets.

  Conditions: The symptom is observed when a ping is issued with a packet size of more than 1500 bytes.

  Workaround: There is no workaround.

- CSCtn58128

  Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

  Conditions: The issue may be triggered by route-flaps in scaled scenario where the route reflector may have 4000 route reflector clients and processing one million+ routes.

  Workaround: Ensure “no logging console” is configured.

- CSCtn59075

  Symptoms: A router may crash.

  Conditions: This has been experienced on a Cisco router that is running Cisco IOS Release 15.1(3)T, 15.1(3)T1, and 15.1(4)M. Flexible Netflow needs to be running.

  Workaround: There is no workaround.

- CSCtn65060

  Symptoms: A Cisco device crashes.

  Conditions: This symptom is observed with Cisco IOS Release 15.0M and Release 15.1T when configuring “snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL.”

  Workaround: Avoid using the **snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL** command.

- CSCtn68117

  Symptoms: Session command does not work on Cisco C3K series routers that have become the master after a mastership change.

Conditions: This symptom is seen when fail-over to slave occurs.

Workaround: There is no workaround.

- CSCtn79475

  Symptoms: A Cisco router reloads often due to stack overflow under some traffic conditions.

  Conditions: This symptom is observed when calls resulting in VOIPRTP media loop are seen.

  Workaround: There is no workaround.

- CSCtn93891

  Symptoms: Multicast traffic is getting blocked.

  Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

  Workaround: There is no workaround.

- CSCtn97267

  Symptoms: There is a router crash in the URLF code using Websense.

  Conditions: The symptom is observed on a Cisco ISR G2 during normal operation. It is caused by long URLs overwriting the end of a fixed length buffer.

  Workaround: There is no workaround.

- CSCto00796

  Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending RT extended community for one of the redistributed vpnv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).

  Conditions: This symptom occurs when a new interface is provisioned inside a vrf and the configuration such that the connected routes are redistributed in the vrf. This redistributed route fails to tag itself with the RT when it reaches the peering PE(+RR)

  Workaround: Soft clear the peer that missed getting the RT.

- CSCto02712

  Symptoms: A router that is running Cisco IOS Release 15.1(4)M1 with “proxy-arp” enabled will incorrectly reply to duplicate address detection ARP requests sourced from end devices.

  Some end devices will send an ARP request for their assigned IP to check for duplicate address detection per RFC5227. When this occurs the router should ignore this ARP request. With this issue, the router will respond to the request, which triggers the duplicate address detection on the end device and breaks connectivity between the router and end device.

  Conditions: The symptom is observed with the following conditions:

  – “proxy-arp” is enabled on client facing Layer-3 interface.
  – end device sends a “duplicate address detection” ARP request on its local subnet.

  Workaround 1: Configure **no ip proxy arp** on client-facing interface.

  Workaround 2: Disable “duplicate address detection” on the end device.

- CSCto05108

  Symptoms: A Cisco 7206 with VSA card is used as a GETVPN GM. After some time of operation, the router prints VSA-related traceback and completely stops encrypting/decrypting any traffic:

```
%008720: Feb 24 11:11:01.674 GMT+5: VSA shim: crypto_ike_encrypt_callback ctx_next
NULL -Traceback= 0x1BF4364z 0x3D38AE4z 0x3D007FCz 0x3CFA77Cz 0x3CFE108z 0x15829FCz
0x15857ACz 0x1584800z 0x15822C8z 0x5580000z 0x1584E78z 0x1582384z 0x3D00DD8z
0x3D00A64z 0x3D3852Cz 0x3D411B0z
```

After that, all encrypted traffic is dropped. Crypto debugs (debug crypto isakmp, etc) do not produce any messages. The only way to recover is to reboot the router.

Conditions: This symptom is observed on a Cisco 7206 where a VSA card is used as a GETVPN GM and running Cisco IOS Release 15.0(1)M4 or Release 12.4(24)T3.

Workaround: Disable encryption.

- CSCto08135

  Symptoms: When a deny statement is added as the first ACL, the message gets dropped.

  Conditions: An ACL with deny as the first entry causes traffic to get encrypted and denied.

  Workaround: Turn off the VSA, and go back to software encryption.

- CSCto10485

  Symptoms: With a GRE over IPSec configuration using tunnel protection, traffic originated from the router may be dropped on the receiving router due to replay check failures. This is evident by the %CRYPUO-4-PKT-REPLAY drops as shown in the syslog.

  Conditions: This issue typically occurs during high traffic load conditions.

  Workaround: There is no workaround.

- CSCto14518

  Symptoms: The command **show memory debug leak** may crash a router.

  Conditions: The symptom is observed when using the command **show memory debug leak**.

  Workaround: There is no workaround.

- CSCto15361

  Symptoms: MF: Active Supervisor crashes after removing the “router eigrp” configuration.

  Conditions: This symptom occurs when the Active Supervisor crashes while disabling the Ipv6 router eigrp because the EIGRP Hello process gets killed. This issue occurs because the EIGRP Hello process calculates the size of the packet. After investigation, it was found that this is purely a timing-based issue. During cleanup, which is done by the EIGRP PDM process, the peer list is cleaned up first, and then an attempt is made to kill the Hello process. In case the peer list is cleaned up, and then the Hello process tries to calculate the size of a particular peer, then it finds the peer as NULL and crashes.

  Workaround: Modify the igrp2_procinfo_free function to kill the EIGRP Hello process prior to cleaning up the peer list.

- CSCto34844

  Symptoms: The Cisco 891 may perform lower than the older generation Cisco 1812 platform.

  Conditions: This symptom occurs when Ethernet traffic using the VLAN tag is encapsulated inside the L2TPv3 tunnel.

  Workaround: There is no workaround.

- CSCto39885

  Symptoms: A router crashes.

  Conditions: gcid and callmon is turned on.

  Workaround: There is no workaround.

- CSCto41165

  Symptoms: The standby router reloads when you use the **ip extcommunity-list 55 permit|deny** command, and then the **no ip extcommunity-list 55 permit|deny** command.

  Conditions: This symptom occurs when the standby router is configured.

  Workaround: There is no workaround.

- CSCto41173

  Symptoms: A voice gateway crashes by TLB (store) exception with BadVaddr = 00000244.

  Conditions: This symptom is observed with a platform that acts as an H323 gateway and runs Cisco IOS Release 15.1(3)T.

  Workaround: Revert to Cisco IOS Release 12.4(20)T.

- CSCto43683

  Symptoms: Suspended service policy is not re-enabled when an MFR bundle link comes up.

  Conditions: The symptom is observed when the service policy is attached to MFR DLCI.

  Workaround: There is no workaround.

- CSCto48060

  Symptoms: A Cisco 3900 series router may crash with the following error:

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

  Conditions: The symptom is observed when the router is configured as a voice gateway using H323 and H245 and connected to CUCM. If CUCM is sending a MultiMediaSystemControl messages with no entry, the router may crash.

  Workaround: There is no workaround.

- CSCto60047

  Symptoms: A crash occurs either due to a chunk corruption or at ssh_send_queue_data.

  Conditions: This symptom occurs under the following conditions:

  - An SSH session exists between two routers.
  - The **show tech** command is issued and then aborted.

  Workaround: There is no workaround.

- CSCto63268

  Symptoms: A Cisco 3900e router may crash while configuring a PRI-group on a VWIC2 in a native HWIC slot.

  Conditions: The router must be a Cisco 3900e and the number of timeslots in the new PRI-group must be greater than the number of available DSPs. Additionally, a EVM-HD-8FXS/DID must be installed and the onboard DSPs must be configured for DSP sharing.

  Workaround: Remove the EVM or disable DSP sharing.

- CSCto65352

  Symptoms: A system crashes randomly when an Apex module is in the system.

  Conditions: The system crashes under normal conditions.

  Workaround: There is no workaround.

- CSCto72629

  Symptoms: A MAXAGE LSA is repeatedly retransmitted bringing down the OSPFv3 adjacency.

  Conditions: This symptom occurs when the unadjusted age of the LSA in the OSPFv3 database (as opposed to the advertised age, which includes time spent in the database) is less than MAXAGE. Note that the age of the LSA in the database is not updated once it is installed unless maxaging is initiated by OSPFv3 process.

  Workaround: Use the **clear ipv6 ospf process** command to clear the OSPF state based on the OSPF routing process ID.

- CSCto81701

  Symptoms: The PfR MC and BR sessions flap.

  Conditions: The symptom is observed with a scale of more than 800 learned TCs.

  Workaround: Use the following configuration:

  pfr master

  keepalive 1000

- CSCto81916

  Symptoms: Voice gateway crashes due to insufficient free memory.

  Conditions: The symptom is observed when the copy feature is used in a voice class SIP profile similar to the example below:

```
voice class sip-profiles 500
 request INVITE peer-header sip Remote-Party-ID copy ":(.*)@" u01
 request INVITE sip-header From modify "From: \"anonymous\" <(.*):(.*)
@" "From: \"\u01\" <\1:\u01@"
!
```

  In this case, a memory leak occurs and depletes all the free memory causing the router to crash.

  Workaround: There is no workaround.

- CSCto85479

  Symptoms: Spanning Tree Protocol (STP) failure on EHWIC-4ESG.

  Conditions: The symptom is observed on a Cisco 3945 chassis that is running the c3900-universalk9-mz.SPA.151-4.M.bin image. Interfaces gi0/3/0-1 are on EHWIC-4ESG card.

  Workaround: There is no workaround.

- CSCto88393

  Symptoms: CPU hogs are observed on a master controller:

```
%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (0/0),process =
OER Master Controller.
```

  Conditions: This symptom is observed when the master controller is configured to learn 10,000 prefixes per learn cycle.

  Workaround: There is no workaround.

- CSCto99343

  Symptoms: Linecards do not forward packets which causes a failure on the neighborship.

  Conditions: The symptom is observed on VSL-enabled linecards on a VSS system.

  Workaround: There is no workaround.

- CSCto99523

  Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).

  Conditions: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.

  Workaround: There is no workaround.

- CSCtq04117

  Symptoms: DUT and RTRA have IBGP-VPNv4 connection that is established via loop back. OSPF provides reachability to BGP next hop, and BFD is running.

  Conditions: This symptom occurs under the following conditions:

  1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.
  2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

  Workaround: Use the **clear ip route vrf x *** command.

- CSCtq05004

  Symptoms: A dialer loses its IP address sporadically.

  – "show interface atm x" will record output drops during the issue.

  ```
  ATM0 is up, line protocol is up
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 31956 <<
  Incrementing during the issue
  ```

  – "show interface queueing atm0.1" (hidden command) will show as follows:

  ```
  Interface ATM0 VC 8/35 Queueing strategy: fifo Output queue 40/40, 31956 drops per
  VC << Incrementing during the issue
  ```

  – During the issue, if "debug ppp negotiation" is on, we will see the following:

  ```
  PPP: Missed 5 keepalives, taking LCP down
  PPP DISC: Missed too many keepalives
  ```

  – There will be no ATM (physical interface) flap in this case (during the issue).

  – shut/no shut on the ATM interface does not help.

  Conditions: No conditions so far. The behavior is sporadic.

  Workaround: Reload.

- CSCtq05636

  Symptoms: When sending calls between two SIP endpoints, alphanumeric characters (non-numeric) are stripped when forwarding the invite to the outgoing leg. For example:

  Received:

  ```
  INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
  ```

  Sent:

  ```
  INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
  ```

  In Cisco IOS Release 15.1.3T1, the * character is not forwarded.

Conditions: This symptom is observed when CUBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1.3T1.

Workaround: Upgrade the code to Cisco IOS Release 15.1.3T or Cisco IOS Release 15.1(M4).

- CSCtq06538

  Symptoms: RP crashes due to bad chunk in MallocLite.

  Conditions: This symptom occurs while executing testcase number 4883. The test case 4883 sends an incorrect BGP update to the router to test whether the router is able to handle the problematic update. The incorrect BGP update has the local preference attribute length incorrect:

  ```
  LOCAL_PREF Header AttributeFlags Optional: 0b0 Transitive: 0b1 Partial: 0b0
  ExtendedLength: 0b0 Unused: 0b0 0b0 0b0 0b0 TypeCode: 0x05 Length: 0x01 <----- should
  be 0x04 instead Value: 0xff 0xff 0xff 0xff NetworkLayerReachabilityInfo: 0x08 0x0a
  <snip>
  ```

  Workaround: There is no workaround.

- CSCtq07413

  Symptoms: A hardware crypto engine may fail to decrypt packets. An “invalid parameter” error is seen after decryption. Software encryption works fine.

  Conditions: This symptom is observed in Cisco IOS Release 12.4.15T6.

  Workaround: Use software encryption.

- CSCtq10356

  Symptoms: When video is enabled under a call manager profile, the Zone-Based Firewall SIP inspection engine will not create the RTP pinhole for voice.

  Conditions: This symptom is observed when video is enabled under the phone profile.

  Workaround: Disable video under the phone profile; the two options to disable are “Cisco Camera” and “Video Capabilities.”

- CSCtq10524

  Symptoms: A Cisco device may crash.

  Conditions: This symptom is observed when more than the recommended number of Mediatrace sessions (>255) is applied to one interface.

  Workaround: Keep the number of Mediatrace sessions below the recommended maximum per interface.

- CSCtq10684

  Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in ipsec.

  Conditions: This symptom occurs when tunnel flap is observed before the crash.

  Workaround: A possible workaround is to reload the box.

- CSCtq12007

  Symptoms: 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.

- CSCtq15247

  Symptoms: The router crashes when removing the virtual-ppp interface. The crash is more common if the l2tp session is flapping when the virtual-ppp interface is removed.

  Conditions: This symptom occurs if the l2tp session is flapping when the virtual-ppp interface is removed.

  Workaround: Remove the **pseudowire** command from under the **virtual-ppp interface** command before removing the interface.

  For example:

```
LAC1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.
LAC1(config)#interface virtual-ppp1
LAC1(config-if)#no pseudowire
LAC1(config-if)#exit
LAC1(config)#no interface virtual-ppp1
```

- CSCtq18068

  Symptoms: An “autoqos:error” is seen when configuring auto QoS VoIP.

  Conditions: This symptom is observed in Cisco IOS Release 15.2(1)T.

  Workaround: There is no workaround.

- CSCtq21234

  Symptoms: Label is not freed.

  Conditions: The symptom is observed after shutting down the link.

  Workaround: There is no workaround.

- CSCtq21785

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(2)S may crash upon performing a CRL check on an invalid certificate.

  Conditions: The conditions are unknown.

  Workaround: Turning off CRL check should stop the crash. It should be configured as:

  “revocation-check none”

  This will stop the CRL check of the peer certificate but should not be a long term solution.

- CSCtq26892

  Symptoms: CUBE crashes @ sipSPI_ipip_IsHdrInHeaderList.

  Conditions: This symptom is observed with a PRACK-NO PRACK configuration on Cisco IOS Release 15.2(1)T.

  Workaround: There is no workaround.

- CSCtq28392

  Symptoms: A Cisco 860 router crashes.

  Conditions: The symptom is observed on a Cisco 860 router when applying tunnel protection on the tunnel interface.

Workaround: Use a crypto map configuration.

- CSCtq28732

  Symptoms: Memory leak is observed when device is configured **parameter-map type inspectglobal**.

  Conditions: Device is configured with **parameter-map type inspect global**.

  See also Cisco Security Advisory: Cisco IOS Software IPS and Zone Based Firewall Vulnerabilities, at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw

  Workaround: There is no workaround.

- CSCtq29554

  Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the **show ipc port | in MRIB** command on a failed line card does not display a port.

  Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover. The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.

  Workaround: Reload the failing line card to recover it.

- CSCtq30686

  Symptoms: A Cisco router crashes in a Secure Device Provisioning (SDP) environment.

  Conditions: This symptom is seen when the Registrar router crashes when a client router submits an enrollment request that was previously stuck in “granted” status with the same fingerprint.

  Workaround: There is no workaround.

- CSCtq33102

  Symptoms: A Cisco router that is acting as an RA crashes in an SDP environment with CVO setup.

  Conditions: This symptom occurs during CVO enrollment request.

  Workaround: There is no workaround.

- CSCtq36153

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
  - Memory Leak in H.323 Inspection
  - Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

- CSCtq49325

  Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.

Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However if a particular path is threaded to be sent, in this case it is scheduled for a reply message, the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths from sending before deletion. A similar condition will occur if the packtization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq55173

  Symptoms: A device that is configured with NAT crashes. SIP appears to be translated trough NAT. However, some cases report that the crash still occurs after redirecting SIP traffic elsewhere.

  Conditions: The crash is triggered when the **clear ip nat translation ***, **clear ip nat translation forced**, or **clear crypto ipsec client ezvpn** command is entered.

  Workaround: There is no workaround.

- CSCtq56727

  Symptoms: Bulk call failures occur during heavy traffic loads, followed by a gateway crash.

  The crash report indicates mallocfail tracebacks on CCSIP_SPI_CONTROL, AFW, VTSP, and other processes.

  “sh proc mem sorted” shows a continuous increase in memory held by the CCSIP_SPI_CONTROL process even when the average number of calls at the gateway is constant.

  Conditions: This symptom occurs when the SIP trunk in Unified Communications Manager pointing to the gateway is configured with a DTMF signaling type of “no preference” and the SIP gateway is configured with DTMF relay as sip-kpml.

  Workaround: There are two workarounds:

  1. Set the DTMF signaling type as “OOB and RFC 2833” in the Communications Manager SIP trunk configuration that is pointing to the SIP gateway.
  2. Configure “dtmf-relay rtp-nte” (instead of “sip-kpml”) in the SIP gateway dial-peer configuration. The Unified Communications Manager is configured with “no preference.”

  Recovery: In order to recover from the crash, you must reload the gateway router.

- CSCtq58383

  Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.

Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.

Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq61850

  Symptoms: When the SNR call is forwarded to CUE after the SNR call-forward noan timer (cfwd-noan) expires, the call gets dropped unexpectedly after CUE answers the call.

  Conditions: This symptom occurs when calls to the SCCP SNR phone and SNR call-forward noan timer (cfwd-noan) are configured. Both SNR and mobile phones do not answer the call and the call is forwarded to voice mail.

  Workaround: There is no workaround.

- CSCtq62322

  Symptoms: On an SNR call, when the call is forward and connected to CUE after ringing to the remote target, nothing happens (for example, no CUE prompt occurs, and the user cannot leave voice mail).

  Conditions: This symptom is observed if the answer-too-soon timer is configured, the remote target is a pstn call, and the calling party is using a sccp phone.

  Workaround: There is no workaround.

- CSCtq62759

  Symptoms: CLNS routing table is not updated when LAN interface with CLNS router isis configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when isis ages out the stale routes.

  Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

  Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq64034

  Symptoms: NAT does not send gratuitous ARP for a translated address when an interface comes up.

  Conditions: The symptom is observed when an alias (translated address) is created with the interface (whose IP address is in the same subnet as the alias entry) is in shut down state.

  Workaround: Perform an admin shut/no shut on the interface with an IP address in the same subnet as the alias entry.

- CSCtq67959

  Symptoms: Tracebacks are seen on a Cisco 7200 series router.

  Conditions: The issue seen while testing the IPv6 OSPF feature.

  Workaround: There is no workaround.

- CSCtq69083

  Symptoms: Nested IPSec tunnel with outer tunnel GRE and inner tunnel VTI/GRE is not working.

  Conditions: The symptom is observed with the v150-1.M4.6 image.

  Workaround: There is no workaround.

- CSCtq75008

  Symptoms: A Cisco 7206 VXR crashes due to memory corruption.

Conditions:

- The Cisco 7206 VXR works as a server for L2TP over IPsec.
- Encryption is done using C7200-VSA.
- More than two clients are connected.

If client sessions are kept up for about a day, the router crashes.

Workaround: There is no workaround.

- CSCtq76005

  Symptoms: Configuring “atm route-brige ip”on MPLS-enabled ATM interface makes router punt all incoming MPLS packets to CPU.

  Conditions: The symptom is observed when RBE is configured on a MPLS-enabled ATM interface.

  Workaround: Remove RBE.

- CSCtq77274

  Symptoms: FXS phones are not recognized as SCCP endpoints.

  Conditions: This symptom occurs when FXS phones are configured as SCCP endpoints.

  Workaround: There is no workaround.

- CSCtq77363

  Symptoms: License images are not working properly.

  Conditions: This symptom is seen when the license image is loaded. There is a traceback due to access of uninitialized variables.

  Workaround: There are no workarounds.

- CSCtq78217

  Symptoms: A router crashes with the following information:

  ```
  System returned to ROM by address error at PC 0xZZZZZZZZ, address 0xZZZZZZZZ
  ```

  Conditions: The symptom is observed with CUBE + SIP.

  Workaround: There is no workaround.

- CSCtq80648

  Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP ipv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.

  For example:

  ```
  interface Ethernet1/0
    vrf forwarding vpn1
     ipv6 address 1::1/64
  !
   router bgp 65000
    address-family ipv6 vrf vpn1
     neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
  ```

  If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.

  Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.

Conditions: This symptom occurs when a user changes the VRF assignment.

Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCtq80858

  Symptoms: A router crashes randomly at various decodes.

  Conditions: This symptom is observed when MACE and IP SLA TCP-based probes are configured.

  Workaround: There is no workaround.

- CSCtq84635

  Symptoms: Trunk DNs can act as if busy (such as by triggering CFB) even though they have no calls and show commands for ephone-dns or ports report nothing unusual.

  Conditions: This symptom occurs in Cisco IOS Release 15.0(1)M after heavy use; it is believed not to occur in Cisco IOS Release 12.4(20)T or prior releases.

  Workaround: Delete and re-add trunk DNs.

- CSCtq85728

  Symptoms: An EHWIC-D-8ESG card is causing an STP loop.

  Conditions: EHWIC-D-8ESG might not be blocking appropriate ports according to calculated STP topology that introduces the loop in the network.

  Workaround: There is no workaround.

- CSCtq86500

  Symptoms: With the fix for CSCtf32100, clear text packets destined for the router and coming into a crypto-protected interface are not switched when VSA is used as the crypto engine.

  Conditions: This symptom occurs with packets destined for the router and coming in on an interface with the crypto map applied and VSA as the crypto engine.

  Workaround: Disable VSA and use software encryption.

- CSCtq86515

  Symptoms: UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.

  Conditions: This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.

  Workaround: Do not drop traffic on the device sending the UDP Jitter probe.

- CSCtq90577

  Symptoms: A router crashes when removing Netflow.

  Conditions: The symptom is observed when removing Netflow.

  Workaround: There is no workaround.

- CSCtq91176

  Symptoms: When the Virtual-PPP interface is used with L2TP version 2 and the topology uses an L2TP Tunnel Switch (LTS) (multihop node) and L2TP Network Server (LNS), and PPP between the client and LNS does renegotiation, then the PPP session cannot be established.

  Conditions: This symptom occurs when the LTS forwards the call based on the domain or full username from the PPP authentication username, and the LNS does PPP renegotiation.

  Workaround 1: Disable lcp renegotiation on the LNS and clear the L2TP tunnel at the LNS and LTS.

Workaround 2: Forward the call on the LTS using an L2TP tunnel name instead of the PPP username/domain name.

- CSCtq92182

  Symptoms: An eBGP session is not established.

  Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- CSCtq92940

  Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.

  Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

  Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.

  Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when bgp deterministic-med is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtr09251

  Symptoms: Continuous alignment errors and performance degradation in throughput of MS RPC traffic through the ZBFW.

  Conditions: The symptom is observed when inspecting MS RPC traffic through the ZBFW on a Cisco 2911 router that is running Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCtr11620

  Symptoms: In a simple HSRP setup with Cisco 2900 devices, a ping to the virtual IP address fails intermittently.

  Conditions: This symptom is observed when a Cisco 2911 is used.

Workaround: Replace the Cisco 2900 with a Cisco 18XX or Cisco 1941.

- CSCtr13172

  Symptoms: The **config replace** command crashes the router.

  Conditions: The symptom is observed when close to the maximum number of mediatrace and performance monitoring policies along with DMVPN are configured on the router and the target configuration contains none of these elements.

  Workaround: Uninstall the mediatrace and performance monitor policies prior to replacing the configuration.

- CSCtr14763

  Symptoms: A BFD session is always up, although the link protocol is down.

  Conditions: First the BFD session is up between the routers. After the VLAN is changed on the switch between the routers, the BFD peer is not reachable but the BFD sessions are always up.

  Workaround: There is no workaround.

- CSCtr15891

  Symptoms: On-demand DPD is being sent on every IPsec SA even though a response is seen on at least one of them.

  Conditions: Periodic DPD is configured, and multiple IPsec SAs exist with the peer with outbound traffic flowing on each of them without any inbound traffic.

  Workaround: There is no workaround.

- CSCtr18559

  Symptoms: An unallocated/unassigned number is received from PBX but as a response, a network congestion message is sent back. Gateway rejects call with 4# when actually its supposed to send a 7#.

  Conditions: The issue occurs only when the country Brazil is configured. When country is set to “itu”, then a 5# is sent which is correct for an unallocated/unassigned number. Follow this link to track cause code to CAs mapping sbased on selection of countries: http://www.pulsewan.com/data101/r2mfc.pd

  Workaround: There is no workaround.

- CSCtr20908

  Symptoms: A spurious access will occur on platforms that detect spurious accesses. A crash will occur on platforms that do not detect spurious accesses such as the Cisco ASR 1000, Cisco 3900 and 3900e.

  Conditions: The issue occurs when running the **show run all** command and when WEBVPN configurations are present.

  Workaround: Use the Cisco IOS 15.1(3)T train.

- CSCtr25821

  Symptoms: A Cisco 800 series router crashes with **isdn leased-line bri*0* 128** command:

  ```
  Unexpected exception to CPU: vector 1000, PC = 0x0 , LR = 0x8155A310
  ```

  Conditions: The symptom is observed with the **isdn leased-line bri*0* 128** command.

  Workaround: The issue does not occur if there is no cable that connects to the BRI interface. Disconnect the cable from the BRI interface while **isdn leased-line bri*0* 128** is configured.

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained 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-20120328-msdp

- CSCtr29338

  Symptoms: A router crashes.

  Conditions: The symptom is observed after an %ISDN-6-DISCONNECT message from “unknown” followed by a couple of “Illegal Access to Low Address” messages.

  Workaround: There is no workaround.

- CSCtr44686

  Symptoms: There is a crash after matching traffic and resetting the connection using following maps:

```
policy-map type inspect smtp SMTP_L7_P1
 class type inspect smtp SMTP_L7_C1
  reset
policy-map type inspect smtp SMTP_L7_P2
 class type inspect smtp SMTP_L7_C2A
  reset
 class type inspect smtp SMTP_L7_C2B
  reset
```

  Conditions: The symptom is observed with the above maps.

  Workaround: Replace “reset” with “log”.

- CSCtr45608

  Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.

  Conditions: The symptom is observed on a Cisco Catalyst 4000 Series Switch when “set vrf” is configured on the route-map and the VRF is IPv6 only.

  Workaround: Configure “ipv4 vrf” along with “ipv6 vrf” and refer “ipv6 vrf” on the route-map by configuring “ipv6 policy” on the ingress interface.

- CSCtr45633

  Symptoms: A BGP dynamic neighbor configured under VPNv4 address-family does not work correctly.

  Conditions: The symptom is observed when a BGP dynamic neighbor is configured under a VPNv4 address-family.

  Workaround: Add “dynamic neighbor peer-group” under “ipv4 unicast address-family”.

- CSCtr49064

  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh

- CSCtr51786

  Symptoms: The command **passive-interface** for a VNET auto-created subinterface x/y.z may remove the derived interface configuration command **ip ospf** *process id* **area** *number*. Consequently, putting back **no passive-interface** command will not form the lost OSPF ADJ.

  Conditions: The symptom is observed only with interfaces associated with the OSPF process using the command **ip ospf vnet area** *number*.

  Workaround: Associate the interface with the OSPF process using a network statement or using the interface command **ip ospf** *process id* **area** *number*.

  Further Problem Description: Interfaces associated with a process using a network statement under "router ospf" or interfaces configured with the command **ip ospf** *process id* **area** *number* are not affected.

- CSCtr54269

  Symptoms: CUBE sends an RTCP BYE message to MS OCS R2, causing loss of audio for about 20 seconds.

  Conditions: CUBE sends an RTCP BYE message only upon reINVITE due to session refresh timer.

  Workaround: Downgrade to Cisco IOS Release 12.4(22)YB.

- CSCtr58140

  Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.

  Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.

  Workaround: There is no workaround.

- CSCtr71465

  Symptoms: A router crashes at ipv4fib_les_switch_fastswitching_compat while booting.

  Conditions: The symptom is observed on a Cisco 888E router that is running Cisco IOS interim Release 15.1(2)T1.1 or later.

  Workaround: There is no workaround.

- CSCtr89322

  Symptoms: NME-RVPN module is not recognized by a Cisco 3900e router.

  Conditions: The symptom is observed with a Cisco 3900e router.

  Workaround: There is no workaround.

- CSCtr91106

  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCtr94887

  Symptoms: Using MRCP v1, VXML script with ASR operation will always receive noinput event.

  Conditions: The symptom is observed with Cisco IOS Release 15.2(1)T.

  Workaround: There is no workaround.

- CSCtr97640

  Symptoms: Start-up configuration could still be retrieved bypassing the “no service password-recovery’’ feature.

  Conditions: None.

  Workaround: None--Physically securing the router is important.

  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 1.9/1.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C

  CVE ID CVE-2011-3289 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

- CSCts20102

  Symptoms: NVRAM may lose or corrupt after router comes up.

  Conditions: The symptom is observed during stress testing.

  Workaround: Use the **wr erase** and then the **wr memory** commands if NVRAM corruption occurs.

- CSCts28462

  Symptoms: snmp-server host 1.2.3.4 traps version 2c public nhrp is reported as snmp-server host 1.2.3.4 traps version 2c public ds3.

  Conditions: Unknown.

  Workaround: There is no workaround.

- CSCts33952

  Symptoms: An rsh command fails from within TclScript. When rsh command constructs are used within TclScript, bad permissions are returned and the rsh aspect fails to execute, causing the script to fail.

  Conditions: This symptom is observed in Cisco IOS releases after 12.4(15)T14.

  Workaround: There is no workaround.

- CSCts39535

  Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.

Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path”, “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

Resolved Caveats—Cisco IOS Release 15.1(4)M1

Cisco IOS Release 15.1(4)M1 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M1 but may be open in previous Cisco IOS releases.

- CSCsl18054

  Symptoms: A local user created with a one-time keyword is removed after unsuccessful login attempts. A one-time user should be removed automatically after the first successful login, not after failed logins.

  Symptoms: This symptom occurs on a router running Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCso33003

  Symptoms: If a child policy is attached to a parent policy twice, the router will reload if the child policy configuration is removed.

  Conditions: The parent policy needs to be attached to the target interface.

  Workaround: Do not attach the same child policy twice in the same parent policy. Use a different policy instead.

- CSCtc11266

  Symptoms: The router undergoes a bus error crash. Before the crash, the following error messages are displayed:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
  %SYS-4-SNMP_WRITENET: SNMP WriteNet request.
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions: This symptom is observed on a router running Cisco IOS Release 12.4(22)T1 that is used as a zone-based firewall with no routing and VPN configured.

  ```
  outside---ASA firewall-----gig-IOS firewall-gig-----inside network
  ```

  Workaround: There is no workaround.

- CSCtd23069

  Symptoms: A crash occurs because of a SegV exception after configuring the **ip virtual-reassembly** command.

Conditions: This symptom is observed on a Cisco 7206VXR router that is configured as an LNS and that is running Cisco IOS Release 12.4(15)T7 and Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtd90030

  Symptoms: A Cisco 2851 router may crash with a bus error.

  Conditions: This symptom is observed when the function calls involve Session Initiation Protocol (SIP) and are possibly related to an IPCC server. This issue is seen with Cisco IOS Release 12.4(24)T1 or Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtf39056

  Symptoms: RRI route will not be deleted even after IPsec SA has been deleted.

  Conditions: This symptom was first observed on the Cisco ASR1k running Cisco IOS Release 12.2(33)XND, but is not exclusive to it. The conditions are still under investigation.

  Workaround: Reload the router to alleviate this symptom temporarily. One possible workaround would be set up an EEM script to reload the device at night. In this case, the reload should occur at 3:00 a.m. (0300) in the morning. For example (the syntax may vary depending on the versions used):

```
############
configure terminal
!
event manager applet SR_000000526
event timer cron name SR_000000526 cron-entry "0 3 * * *"
action 1 cli command "en"
action 2 cli command "reload"
!
end
############
```

- CSCtf71673

  Symptoms: A Cisco 10000 series router shows a PRE crash due to memory-corruption with block overrun.

  Conditions: This symptom is seen when the system is configured for PTA and L2TP access. The system is using a special based on Cisco IOS Release 12.2(34) SB4 during a pilot phase. Other systems in same environment that are using a widely deployed special based on Cisco IOS Release 12.2(31)SB13 have not shown this so far.

  Workaround: There is no workaround.

- CSCth20018

  Symptoms: On a Cisco ISR G2 or Cisco 8xx product line, unconfiguring a subinterface (via config CLI, for example, **no interface g0/0.100** or **no interface atm0/0.100**), may sometimes crash the system.

  Conditions: This symptom occurs during basic configuration.

  Workaround: Do not unconfigure a subinterface.

- CSCti53157

  Symptoms: If the console speed is changed, sometimes due to a change in speed, the characters are treated as break characters by Cisco IOS, and the system goes to ROMmon.

  Conditions: This symptom is seen if the console speed is changed.

  Workaround: There is no workaround. This caveat is Closed.

- CSCti64685

  Symptoms: User may not be able to configure SLA MPLS configuration.

  Conditions: This symptom occurs when the router is booted up and may be random.

  Workaround: There is no workaround.

- CSCtj15798

  Symptoms: Some modems in PVDM2-xxDM module are marked as BAD after running clean for few days. The **show modem** command will report a “B” in front of the modem (“B - Modem is marked bad and cannot be used for taking calls”).

  Conditions: The symptom is observed with the PVDM2-xxDM module.

  Workaround: Reloading the router gives a few more days of clean connections before the issue is seen again.

- CSCtj21045

  Symptoms: Header compression decodes RTP timestamp incorrectly.

  Conditions: This issue occurs mainly with IPHC format compression interacting with older Cisco IOS releases.

  Workaround: Use IETF format compression.

- CSCtj23189

  Symptoms: Packet drops occur on low-rate bandwidth guarantee classes even if the offered rate is less than the guaranteed rate.

  Conditions: This symptom occurs only when highly extreme rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with three classes: one with 16kbps, the second one with 1Mbps, and the third one with 99Mbps.

  Workaround: There is no workaround.

- CSCtj46670

  Symptoms: IPCP cannot be completed after the dialer interface is moved out of standby mode. CONFREJ is seen while negotiating IPCP.

  Conditions: The symptom is observed when a dialer interface has moved out from standby mode.

  Workaround: Reload the router.

- CSCtj57173

  Symptoms: The Cisco IOS Software crashes when processing a specially crafted DNS reply packet.

  Conditions: This symptom occurs when the router is configured for DNS server operations via the **ip dns server** command. This issue affects all versions of the Cisco IOS Software prior to first fixed software.

  Workaround: Disable the IP Name server functionality on the Cisco IOS Software.

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

  CVE ID CVE-2011-0958 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

- CSCtj78966

  Symptoms: A Cisco ASR 1000 router crashes with thousands of IKEv2 sessions, after many operations on IKEv2 session.

  Conditions: This symptom occurs when the IKEv2 SA DB WAVL tree is getting corrupted if you fail to insert the SA due to some error, for example, PSH duplication.

  Workaround: There is no workaround.

- CSCtj84234

  Symptoms: With multiple next-hops configured in the set ip next-hop clause of route-map, when the attached interface of the first next-hop is down, packets are not switched by PBR using the second next-hop.

  Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are PBR'd in hardware. This symptom is observed with route-map configuration, as given below:

```
route-map <RM name>
    match ip address <acl>
    set ip next-hop <NH1> <NH2>
```

  Workaround: There is no workaround.

- CSCtj87846

  Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

  Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.

  Workaround: Do a shut/no shut on PfR master or PfR border.

- CSCtj91149

  Symptoms: A delay of approximately 30 seconds is observed in a dynamic xconnect-based ISG session that comes up on standby, after it is up on active.

  Conditions: This symptom occurs on switchover.

  Workaround: There is no workaround.

- CSCtj91419

  Symptoms: When the reset push button is pressed and the default golden Cisco IOS image (*.default) is not present in flash, the push button status is not shown in "show platform boot-record" after Cisco IOS boots up.

  Conditions: This symptom is seen when the reset push button is pressed when ROMmon boots up, and the default golden Cisco IOS image should not be present in the flash.

  Workaround: Make sure .default Cisco IOS image is present in the flash whenever the reset push button is pressed. This caveat is Closed.

- CSCtj94510

  Symptoms: When sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), with one IKE session per VRF and four SA dual per session, a crash happens on Crypto_SS_process.

  Conditions: This symptom occurs when sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), with one IKE session per VRF and four SA dual per session.

  Workaround: There is no workaround.

- CSCtk09402

Symptoms: Bandwidth class may not get the correct bandwidth when policy map is configured.

Conditions: This problem is seen on Cisco 800 series routers (Cisco 886W, Cisco 887W) on the DSL interface.

Workaround: Fine tune using the **queue-limit** command. This will ensure the total bandwidth is available for the desired stream of traffic. Default queue-limit is 64 packets. Increasing it to 128 packets should solve the problem. This caveat is Closed.

- CSCtk18330

  Symptoms: MSCHAPv2 auth fails when matching the user/password pair is configured.

  Conditions: This symptom is observed when matching the user/password pair is configured.

  Workaround: There is no workaround.

- CSCtk53674

  Symptoms: An rtr running Cisco IOS Release 12.4(15)T14 and Cisco IOS Release 15.0M will crash when SNMPv3 configuration is removed.

  Conditions: This symptom occurs when the running configuration contains the following depending on the Cisco IOS Release:

  Cisco IOS Release 12.4(15)T14

  ```
  snmp-server user QOSqosuser1 QOSqosgroup v3 enc auth sha <DIGEST>
      priv aes 128 qosQOO!priv acc SNMP
  ```

  Cisco IOS Release 15.0(1)M4

  ```
  snmp-server user QOSqosuser1 QOSqosgroup v3 enc auth sha <DIGEST>
      priv aes 128 qosQOO!priv acc SNMP
  ```

  When you remove the above configuration using the **no snmp-server user** command, the rtr crashes.

  Workaround: There is no workaround.

- CSCtk58027

  Symptoms: The router crashes with the ip sla icmp jitter operation.

  Conditions: This symptom is observed when recreate steps have the ip sla icmp jitter operation with more number of packets running along with voice and data traffic running. When the status of the ip sla is OK, enter the **no ip sla schedule** command, and then enter the **no ip sla** *operation-number* command.

  Workaround: There is no workaround.

- CSCtk67073

  The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipsla.

- CSCtk67709

  Symptoms: The AnyConnect 3.0 package does not install correctly on the Cisco IOS headend. It fails with the following error:

  ```
  ssl2-uut-3845a(config)#crypto vpn anyconnect flash:anyconnect-win-3.0.0432-k9.pkg
  ```

```
SSLVPN Package SSL-VPN-Client (seq:1): installed %%Error: Invalid Archive
```

Conditions: This symptom is observed with AnyConnect 3.0.

Workaround: There is no workaround.

- CSCtk67934

  Symptoms: A Cisco router is forced to reload after a few days of encryption and decryption while processing high traffic.

  Conditions: This symptom is observed when VSA is enabled as a hardware crypto engine used for processing both firewall and encryption/decryption on the same interface.

  Workaround: Switch from VSA HW crypto engine to either SW crypto engine or VAM2+ HW crypto engine.

- CSCtk74660

  Symptoms: The Network Time Protocol (NTP) tries to resync after the server clock changes its time and after the NTP falls back to the local clock.

  Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.

  Workaround: There is no workaround.

- CSCtl04432

  Symptoms: The **show power inline fastethernet** command will show the interfaces that do not support power over ethernet. On Cisco 88xW platforms, PoE is supported only on FE0 and FE1.

  Conditions: This symptom happens on Cisco 88x series routers that are running Cisco IOS Release 15.1(4)M1.

  Workaround: There is no workaround. This caveat is Closed.

- CSCtl20993

  Symptoms: The router crashes during IPSec rekey.

  Conditions: The conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtl43156

  Symptoms: When using a BVI interface configured for IPv6 on a Cisco ISR-G2 series router, IPv6 neighbors are never discovered over the BVI. Neighbors will never be seen in the **show ipv6 neighbors** output and all traffic to/through the BVI will fail.

  Conditions: This symptom occurs when IPv6 is configured on Cisco ISR-G2 router images running on the “datak9” package.

  Workaround: Use the “uck9” technology package, where the IPv6 feature is already present.

- CSCtl44103

  Symptoms: The Cisco 3945 router that is running Cisco IOS Release 15.1(3)T has a zone-based firewall configured.

  Conditions: This symptom occurs when using any of the following three debug commands:

  - **debug policy-map type inspect events**
  - **debug policy-firewall events**
  - **debug ip inspect events**

  This symptom crashes the router immediately.

Workaround: There is no workaround.

- CSCtl45307

  Symptoms: BOOTP requests are not forwarded by the router.

  Conditions: This symptom occurs with BOOTP requests.

  Workaround: There is no workaround.

- CSCtl45684

  Symptoms: A Cisco device may crash due to “CPU Signal 10” preceded by the following messages in the logs:

  ```
  ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 726
  ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 30
  ```

  Conditions: This symptom is observed only when the HWIC-4SHDSL-E card is present in the router.

  Workaround: There is no workaround.

- CSCtl53899

  Symptoms: SIP to SIP calls through CUBE may cause memory corruption when resource priority passthrough is enabled on the dial peers.

  Conditions: This symptom is observed on CUBE with Cisco IOS Release 15.1(3)T, where the following was configured under the SIP dial peers:

  ```
  voice-class sip resource priority mode passthrough
  ```

  Workaround: Disable memory lite allocations using the **no memory lite** command. This will increase the size of memory allocations, so be careful when using it on a device with high memory utilization.

- CSCtl54415

  Symptoms: A Cisco router or switch may reload.

  Conditions: This symptom is experienced on multiple platforms when single-connection timeout is configured under an aaa group server, and there is no TACACS key configured:

  ```
  aaa group server tacacs+ <NAME>
      server-private x.x.x.x single-connection timeout 2
      server-private x.x.x.x single-connection timeout 2
      ip tacacs source-interface Loopback0
  (no tacacs-server key configured)
  ```

  Workaround: Either configure the correct matching key or do not configure single-connection timeout.

- CSCtl58005

  Symptoms: Accounting delay start is sent before any NCP has been negotiated, with “aaa accounting delay-start” configured. According to PRD, accounting start should not be sent until first NCP has been negotiated.

  Conditions: This symptom occurs when “aaa accounting delay-start” is configured.

  Workaround: There is no workaround.

- CSCtl70143

  Symptoms: LAC does not forward a PPP CHAP-SUCCESS message from LNS to the client sometimes.

Conditions: This symptom is seen when T1/PRI is used between the client and LAC.

Workaround: There is no workaround.

- CSCtl73914

  Symptoms: A Cisco 2921 Gateway that is running Cisco IOS Release 15.1(1)T1 is unable to register with IMS.

  Conditions: This symptom is observed if the P-Associated-URI of the 200 Ok response contains any special characters (!*.!) in Tel URI Parsing.

  Workaround: There is no workaround.

- CSCtl78285

  Symptoms: In a VRF configuration, rd cannot be added after deleting rd configuration once:

```
A-SUP5-6509E#sho run | be vrf
ip vrf CUST1
    rd 1:1
    route-target export 1:1
    route-target import 1:1
    mdt default 239.39.39.39

A-SUP5-6509E(config)#ip vrf CUST1
A-SUP5-6509E(config-vrf)#no rd 1:1
% "rd 1:1" for VRF CUST1 scheduled for deletion
```

  Wait and try to add rd again (for more than 2 hours).

```
A-SUP5-6509E(config)#ip vrf CUST1
A-SUP5-6509E(config-vrf)#rd 1:1
% Deletion of "rd" in progress; wait for it to complete
A-SUP5-6509E(config-vrf)#
```

  Conditions: This symptom is seen in a VRF configuration with rd.

  Workaround: Remove the VRF configuration and add it again.

- CSCtl79627

  Symptoms: The Cisco 891W router stops accepting new connections via SSL VPN, SSH, Telnet, and HTTP due to a memory leak, which results in memory depletion on the router.

  Conditions: This symptom is observed on a Cisco 891W router running the latest Cisco IOS Release 15.1(3)T.

  Workaround: There is no workaround.

- CSCtl81133

  Symptoms: A Cisco CUBE router using SIP TLS will crash if the outgoing SIP TLS connection attempts from CUBE to another endpoint do not successfully negotiate.

  Conditions: This symptom occurs on CUBE running Cisco IOS Release 15.1(3)T, using SIP TLS, and SIP options keepalive between CUBE and a third-party SIP device. Outgoing TCP connections from CUBE are accepted by the third-party device, but then closed shortly following the TLS client hello message from CUBE.

  Workaround: There is no workaround.

- CSCtl94813

  Symptoms: When using iLBC, the VG224 fails to play audio out the FXS port. The call uses iLBC when the analogue phone on the VG224 attends a conference bridge. It causes one-way audio.

  - When the IP capture is decoded from the VG224, the iLBC audio packet received and sent to the VG224 Fast Ethernet interface is clearly seen.
  - For the same call, the PCM trace shows no audio in the RIN stream.

  Conditions: This symptom occurs with Cisco IOS Release 15.1(2)17T. As per the HPI logs, the Cisco IOS does not send any packets to the dsp:

```
*Mar 10 23:36:54.988: //1944/9948BD1D87E7/HPI/[0/1:1]/hpi_receive_query_rx:
   Got RX stats
   Packet details:
    Packet Length=188, Channel Id=1, Packet Id=200
    RX Packets=0: Signaling=0, ComfortNoise=0
    Receive Duration=129180(ms): Voice=0(ms), FAX=0(ms)
    Packet Counts: OOSequence=0, Bad header=0, Late=0, Early=0Receive
inactive duration=129(ms)
```

  Workaround: Downgrade the Cisco IOS to Cisco IOS Release 12.4(4)T8.

- CSCtl95752

  Symptoms: HWIC-4SHDSL-E reports erroneous EOC and PBO values over time.

  Conditions: This symptom is observed when the HWIC-4SHDSL-E port is connected to the Alcatel-Lucent DSLAM.

  Workaround: There is no workaround.

- CSCtn00405

  Symptoms: A Cisco router may crash when “isdn test call” is run.

  Conditions: This symptom has been experienced on multiple IOS versions, including Cisco IOS Release 12.4(15)10, 12.4(24)T4, and 15.0(1)M4.

  Workaround: There is no workaround.

- CSCtn02428

  Symptoms: In “show mem alloc tot”, the top allocators are “CCE DP SIP Tx” and “FW SIP SESS WRAP”:

```
Allocator PC Summary for: Processor
Displayed first 2048 Allocator PCs only

PC           Total        Count        Name
0x63DE1B14   163317100    10236        CCE DP SIP Tx
0x64713A20   23784460     241386       FW SIP SESS WRAP
...
```

  Conditions: This symptom is observed during ZBF + SIP traffic.

  Workaround: There is no workaround.

- CSCtn04686

  Symptoms: When MHSRP is configured and the hello packets are passing through Etherchannel, and the cables connected to the Etherchannel port are unlugged/plugged, the MHSRP hello packets are not received on the Etherchannel interface.

  Conditions: This symptom is observed on a Cisco 3845 router running Cisco IOS Release 15.0(1)M4.

  Workaround: Unplug/plug the cables.

- CSCtn08208

  Symptoms: Clicking on the Citrix bookmark causes multiple windows of the browser to open. The web page tries to refresh itself a few times, and finally the browser window hangs.

  Conditions: This symptom occurs when upgrading to Cisco IOS Release 15.0(1)M4.

  Workaround: Downgrade to Cisco IOS Release 15.0(01)M2.4.

- CSCtn15317

  Symptoms: Traffic on MPLS VPN is dropped. When you check LFIB information on the P router, the entry has an instruction to TAG all packets that are destined to the PE router instead of a POP instruction which is expected on a directly connected P.

  Conditions: This symptom occurs with the following conditions:

  – The ISIS protocol is running as IGP on MPLS infrastructure.
  – ISIS on the PE router is summarizing network that includes BGP vpnv4 update-source.
  – The P router is running an MFI-based image.

  Workaround 1: Remove the **summary-address** command in ISIS on PE.

  Workaround 2: Change the BGP update source.

- CSCtn19178

  Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working vrf “A” and a new local label will not be reassigned.

  Conditions: This symptom occurs on the MPLS Edge LSR when you remove the configuration of an unused vrf “B”, including:

  – The vrf interface, for example, **no interface Gi1/0/1.430**.
  – The same vrf process, for example, **no router ospf** *process id* vrf *vrf name*.

  Run the following commands to verify whether you are facing this issue:

  – **show ip bgp vpnv4 vrf A** *subnet* (this is for the working vrf)
  – **show mpls forwarding-table labels** *local label*

  Workaround: To reprogram a new local label on the PE router, clear the MP-BGP session by using either of the following commands:

  – **clear ip bgp** *mp-bgp neighbor* **soft in**
  – **clear ip bgp** *mp-bgp neighbor* **soft out**

- CSCtn19496

  Symptoms: Packet loss is seen when the service policy is applied on the tunnel interface. The **show hqf interface** command output shows drops in a particular queue with the following:

  ```
  Scheduler_flags 177
  ```

  The above value of 177 indicates an ATM driver issue. Once the issue is seen, the tunnel interface transitions to the down state.

  Conditions: This symptom is observed when the service policy is applied on the tunnel/GRE interface, and when the source of the tunnel interface is the ATM interface(hwic-shdsl)

  Workaround: There is no workaround.

  Further Problem Description: The above-described symptom is seen only with the SHDSL link.

- CSCtn26785

  Symptoms: Incoming traffic on DS3 atm 1/0 is process-switched:

```
3845#sh int atm 1/0 stat
ATM1/0
    Switching path       Pkts In       Chars In       Pkts Out      Chars Out
         Processor         98170       10995040              1             68
      Route cache              0              0          98170       10995040
            Total          98170       10995040          98171       10995108
3845#

3845#sh cef int atm 1/0
ATM1/0 is up (if_number 5)
    Corresponding hwidb fast_if_number 5
    Corresponding hwidb firstsw->if_number 5
    Internet address is 64.65.248.174/30
    ICMP redirects are never sent
    Per packet load-sharing is disabled
    IP unicast RPF check is disabled
    Input features: Ingress-NetFlow
    Output features: Post-Ingress-NetFlow
    IP policy routing is disabled
    BGP based policy accounting on input is disabled
    BGP based policy accounting on output is disabled
    Hardware idb is ATM1/0
    Fast switching type 9, interface type 138
    IP CEF switching enabled
    IP CEF switching turbo vector
    IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
    Input fast flags 0x0, Output fast flags 0x0
    ifindex 5(5)
    Slot Slot unit 0 VC -1
    IP MTU 4470
3845#
```

  Conditions: The conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtn32323

  Symptoms: 802.1p information is not set on local generated traffic when bridge-dot1q is used on the DSL lines.

  Conditions: Configure the device to transport 802.1p information over a DSL link connection, considering different CoS values for LAN and local generated traffic on the router.

```
interface ATM0.y point-to-point
  bridge-group <x>
  pvc 1/199
    bridge-dot1q encap <vlan>
    service-policy out <egress-policy>
```

  Workaround: There is no workaround.

- CSCtn38996

  Symptoms: All MVPN traffic is getting blackholed when a peer is reachable using a TE Tunnel, and an interface flap is done so that a secondary path can be selected. The multicast route does not contain a native path using the physical interface.

  Conditions: This symptom is seen when **mpls traffic-eng multicast-intact** is configured under OSPF.

  Workaround: Issue the **clear ip ospf process** command on the core router.

- CSCtn39632

  Symptoms: The RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.

  Conditions: This symptom occurs on a Cisco ASR 1000 series router configured for RSA key encryption with a keyring name having more than eight characters.

  Workaround: Modify the keyring name to be less than eight characters.

- CSCtn48744

  Symptoms: Memory leaks on OER border router while running the PfR-IPSLA configuration.

  Conditions: This symptom is seen on a Cisco 7200 router that is running Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCtn53094

  Symptoms: The router crashes or generates the following error:

  ```
  %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 8796350. -Process=
  "Mwheel Process", ipl= 2, pid= 315
  ```

  Conditions: This symptom is observed when toggling very fast between the **ip pim** *mode* and **no ip pim** commands on an interface when that interface is the only one where PIM is being enabled. The most common way this can happen in a production network is through the use of “config replace”, which results in the toggling of the command from ON to OFF and then ON on a different interface.

  Workaround: Avoid fast toggling of the **pim** *mode* command if possible when it is only present on a single interface.

- CSCtn57655

  Symptoms: A Cisco router running Cisco IOS Release 15.0M crashes during a SIP call.

  Conditions: This symptom occurs when a Cisco router is running Cisco IOS Release 15.0M. This issue occurs only when the “callmonitor” CLI under “voice service voip” is configured.

  Workaround: There is no workaround.

- CSCtn61834

  Symptoms: NAT-T keepalive cannot send out cause NAT translation timeout.

  Conditions: This symptom is seen when the NAT translation table is getting timeout since no NAT keepalive message is received.

  Workaround: There is no workaround.

- CSCtn63109

  Symptoms: After reload or on a freshly upgraded router, Ping fails when the MTU is set above 1500 bytes on the FastEthernet 4 - WAN interface of a Cisco 800 series router connected directly to another router.

  ```
  Router# ping 10.1.1.1 rep 5 df-bit size 1650
  Type escape sequence to abort.
  Sending 5, 1650-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
  Packet sent with the DF bit set
  .....
  ```

Conditions: This symptom is only observed with Cisco IOS Release 15.0(1)M4 and is specific only to Cisco 800 series routers. To be specific, only the Cisco 881SRST router is found faulty with the IOS, that is, c880voice-universalk9-mz.150-1.M4.bin so far. This issue is consistently seen with subinterface configurations based on the Fa4 interface.

Also, the following Traceback is noticed:

```
*Feb 28 15:26:19.639: %LINK-4-TOOBIG: Interface FastEthernet4, Output packet
size of 1664 bytes too big, -Traceback= 0x81056958z 0x81056EF8z 0x8112CBF4z
0x8200073Cz 0x82001264z 0x82001978z 0x820019D4z 0x8201BBF4z 0x8201C16Cz
0x8203F5C8z 0x8203FDACz 0x82D86B9Cz 0x81A1DC70z 0x819E6FD8z 0x819F6114z
0x8128C0CCz
```

Workaround: Remove and reconfigure MTU on the interface.

- CSCtn63325

  Symptoms: The Cisco 1841 router crashes during firmware upgrade.

  Conditions: This symptom occurs when microcode CLI is used during firmware upgrade on the Cisco 1841 router.

  Workaround: There is no workaround.

- CSCtn68643

  Symptoms: OSPFv3 hellos are not processed and neighbors fail to form.

  Conditions: This symptom occurs when configuring OSPFv3 IPsec authentication or encryption.

  ```
  ipv6 ospf encryption ipsec spi 500 esp null sha1
  1234123412341234123412341234123412341234
  ```

  or

  ```
  ipv6 ospf authentication ipsec spi 500 md5 abcdabcdabcdabcdabcdabcdabcdabcd
  ```

  Workaround: There is no workaround.

- CSCtn70367

  Symptoms: The IPSEC key engine crashes at sessions setup.

  Conditions: This symptom is observed when setting up sessions with the configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. The crash happens on the IPSEC key engine. The crash occurs while UUT is establishing SAs that are requested. This issue is reproduced by clear crypto session on CES after all SAs are established.

  Workaround: There is no workaround.

- CSCtn72853

  Symptoms: Crash/watchdog timeout occurs at udb_classify_child.

  Conditions: This symptom occurs due to various triggers like applying service-policy changes to complex level 2 or 3 policies where the same child/grand-child policy is used multiple times in the same parent.

  Workaround: There is no workaround.

- CSCtn72939

  Symptoms: The L2tpv3 feature is not working on Cisco c181x platforms.

  Conditions: This symptom occurs with Cisco c1812 running Cisco IOS Release 15.(0)M and later releases.

  Workaround: Configure bridge-group under that xconnect interface.

- CSCtn76183

  Symptoms: A Cisco router configured for SIP NAT processing may crash.

  Conditions: This symptom is observed while processing a SIP message from Cisco SPA phones (509, 524) in the inside network side.

  Workaround: Use Cisco IOS Release 12.4(24)T3.

- CSCtn77211

  Symptoms: Spurious memory access occurs at cce_dp_ipc_cache_classify at bootup.

  Conditions: This symptom is observed when IPv6 SLA probes are configured, along with the firewall.

  Workaround: There is no workaround.

- CSCtn87012

  Symptoms: FXS ports that are SCCP-controlled stay in the “ringing” state, and the DSP thermal alarm pops up.

  Conditions: This symptom is observed on a Cisco VG200 series voice gateway running Cisco IOS Release 15.0(1)M4 if the phone is answered during the ringing ON cycle.

  Workaround: Pick up the phone during the ringing OFF cycle.

- CSCtn90673

  Symptoms: The Cisco 887 router crashes when sending baby jumbo frames downstream over the VDSL line.

  Conditions: This symptom is observed when the VDSL interface, “interface e0”, is configured for Pppoe, a subinterface (that is, vlans), and an output service policy on interface e0. This issue is seen when an etherswitch interface is configured for trunking and baby jumbo frames or jumbo frames are sent downstream to the router. There is bidirectional traffic and the etherswitch vlan is then shut.

  Workaround: Do not send baby jumbo frames or jumbo frames downstream to the Cisco 887 router. Do not shut the etherswitch vlan interface(s) when the router is routing traffic.

- CSCtn91807

  Symptoms: A router acting as a voice gateway may crash due to a bus error.

  Conditions: This symptom occurs when a button is pressed on a phone while using skinny. However, the exact conditions that cause this symptom are currently unknown.

  Workaround: There is no workaround.

- CSCtn96521

  Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.

  Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.

  Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.

- CSCtn97451

  Symptoms: The bgp peer router crashes after executing the **clear bgp ipv4 unicast** *peer* command on the router.

  Conditions: This symptom occurs with the following conditions:

  ```
  Router3 ---ebgp--- Router1 ---ibgp--- Router2
  ```

ROUTER1:

```
--------

interface Ethernet0/0
    ip address 10.1.1.1 255.255.255.0
    ip pim sparse-mode
!

router ospf 100
    network 0.0.0.0 255.255.255.255 area 0
!

router bgp 1
    bgp log-neighbor-changes
    network 0.0.0.0
    neighbor 10.1.1.2 remote-as 1
    neighbor 10.1.1.3 remote-as 11 !
```

ROUTER2:

```
--------

interface Ethernet0/0
    ip address 10.1.1.2 255.255.255.0
    ip pim sparse-mode
!
router ospf 100
    redistribute static
    network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
    bgp log-neighbor-changes
    network 0.0.0.0
    redistribute static
    neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

ROUTER3:

```
-------

interface Ethernet0/0
    ip address 10.1.1.3 255.255.255.0
    ip pim sparse-mode
!

router bgp 11
    bgp log-neighbor-changes
    network 0.0.0.0
    network 0.0.0.0 mask 255.255.255.0
    redistribute static
    neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

Crash reproduce steps are as follows:

1. Traffic travel from ROUTER3 to ROUTER2.
2. “clear bgp ipv4 unicast 10.1.1.1” on ROUTER2.

Workaround: There is no workaround.

- CSCto02448

  Symptoms: On doing an inbound route refresh, the AS-PATH attribute is lost.

  Conditions: This symptom is observed with the following conditions:

  1. The neighbor is configured with soft-reconfiguration inbound.
  2. The inbound routemap is not configured for the neighbor.
  3. The non-routemap inbound policy (filter-list) allows the path.

  Workaround: Instead of using the non-routemap inbound policy, use the routemap inbound policy to filter the prefixes.

- CSCto03446

  Symptoms: When a flat bandwidth policy is attached to a serial subinterface via frame-relay map-class, all packets are dropped and no traffic goes through.

  Conditions: This symptom occurs with a flat policy attached to a frame-relay interface with traffic shaping enabled.

  Workaround: Remove traffic shaping from the interface and attach a hierarchical policy.

- CSCto03506

  Symptoms: The Gigabit Ethernet 0/2 interface on Cisco c3900 platforms is not seen by applications using snmp.

  Conditions: This symptom occurs when Gigabit Ethernet 0/2 interface is not seen when you use the **snmpwalk** command.

  Workaround: There is no workaround.

- CSCto07586

  Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.

  Conditions: This symptom occurs with the following conditions:

  1. Create a Cisco IOS image that does not have IPV6 enabled.
  2. Enable BFD on an interface.
  3. Configure an IPV4 static route with BFD routing through the above interface.

  The IPV4 BFD session does not get established, so the static route does not get installed.

  Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

- CSCto11025

  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.

- CSCto13254

  Symptoms: Anyconnect fails to connect to a Cisco IOS headend. The Anyconnect event log shows the following error:

  ```
  Hash verification failed for file <temp location of profile>
  ```

  Conditions: This symptom is observed with Anyconnect 3.x when connecting to a Cisco IOS headend that is configured with a profile.

  Workaround: Remove the profile from the Cisco IOS headend.

- CSCto14435

  Symptoms: A Cisco 7200 router with a C7200-VSA module may crash when the tunnel interface is enabled.

  Conditions: This symptom is observed on a Cisco 7200 router with a C7200-VSA module enabled. This issue is seen with Cisco IOS Release 12.4(24)T4 and Cisco IOS Release 15.0(1)M.

  Workaround: Disable ip route-cache and ip route-cache cef on the tunnel source interface.

- CSCto23807

  Symptoms: A Cisco device crashes when trying to transfer a call.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(1)T2.

  Workaround: There is no workaround.

- CSCto24338

  Symptoms: Router reload occurs due to the following bus error when the processor reads data from an invalid memory location:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC =
  0xXXXXXXXX
  ```

  Conditions: This symptom occurs with NAT+SIP.

  Workaround: Disable the NAT SIP multipart processing by executing the **no ip nat service allow-multipart** command.

- CSCto31265

  Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.

  Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.

  Workaround 1: Delete/readd the static route that generates Type7.

  Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

  Workaround 3: Execute **clear ipv6 ospf redistribution** command on ASBR.

- CSCto34196

  Symptoms: When two Cisco 3945E routers are connected to each other and an IPSec VPN tunnel is established between them, any kind of traffic passing through the VPN tunnel takes about 10 milliseconds as Round Trip Time in case the Onboard Encryption Engine is used.

  Conditions: This symptom occurs only when that traffic is encrypted by the Onboard Encryption Engine of Cisco 3945E (SPE250). After replacing the routers to Cisco 3945 (SPE150), the RTT is shorter than the one of Cisco 3945E.

  Workaround: Use software encryption.

- CSCto42752

  Symptoms: Removing the existing static policy and applying it back or adding the policy under that interface if it does not exist results in an error on standby.

  Conditions: This symptom occurs when customers use high availability.

  Workaround: Using the non-HA or standalone routine will fix the problem.

- CSCto45019

  Symptoms: The router crashes when you remove the dialer interface and readd it and configure an IP address.

  Conditions: This symptom occurs if you have continuous traffic passing through the router and going out of the dialer interface, and if you remove the dialer interface and readd it and then configure an IP address.

  Workaround: Before configuring an IP address, configure encapsulation ppp or frame-relay but not hdlc.

- CSCto46716

  Symptoms: Routes over the MPLS TE tunnel are not present in the routing table.

  Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In “debug ip ospf spf”, when the SPF process link for the TE tunnel is in its own RTR LSA, the “Add path fails: no output interface” message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.

  Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto47524

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs responder. A **show process memory sorted** command may initially show “MallocLite” growing. By disabling malloclite with the following, one may start to see the process “IP SLAs Responder” growing.:

  ```
  config t
  no memory lite
  end
  ```

  In at least one specific case, the leak rate was 80mb per day.

  Conditions: This symptom is observed on a Cisco ASR 1002 router.

  Workaround: Disable IP SLA on affected router, if possible.

- CSCto50255

  Symptoms: Memory leak occurs while running the UDP echo operation.

Conditions: This symptom is observed when an UDP echo operation successfully runs. The leak is seen on every hundredth run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way to capture it is by monitoring and decoding the PC via the **show processes memory** *pid* command.

Workaround: There is no workaround.

- CSCto53332

  Symptoms: A router configured for IPSEC accounting may display the following error message:

  ```
  %AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
  ```

  This does not seem to result in any impact apart from intermittently lost accounting messages.

  Conditions: This symptom occurs when ipsec accounting is active.

  Workaround: There is no workaround.

- CSCto55708

  Symptoms: There is a build error due to a missing ‘ ” ’ in a printf statement, only in dsgs, due to compiler-specific issues.

  Conditions: This symptom occurs due to a missing ‘ ” ’ in a printf statement only in dsgs due to compiler-specific issues.

  Workaround: There is no workaround.

- CSCto63417

  Symptoms: A spurious access or crash occurs after applying the service policy.

  Conditions: This symptom occurs specifically when applying service-policy type access-control. This issue occurs when a large amount of traffic is being sent to the interface. The class-map uses RegEx in the match statement.

  For example:

  ```
    class-map type access-control match-any bittorrent
      match start l2-start offset 54 size 32 regex "GETinfo_hash="
      match start l2-start offset 54 size 32 regex
  "[a|A][z|Z][v|V][e|E][r|R]
  ```

  Workaround: Apply the service policy during low traffic or do not use RegEx in match statements.

- CSCto63954

  Symptoms: A router with GETVPN configurations is continuously crashing.

  Conditions: This symptom is seen with GETVPN-related configurations with the fail-close feature activated.

  Workaround: There is no workaround.

- CSCto68554

  The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features.

  These vulnerabilities are:

  – Memory leak in Cisco IOS Software

  – Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are not available.

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw.

- CSCto69071

  Symptoms: Metrics collection fails due to invalid DVMC runtime object handle.

  Conditions: This symptom occurs when the transport layer is not passing up an interface type that is acceptable to DVMC.

  Workaround: There is no workaround.

- CSCto71744

  Symptoms: FXO interfaces with the cable-detect feature enabled will automatically transition to the off-hook state when no PSTN battery voltage is detected, and remain off-hook for a duration of up to 1 minute. This condition violates regulatory telecom standards in several countries, including but not limited to the USA and Canada.

  The failing clauses of regulatory standards are as follows:

  - TIA-968-B 5.1.11.3
  - TIA-968-B 5.1.12.3
  - Industry Canada CS-03 Part I, Issue 9 December 2010

  Conditions: This symptom occurs when the FXO interface is up, and the cable is connected to PSTN. Any interruption of the PSTN battery to FXO induces the off-hook condition, and the port does not transition back to on-hook for up to 1 minute.

  Workaround: Disable the cable-detect feature in the FXO <config-voiceport> prompt. You can enable the feature in topologies that are not subject to regulatory standards (that is, on-premise installations).

- CSCto75350

  Symptoms: A crash occurs at udb_classify.

  Conditions: This symptom occurs when level 3 HQoS is configured. The second-level policy from under class-default is removed. This is followed by traffic, either self-generated through IP SLA or possibly through data traffic traversing.

  Workaround: There is no workaround.

- CSCto81814

  Symptoms: When SSH is attempted over an IKEv2 tunnel using ECDSA certificates, the router crashes.

  Conditions: This symptom is only observed when ECDSA certificates are used for IKEv2, and not with RSA certificates or with IKEv1.

  Workaround: There is no workaround.

- CSCto86833

  Symptoms: The router's CPU spikes to 100 percent, leading to voice call failures, among other problems.

  Conditions: This symptom occurs with the Cisco 3945e router configured with SRST (call-manager-fallback) to the maximum supported capacity of 1500 phones, 2500 DNs with octo-line capability, and PRI interfaces controlled via ccm-manager. Under these conditions, MGCP call processing consumes significant amount of CPU. Even at 0.5cps MGCP call arrival rate, the router's average CPU will be around 50 to 60 percent.

Workaround: If possible, reduce the number of voice ports automatically generated by the number DNs and octo-line. Also, if possible, use dual-line support instead. The lower the number of voice ports, the lower the CPU impact of this defect. Use the **show voice port summary** command to view the total number of voice ports created on the router after SRST configuration.

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip

- CSCtq25682

  Symptoms: The router crashes after configuring “gw-accounting file”.

  Conditions: This symptom occurs if the router’s memory usage is already over 80 percent utilization, and after configuring “gw-accounting file”, the following log message is displayed:

  ```
  %VOICE_FILE_ACCT-4-MEM_USAGE_HI_WATERMARK: System memory on high usage
  (81/100). Stopping processing new event log for now.
  ```

  After this log, when the cdrflush-timer expires, the router crashes.

  Workaround: Do not enable “gw-accounting file” when the router’s memory utilization is already over 80 percent.

- CSCtq35297

  Symptoms: Cisco c880 images do not get compiled.

  Conditions: This symptom occurs during compilation of Cisco c880 images.

  Workaround: There is no workaround.

- CSCtj29382

  Symptoms: When cellular interface passes packets and users configure “tx-ring-limit” on cellular interface, the system crashes.

  Conditions: This symptom occurs under the following conditions:

  1. Traffic runs through cellular interface.
  2. 2. Change “tx-ring-limit” on cellular interface with traffic running in the background.

  Workaround: Stop the traffic and change “tx-ring-limit”.

- CSCtn19027

  Symptoms: The **show mediatrace responder sessions brief** command crashes the router.

  Conditions: This symptom is observed on Mediatrace Responder when showing a stale session.

  Workaround: There is no workaround. Avoid issuing this impacted **show** command.

- CSCto77537

  Symptoms: Calls between SME-CUBE fail due to no audio path when the originating leg is G729r8 and the CUBE preferred codec list contains g729br8.

Conditions: This symptom occurs under the following conditions:

- CUBE ISR: c3845-ipvoicek9-mz.151-4.M
- There is no audio path after call setup. The call either disconnects (case SIP-H323) or stays up without voice path (case SIP-SIP).

The call flow is as follows:

```
OriginatingCluster--> SAF SIP Trunk ---> SME ---> CUSP --> CUBE (originating)
--> CUSP <--------->
CUSP --> CUBE (Terminating) --> CUSP --> SME --> SAF H323 Trunk --->
TerminatingCluster

CUBE codec Config:
    voice class codec 1
    codec preference 1 g729r8
    codec preference 2 g729br8
    codec preference 3 g711ulaw
    codec preference 4 g722-64
```

Workaround 1: Remove the g729br8 codec in the voice-class codec config on CUBE to ensure that CUBE will offer only g729r8 in the outgoing offer.

Workaround 2: Change the Originating SME, SIP trunk to Originating CUBE from DelayOffer to EarlyOffer.

Workaround 3: Configure a transcoder.

- CSCtq64951

  Symptoms: The following message is displayed:

  ```
  %CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto
  functionality with securityk9 technology package license.
  ```

  The **show platform cerm** command output shows all tunnels in use by SSLVPN.

  ```
    Number of tunnels      225
  ...
    SSLVPN   D      D     225     N/A
  ```

  The **show webvpn session context all** command output shows no or very few active sessions.

  ```
  WebVPN context name: SSL_Context

  Client_Login_Name  Client_IP_Address  No_of_Connections  Created Last_Used
  ```

  Conditions: This symptom occurs on SSLVPN running Cisco IOS Release 15.x. This issue is seen only on ISR G2 platforms.

  Workaround: Upgrade to Cisco IOS Release 15.1(4)M1 or later releases.

- CSCtq36726

  Symptoms: Configuring the **ip nat inside** command on the IPSEC dVTI VTEMP interface does not have any effect on the cloned Virtual-access interface. The NAT functionality is thus broken, because the V-access interface does not get this command cloned from its respective VTEMP.

  Conditions: This symptom is observed on Cisco ASR1006 (RP2/FP20) routers with ikev2 dVTI. This issue may be service impacting and is easily reproducible.

  Workaround: Reconfigure the Virtual-template interface such that the **ip nat inside** command is applied first, followed by other commands.

- CSCtn76183

  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

Open Caveats—Cisco IOS Release 15.1(4)M

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(4)

m. All the caveats listed in this section are open in Cisco IOS Release 15.1(4)M. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtr44373

  Symptoms: This is a platform independent issue. Users cannot receive a call through a BRI port. A fast tone will be heard.

  Conditions: This symptom is observed on a newly released image.

  Workaround: Configure forward digital all in the CLI.

  The following example shows a sample configuration:

  dial-peer voice 111 pots

  destination-pattern 111

  !direct-inward-dial

  port 2/0

  forward-digits all

Resolved Caveats—Cisco IOS Release 15.1(4)M

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(4)M. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsm23548

  Symptoms: The standby supervisor may crash when pasting in a crypto certificate on the active supervisor.

  Conditions: This symptom is observed in configuration mode when applying a certificate.

  Workaround: There is no workaround.

- CSCsr17680

  Symptoms: AA-request, sent to a particular server, getting failed-over to all other servers in the server group, when the first server is not responding or first server is unreachable.

  Conditions: This symptom is observed when sending a request to a particular server on a server-group.

  Workaround: There is no workaround.

- CSCsv30540

  Symptoms: The error message `%SYS-2-CHUNKBOUNDSIB` and a traceback are seen.

  Conditions: These symptoms are observed when the **show running-config/write memory** command is issued.

  Workaround: There is no workaround.

- CSCsx62864

  Symptoms: Active RP may reload due to IOSD failure if clear crypto session is done after attaching the gdoi crypto map.

  Conditions: This symptom is observed when the following actions are taken:

  3. remove the gdoi crypto map from the interface connected to the Key Server (KS)
  4. clear crypto sessions
  5. attach the crypto map again

  Now, if the crypto sessions are cleared, IOSD will restart and will result in an RP reload.

  Workaround: Avoid clearing crypto sessions after attaching a crypto map. Wait for the GM to send the registration in default manner and allow the KS to send the SAs.

- CSCsx65975

  Symptom: The router may reset unexpectedly during an ISSU process from RLS2 to RLS3.

  Conditions: This symptom is observed when all of the following conditions exist:

  1. SSH rsa keys are configured
  2. the RLS2 image does not have CSCsx65975 integrated
  3. the RLS3 image does not have CSCsz05125 integrated

  This symptom will not occur if the SSE keys are zeroized (removed). It will not occur if RLS2 has CSCsx65975 integrated; nor will it occur if RLS3 has CSCsz05125 integrated.

  Workaround: The workaround is only required if all three conditions above exist. Zeroize your SSE rsa keys before the ISSU process:

  ```
  asr1k(config)#crypto key zeroize rsa
  ```

  Then, after the ISSU process, create new keys:

  ```
  asr1k(config)#crypto key generate rsa
  ```

  Further Problem Description: Enter the **show ip ssh** command to determine whether SSE is enabled or disabled. (you cannot tell by entering the **show running configuration** command).

- CSCsy54233

  Symptoms: “Exception_reserve_memory” is invalid in a UNIX image.

  Conditions: This symptom is observed in a UNIX image, which do not support “exception_reserve_memory.”

  Workaround: There is no workaround.

- CSCsz18634

  Symptoms: An input/output rate is always displayed with “0” in interface status, even though packets are flowing on the ports normally.

  ```
  show int gig 4/1 output GigabitEthernet4/1 is up, line protocol is up (connected)
  ......
  Output queue: 0/40 (size/max) 30 second input rate 0 bits/sec, 0 packets/sec
  ```

```
<<<<<<<<<<< 30 second output rate 0 bits/sec, 0 packets/sec <<<<<<<<<<< 3411001
packets input, 567007874 bytes, 0 no buffer Received 818876 broadcasts (725328
multicasts)
```

Conditions: This symptom is observed on a Cisco 3750 that is running Cisco IOS Release 12.2(46)SE, as well as a Cisco 4500 and Cisco 4900M that are running Cisco IOS Release 12.2(46)SG and Cisco IOS Release 12.2(53)SG1.

Workaround: This issue is a cosmetic issue and does not affect the functionality of the switch or the traffic flow.

Use the value of the **show int gigx/y count detail** command to see the raw statistics.

The rate shown in the **sh int** command uses a complex convergence algorithm. If the rate changes from X to Y, it could take several minutes (15-30) for the rate to converge from X to Y. The rate must be steady and should be sent from a tester to confirm that the convergence is happening correctly.

Or, execute reload.

Further Problem Description: On the Cisco 3570 platform, the fix is in Cisco IOS Release 12.2(53)SE. On the Cisco 4500/4900M, the fix for this bug is scheduled to be in Cisco IOS Release 12.2(53)SG2 and Cisco IOS Release 12.2 (50)SG7.

- CSCsz29564

  Symptoms: ASR starts using the new SA as soon as it received. This causes traffic loss in the network.

  Conditions: This symptom is observed if a GM misses the rekey. Communication to this GM from the ASR fails because the ASR immediately begins using the new SA to encrypt, rather than waiting for the GM that missed the rekey to reregister.

  Workaround: There is no workaround.

- CSCsz35913

  Symptoms: An interface goes down in spite of carrier-delay configuration.

  Conditions: This symptom is observed on a PA-E3, when the serial interface carrier-delay is configured for one second and any of the alarms (AIS, LOF) are generated for less than or equal to one second.

  Workaround: Increase the carrier-delay.

- CSCsz44301

  Symptoms: NHRP is not registered to the root hub.

  Conditions: This symptom is observed after an RP switchover.

  Workaround: There is no workaround.

  Further Problem Description: During platform RP switchover, the root hub is not seeing NHRP registration messages from first-level hubs.

- CSCsz92328

  Symptom: None of the interfaces come up after SSO is done with configuration with self-signed certificates.

  Conditions: This symptom is observed under the following conditions:

  1. RSA self-signed certificate is generated on the router
  2. Router is reloaded
  3. SSO is done on the router

  Workaround: After reload, remove and add the self-signed certificate.

- CSCta02570

  Symptoms: The IOSd resets when 1500 dVTIs are brought up at the same time.

  Conditions: This symptom is observed when a large number of dVTIs are brought up at the same time.

  Workaround: There is no workaround.

- CSCta14505

  Symptoms: No source group (SG) entry forms in the network for PIM sparse-mode groups. This leads to traffic failures.

  Conditions: This symptom is observed when PIM-SM is configured in the network and traffic is sent for PIM-SM groups.

  Workaround: Shut down the upstream interface, remove the IP address, configure it again, then perform a **no shutdown** on the interface.

- CSCta22480

  Symptom: Memory leaks are not removed after reload on a Cisco ASR.

  Conditions: This symptom is observed after the following sequence of events:

  1. After making some stress calls, the **show mem deb leak summ** command is entered in order to see the memory leaks.

  2) The router is reloaded to remove the leaks.

  3) Once the router is up, the **show mem deb leak summ** command is entered again to check for leaks.

  Result: None of the memory leaks are removed.

  Workaround: There is no workaround.

  Further Problem Description: The **show mem deb leak summ** command is a debug command that is not used under normal router operations and that therefore does not affect normal router behavior.

- CSCta22746

  Symptoms: A Cisco ASR1000 may crash when a large number of DMVPN tunnels have been brought up and a user enters the **sh cry isakmp sa** command.

  Conditions: This symptom is observed on a Cisco ASR1K with RP2, configured as IPSec DMVPN Phase3 spoke, and when multiple routing protocols are configured for overlay routing.

  Workaround: There is no workaround.

- CSCta26520

  Symptoms: The following traceback is seen:

  ```
  %IDBINDEX_SYNC-3-IDBINDEX_LINK: Driver for IDB type 0 changed the Identity of
  interface “Tunnel1” without deleting the old Identity first
  ```

  Conditions: This symptom is observed when numerous tunnel interfaces are rapidly added and removed.

  Workaround: There is no workaround

- CSCtb20400

  Symptoms: A Cisco ASR may crash.

Conditions: This symptom is observed when certain IPv6 crypto configurations are unconfigured when configurations are copied from tftp to the running config. The problem is not seen when an actual CLI is used (as opposed to the **copy tftp running** command) on the router to unconfigure IPv6 IPSec. The problem also seems specific to RP2 since only the RP2 router has crashed so far. It does not seem to affect RP1.

- Workaround: Use CLI to unconfigure instead of configuring via the **copy tftp running** command.
- CSCtb42862

  Symptoms: A Cisco 3845 router crashes due to illegal memory access.

  Conditions: The symptom is observed in a scale testing environment which has eight key servers and 20 GM routers (simulating 2000 group members) and when there is unicast rekeying. The GM router crashes in steady state (no traffic). This seems to be intermittent.

  Workaround: There is no workaround.

- CSCtb74547

  Symptom: A Cisco ASR 1000 Series Aggregation Services router DMVPN HUB reloads at process IPSEC key engine.

  Conditions: This symptom is observed when the dual DMVPN with shared tunnel protection feature is enabled.

  Workaround: There is no workaround.

- CSCtc00851

  Symptoms: The output of the **show mfib table** command on a line card can show tables not in "sync" state, and instead in "disconnecting" or "connecting" state for some time (minutes). In this state the multicast forwarding tables are not being updated and may be out of sync with the active RP.

  Conditions: This symptom is observed on line cards or the redundant RP on a distributed router. It is usually associated with conditions of high CPU due to large numbers of routing updates in a scaled configuration.

  Workaround: The **clear mfib table** command may clear the problem. Alternatively, the affected line cards may need to be reloaded.

  Further Problem Description: Often the problem will be accompanied with error messages relating to MFIB connectivity to the multicast routing information base.

- CSCtc67457

  Symptom: A Cisco ASR 1000 Series RP2 crash occurs with the process IKMP.

  Conditions: This symptom is observed with GetVPN Group Member Configs with vrf-lite.

  Workaround: There is no workaround.

- CSCtd59027

  Symptoms: The device crashes due to a bus error.

  Conditions: This symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

  Workaround: There is no workaround.

- CSCtd92821

  Symptoms: A router continuously crashes upon bootup.

  Conditions: The symptom occurs if SSH is configured and if the router is in SSO mode.

  Workaround: Remove SSH keys or use NONE mode for RPR.

- CSCte39643

  Symptoms: If PfR receives an EIGRP route change, the router may unexpectedly reload.

  Conditions: This symptom is observed with PfR and EIGRP configurations. It is observed some time after PfR receives an EIGRP route change, but before the previous EIGRP route is removed in the routing table, when PfR tries to recycle a previous EIGRP route.

  Workaround: There is no workaround.

- CSCte58962

  Symptoms: If an OSPF instance is being redistributed by some other routing protocol but is never activated by configuring "router ospf x", the standby RP can crash during a subsequent execution of the **no router ospf x** command.

  Conditions: The symptom is observed on systems with redundant RPs and only if the standby is reloaded after the redistribution is removed.

  Workaround: Have "router ospf x" configuration lines for all the OSPF instances being redistributed by other protocols.

- CSCte83779

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router may crash.

  Conditions: The symptom is observed when DMVPN is configured with GETVPN. It is only seen when running a specific script for ASRs.

  Workaround: There is no workaround.

- CSCte91471

  Symptoms: Clock synchronization with the NTP server could be lost for several hours if router (NTP client) runs NTPv4.

  Conditions: The symptom is observed if the router clock is reset (for example: by using the **clock set** exec command). The router then takes a long time to synchronize again.

  Workaround: There is no workaround. The clock will automatically synchronize after few hours.

- CSCte92659

  Symptoms: The router loses some memory due to flow id.

  Conditions: The symptom is observed with a 32k session scaling scenario and with the PPP session flapping when accounting associated with flow id is configured.

  Workaround: There is no workaround.

- CSCte94221

  Symptoms: A PPP connection over CDMA link is flapping.

  Conditions: This symptom is observed when using Cisco IOS Release 15.0M.

  Workaround: Shut / no shut the interface and wait for 2 minutes.

- CSCte98852

  Symptoms: When the broadband accounting accuracy feature (for example, "subscriber accounting accuracy") is configured and "service accounting" is enabled, a duplicate session accounting start (with unique session ID) message is sent out, creating two entries in the AAA server.

  Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router. The issue is observed only when the accounting accuracy feature and service accounting are enabled.

Workaround: There is no workaround as the accounting accuracy may be off as much as 10-seconds worth of byte-counts if the feature is turned off. You could configure the following:

1. **aaa accounting delay-start**
2. **aaa accounting include auth-profile [delegated-ipv6-prefix, framed-ip-address, framed-ipv6-prefix]**.

- CSCtf23298

  Symptoms: High CPU usage occurs.

  Conditions: This symptom occurs when a Terminal Access Controller Access-Control System (TACACS) server is configured with a single connection.

  Workaround: Remove single connection option.

- CSCtf36117

  Symptoms: Crash occurs when executing the **show crypto session brief** command with multiple IKEv2 tunnel connections.

  Conditions: The symptom is observed when setting up as many as 500 IKEv2 tunnels employing symmetric RSA-Sig based authentication with CRL check enabled. This crash occurs when there are about 450 tunnels established and the command is trying to list down the sessions.

  Workaround: There is no workaround.

- CSCtf53537

  Symptoms: Serial interfaces are messed up in second redundancy switchover.

  Conditions: This symptom is observed upon second switchover in sb_throttles.

  Workaround: The issue is due to a change in if_numbers of serial interfaces.

- CSCtf54561

  Symptoms: A MPLS TE FRR enabled router can encounter a crash if the **show ip cef vrf** *vrf-name* command is issued.

  Conditions: This symptom occurs when the VRF contains many entries (17k) in which the outgoing interface changes due to a topology change.

  Workaround: The command should not be entered when many topology changes occur on interface flaps.

- CSCtf56107

  Symptoms: A router processing an unknown notify message may run into a loop without relinquishing control, kicking off the watchdog timer and resulting in a software-based reload.

  Conditions: The symptom is observed when an unknown notify message is received.

  Workaround: There is no workaround.

- CSCtf72328

  Symptoms: BFD IPv4 Static does not fully support AdminDown.

  Conditions: The symptom is observed with the following setup and configuration:

```
Router 1: interface e0/0 ip address 192.168.1.1 255.255.255.0 bfd interval 51 min_rx
51 multiplier 4 bfd echo no shut exit
interface loopback 0 ip address 10.10.1.1 255.255.0.0 exit ip route static bfd e0/0
192.168.1.2 ip route 10.20.0.0 255.255.0.0 e0/0 192.168.1.2
Router 2: interface e0/0 ip address 192.168.1.2 255.255.255.0 bfd interval 51 min_rx
51 multiplier 4 bfd echo no shut exit
interface loopback 0 ip address 10.20.1.1 255.255.0.0 exit
```

```
ip route static bfd e0/0 192.168.1.1 ip route 10.10.0.0 255.255.0.0 e0/0 192.168.1.1
interface e0/0 no ip route static bfd e0/0 192.168.1.1
```

Though the BFD state is DOWN, the static has the route active. If the BFD peer signals AdminDown on a session being used to monitor the gateway for a static route, no action will be taken.

Workaround: Perform a shut/no shut the interface on which the BFD session is configured.

- CSCtf87039

  Symptoms: Device crashes at crypto_ikmp_process_xauth_reply.

  Conditions: The symptom could occur while processing the xauth response received from the client. The PPC platform crashes (the MIPS64 platform does not crash).

  Workaround: There is no workaround.

- CSCtf89408

  Symptoms: A crash may be seen on switchover while the session replays on the standby.

  Conditions: The symptom is observed if the nas-port-id in service profile is null.

  Workaround: There is no workaround.

- CSCtg01020

  Symptoms: Due to an invalid SPI (value 0), phase 2 is not established between two Cisco ASR 1000 series routers when a VPN tunnel is configured.

  The output of “show crypto ace spi” shows “Normal SPI allocated .....61140" or in a show tech look for “SPI allocated.....61440" on one of the routers.

  The peer might issue an error about an invalid SPI with value zero.

  Conditions: The symptom is observed when the ASR router has been up for weeks. The failure will show up once we've run out of SPIs to allocate on the hardware.

  Workaround: The tunnel will come up after a reload of the ASR as all the allocated SPIs will be freed. SPIs will be leaked only when a phase 2 negotiation fails. SAs that expire due to hitting their lifetime will not leak their SPIs. Therefore, if the network is stable and all tunnels are properly configured and all endpoints remain reachable and no negotiations fail, the impact of this defect can be minimized.

- CSCtg13269

  Symptoms: On peers of Route Reflectors (RR), the received prefixes counter shows an incorrect number when session flaps occur during a network churn.

  Conditions: The symptom is observed with BGP RRs.

  Workaround: Use the **clear ip bgp *** command.

- CSCtg22674

  Symptoms: The router experiences high CPU for several minutes due to a “MPLS TE LM” process.

  Conditions: This symptom occurs when a router has many (perhaps as few as 100) MPLS TE tunnels that traverse over a link that experiences repeated flapping in a short duration.

  Workaround: There is no workaround.

  Further Problem Description: Use the command **show process cpu** to determine CPU utilization. If this problem exists, the MPLS TE LM process holds greater than 90% resources for 5 minutes or more.

  ```
  CPU utilization for five seconds: 100%/0%; one minute: 100%; five minutes: 100% PID
  Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process 216 867694836 18357673 47266
  99.67% 99.09% 99.11% 0 MPLS TE LM
  ```

- CSCtg41606

  Symptoms: With Reverse Route Injection (RRI) configured with the **reverse-route** command, if the crypto map is applied to a multi-access interface (for example, ethernet) then egress traffic may fail when the router cannot populate an ARP entry for the crypto peer address.

  Conditions: The symptom could occur when the upstream device does not support proxy arping.

  Workaround: Use the **reverse-route remote-peer <next-hop-ip>** command instead of just **reverse-route**.

- CSCtg44097

  Symptoms: The connect-Info(77) attribute is sent twice in a Pre-Auth Access-Request, when it should only be sent once.

  Conditions: The symptom is observed when the outbound service policy and LLID authorization feature are configured.

  Workaround: There is no workaround.

- CSCtg58786

  Symptoms: When an external interface on the BR is shut down, the BR could crash.

  Conditions: This symptom is observed if more than 1000 Application Traffic Classes are configured on MC, and if that traffic is traversing through an external interface on a BR, and if the external interface is shut down.

  Workaround: There is no workaround.

- CSCtg60228

  Symptoms: In a rare condition of using the **config replace <>** command to remove all the bgp configurations that contain bgp peers as part of a peer-group, the router may crash due to a timing issue between the bgp tasks.

  Conditions: This symptom is observed when “config replace <>” is used to replace old router configs when bgp has lots of peers as part of the peer-group, and when the configs are replaced with new config that do not have bgp configurations.

  Workaround: Do not use the **replace config <>** command.

- CSCtg64175

  Symptoms: The ISIS route is missing the P2P link. It is mistakenly marked as “parallel p2p adjacency suppressed.”

  Conditions: The symptom is observed when the ISIS neighbor is up and multiple topologies are enabled on P2P interfaces. It is seen if you enable a topology on a P2P interface of the remote router and send out the serial IIH packet with the new MTID to the local router where the topology has not been enabled on the local P2P interface yet.

  Workaround: Do a **shut** and **no shut** on the local P2P interface.

- CSCtg67346

  Symptoms: After some time of normal operation, a dialer interface (dialer profile configuration) might become stuck. Debugs would only show “Di1 DDR: dialer_fsm_pending() di1.”

  Conditions: The conditions are unknown at this time.

  Workaround: Remove the affected dialer and put the configuration on another dialer.

- CSCtg68047

  Symptoms: The router reloads.

Conditions: The symptom is observed if several tunnels with crypto protection are being shut down on the router console and the **show crypto sessions** command is executed simultaneously on another terminal connected to the router.

Workaround: Wait until the tunnels are shut down before issuing the **show** command.

- CSCtg72481

  Symptoms: Spurious memory access is seen with QoS configurations.

  Conditions: The symptom is observed only when sending the traffic for a while.

  Workaround: There is no workaround.

- CSCtg73631

  Symptoms: Spurious access or crash.

  Conditions: EIGRP undergoes a route delete event for a route that is both redistributed and learned as an external. The redistributed route is deleted and the external route promoted. An error in the route deletion codepath may result in spurious access or crash.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is not present in Cisco IOS Release 15.0(1) M4.

- CSCtg75452

  Symptoms: RP crashes in dual RP system after doing a **config replace** on POS-configured SDH link.

  Conditions: The symptom is observed if you configure a POS SDH link on a 1XCHSTMOC12/DS0 SPA port and do a **config replace** to a basic router configuration that includes redundancy mode change. This crashes the RP and produces a core file.

  Workaround: There is no workaround.

- CSCtg75627

  Symptoms: The **clear ip route vrf** <*vrf-name*> <*address*> command removes the route to the destination network if the host address (rather than the network address) is used.

  Conditions: The symptom is observed when the **clear ip route vrf** <*vrf-name*> <*address*> command is entered. Other conditions are not know at this time.

  Workaround: **Shut** then **no shut** the interface.

- CSCtg84969

  Symptoms: The output of **show ip mfib vrf <vrf name> verbose** may show the following line, and multicast traffic may not be hardware switched:

  ```
  "Platform Flags: NP RETRY RECOVERY HW_ERR"
  ```

  Conditions: The symptom is observed on a dual RP Cisco 7600 series router with linecards after multiple reloads or SSO switchovers. When the symptom occurs the output of **show ip mfib vrf <vrf name> verbose** on the standby SP will show some lines preceded with "###" where an interface name is expected.

  Workaround: There is no workaround.

- CSCtg89555

  Symptoms: There is no forwarding interface seen in the mfib output on a DFC.

  Conditions: This symptom is observed when configuring an ip address after multicast has been configured on a dot1Q interface.

  Workaround: Perform a **shut/no shut** of the interface.

- CSCtg91572

  Symptoms: A router with an SSM (S,G) entry consisting of a NULL outgoing list sends a periodic PIM Join message to the upstream RPF neighbor, thereby pulling unnecessary multicast traffic.

  Conditions: This symptom is observed when the router has a NULL outgoing list for an SSM (S,G) entry either due to PIM protocol action (Assert) or when the router is not the DR on the downstream access interface receiving IGMPv3 reports.

  Workaround: There is no workaround.

- CSCtg93243

  Symptoms: QoS + tunnel protection does not work if UUT2 is running VSA. Packets get dropped at UUT2 after being decrypted by VSA.

  Conditions: The symptom is observed with crypto, tunnel protection, and VSA only. (If static crypto + VSA, or tunnel protection + SW crypto is used, packets get forwarded after decryption as expected.)

  Workaround: There is no workaround.

- CSCtg96280

  Symptoms: Cisco VSA “prefix” is not working.

  Conditions: The symptom is observed when Cisco VSA “prefix” is used.

  Workaround: There is no workaround.

  Further Problem Description: The issue follows from the fix for CSCte35678.

- CSCth01526

  Symptoms: The MDT interface is deactivated and activated after an SSO.

  Conditions: After an SSO switchover, the PIM register tunnel or MDT tunnel may go down briefly on switching to the standby RP.

  Workaround: There is no workaround.

- CSCth05533

  Symptoms: A memory leak occurs in the IPSec key engine.

  Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation services router. It is seen with a VPN hub that has more than 500 spokes.

  Workaround: There is no workaround.

- CSCth09200

  Symptoms: The **show bgp all peer-group** <*group name*> **summary** or **show ip bgp all peer-group** <*group name*> **summary** CLI commands do not show peer-group summary information for all the address families.

  For Cisco IOS 12.2(31)SG and 12.2(31)SGA releases, these CLI commands may crash the router.

  Conditions: This symptom is observed if:

  1. There is a description for the peer-group
  2. There is a description for the first neighbor member of the peer-group.

     The above two conditions can be determined in the show running-config.
  3. The first entry in attribute hash table is non empty (internal)

Workaround: Use the **sh ip bgp** <*address-family*> *[*<*safi*>*]* **peer-group** <*group name*> **summary** command instead.

- CSCth15105

  Symptoms: BFD sessions flap after unplanned SSO (test crash).

  Conditions: The symptom is observed on a UUT up with unicast/multicast along with BGP and BFD configurations. For BFD timers of 1*5, 500*8, after doing a test crash (option C followed by 6), we see BFD sessions flap.

  Workaround: There is no workaround.

- CSCth16962

  Symptoms: The primary KS KEK timer gets stuck or reset to zero after a GDOI policy change and rekey. Once the KEK timer gets stuck/reset to zero, there are repeated rekeys, which will impact the whole GET VPN domain. The trigger occurs after a failure event in the primary key server and the secondary key server becomes primary followed by a policy change.

  Conditions: This symptom occurs when the KEK timer gets stuck at zero and there are repeated rekeys to GMs, resulting in a rekey storm.

  Workaround: There is no workaround.

- CSCth18616

  Symptoms: Decode of Framed-IPv6-Prefix fails.

  Conditions: The symptom is observed whenever Framed-IPv6-Prefix is included in a RADIUS profile.

  Workaround: There is no workaround.

- CSCth19516

  Symptoms: A router crashes if PFR and SAF are enabled on the same device.

  Conditions: The symptom is observed when SAF is enabled and PFR has multiple links. When the network gets congested or delay is seen and if there is a changeover from IN-POLICY state to OOP, the router crashes.

  Workaround: Disable SAF completely and reload the router.

- CSCth20862

  Symptoms: A router crashes upon changing the “ipsec gre tunnel” configuration. The crash is seen when the “invalid SPI” message is displayed. This message is normal in IPSec settings, but is more often seen in a session flap situation.

  Conditions: The symptom is observed when two IPSec GRE tunnels are configured on a PE router. The crash is seen after changing the tunnel’s destination and flapping the tunnel. At certain times the issue is seen when just flapping the GRE tunnel.

  Workaround: There is no workaround.

- CSCth23354

  Symptoms: Packets are not reaching the proper queue.

  Conditions: The symptom is observed when class-map is configured with VLAN.

  Workaround: There is no workaround.

- CSCth29393

  Symptoms: Downstream traffic (to the subscriber) is not forwarded. Only upstream counters are increasing.

Conditions: The symptom is observed with the **show sss session detail** command with PXF output.

Workaround: Clear the affected SSS session.

- CSCth37580

  Symptoms: Dampening route is present even after removing “bgp dampening.”

  Conditions: The symptom is observed under the following conditions:

  - DUT connects to RTRA with eBGP + VPNv4
  - eBGP + VPNv4 peer session is established and DUT
  - DUT has VRF (same RD) as route advertised by RTRA

  In this scenario, when DUT learns the route, it will do the same RD import and the net topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

  Workaround: There is no workaround.

- CSCth38303

  Symptoms: A Cisco router running Cisco IOS with an ISG feature set can crash at radius_remove_pkt_id.

  Conditions: This symptom is observed when radius-proxy is configured and the AZR reboot feature comes into play with immediate retransmits of accounting ON/OFF messages.

  Workaround: If the downstream device works correctly without sending retransmits immediately after sending the first packet, the ISG should not crash.

  Alternate Workaround: Do not configure the forward method list under radius-proxy. With this workaround, radius-proxy responds to the accounting message immediately and there will be little chance of getting a retransmit from the downstream client.

- CSCth40213

  Symptom: More than one preshared key for address 0.0.0.0 may not be configurable in different keyrings.

  Conditions: Multiple preshared keys cannot be configured for address 0.0.0.0 in different keyrings.

  Workaround: There is no workaround.

- CSCth42798

  Symptoms: Memory can be corrupted.

  Conditions: This symptom is observed when BGP is in read-only mode and attributes are deleted before the networks.

  Workaround: There is no workaround.

- CSCth46156

  Symptoms: Sometime the ISIS nexthop is not generated because the MT ISIS neighbor is missing in LSP.

  Conditions: In MTR support case, enabling ISIS on multicast topologies after ISIS adjacency is established on IPv4 unicast base topology.

  Workaround: “Shut” then “no shut” the interface.

- CSCth47686

  Symptoms: A crash is seen on the EXEC process on a GM.

  Conditions: This symptom is observed when the same GDOI map is applied to multiple interfaces and the **sh crypto gdoi gm replay** command is entered.

Workaround: There is no workaround.

- CSCth64316

  Symptoms: Unable to configure “radius-server” using SNMP set.

  Conditions: The symptom is observed when you configure via SNMP MIB.

  Workaround: Radius server can be configured through the CLI.

- CSCth66604

  Symptoms: ISSU incompatibility due to different versions of a protocol (NTP v3 and NTP v4).

  Conditions: The symptom is observed with an ISSU upgrade or downgrade.

  Workaround: Unconfigure the CLIs causing MCL errors and repeat the ISSU process again.

- CSCth66813

  Symptoms: Traffic flows only on one side while sending bi-directional traffic.

  Conditions: This symptom is observed after disabling or enabling “atm route-bridged ip.”

  Workaround: “Shut” then “no shut” the interface.

- CSCth73173

  Symptoms: ASR may crash if a QoS policy applied using CoA through Service-Template is more than 256 characters in length.

  Conditions: This symptom is observed when a QoS Policy string length exceeds 256 characters.

  Workaround: Ensure that the QoS policy string length is less than 256 characters.

- CSCth85294

  Symptoms: A PIM neighborship is not established with the remote PE and RP for the MVRFs.

  Conditions: This symptom is observed with traffic, after removal and restoration of mvrfs. Traffic does not flow properly since the PIM neighborship is not established with the remote PE and RP for those MVRFs.

  Workaround: There is no workaround.

- CSCth85618

  Symptoms: Extra syslog gets printed but no other functionality is impacted.

  Conditions: This symptom occurs under normal conditions.

  Workaround: There is no workaround.

- CSCth90147

  Symptoms: Router will respond to an RS with an RA.

  Conditions: The symptom is observed when you configure the command **ipv6 nd ra suppress**. This command is only intended to suppress periodic mcast RAs. The router will still respond to unicast RS (that is intended behavior).

  Workaround: Use an ACL to block the reception of RS packets.

- CSCth91984

  Symptoms: Standby resets continuously.

  Conditions: This symptom is observed when 32 extended communities are configured with the **set extcommunity** command on the active RP.

  Workaround: Unconfigure the **set extcommunity** command.

- CSCth93218

  Symptoms: The error message `"%OER_BR-4-WARNING: No sequence available"` displays on PfR BR.

  Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

  Workaround: There is no workaround.

- CSCti01036

  Symptoms: A Cisco ASR1000 series router crashes on the Radius Process.

  Conditions: This symptom is observed on a Cisco ASR 1000 series router with Radius AAA services enabled. When the Radius server sends attributes with no information (empty VSA strings), it produces an unexpected reload on the router.

  Workaround: Prevent the AAA server from sending empty VSA strings.

- CSCti02076

  Symptoms: On a system running Cisco IOS, after unconfiguring an IPv6 link-local address from an interface, any global ipv6 addresses may disappear.

  Conditions: This issue may occur on systems running Cisco IOS when IPv6 is being configured. This issue occurs if an attempt is made to remove the IPv6 link-local address without use of the *link-local* keyword.

  Workaround: There is no workaround.

- CSCti03199

  Symptoms: During switchover, standby crashes after every recovery due to config-sync.

  Conditions: The symptom is observed when the standby tries to sync with the active and when "crypto pki trustpoint" is configured with an unavailable port-channel as source-interface.

  Workaround: There is no workaround.

- CSCti03808

  Symptoms: A Cisco 7200 may crash with a fatal error.

  Conditions: This symptom is observed only when PA-POS-1OC3 and C7200-VSA port adapters are installed and the encrypted traffic is being sent through the POS interface. The problem is more likely as traffic load increases.

  Workaround: Use a different POS port adapter or VAM module instead of the VSA encryption module.

  Further problem description: During investigation the router would also occasionally hang instead of crash. With the fix for this symptom the hangs were not seen.

- CSCti13286

  Symptoms: Putting this configuration on a router:

  ```
  router rip version 2 no validate-update-source network 10.0.0.0 no auto-summary!
  address-family ipv4 vrf test no validate-update-source network 172.16.0.0 no
  auto-summary version 2 exit-address-family
  ```
  and doing a reload causes the "no validate-update-source" statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

  Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

Workaround: There is no workaround.

- CSCti17841

  Symptoms: Removing “match condition” from a class map crashes the router.

  Conditions: The symptom is observed when you remove “match condition” from a class map.

  Workaround: There is no workaround.

- CSCti18615

  Symptoms: Reloading a router which has multicast forwarding configured can result in the standby RP out-of-sync with the active RP. A and F flags are missing from the multicast forwarding base entries.

  Conditions: This symptom occurs when multicast forwarding is operational and configured in the startup configuration, the router is in HA mode SSO, and is reloaded from the RP.

  Workaround: Perform a Shut/no shut of the affected interfaces.

- CSCti20016

  Symptoms: Two issues occur:

  1. When “no bgp default ipv4-unicast” is configured, the dynamic neighbors do not get established
  2. If peer-groups have multiple sessions configured, then even if the neighbor belongs to the peer-group, it does not send this capability.

  Conditions: These symptoms occur when multiple sessions are configured.

  Workaround: For the first issue, if the dynamic neighbor peer-group is activated for other topologies, configure a single session. Configuring a single session also resolves the second issue.

  Further Problem Description:

  1. For the first issue, when **default ipv4-unicast** was disabled in the peer-group member parse function, we do not create a neighbor topology for the IPv4 topology at all. Hence, the dynamic neighbors never come up, resetting due to notification that afi/safi is not supported. For normal neighbors, activation needs to be done for each address family. So neighbor topologies are created at configuration time. But for dynamic neighbors, although the peer-group is explicitly configured for each address family, the actual neighbor creation occurs when we get an “open” from the neighbor address, within the dynamic neighbor range configured wherein the pgrp member parse function is called with afi as router mode. But policy commands are not accepted if **default ipv4-unicast** is disabled in router mode, and similarly neighbor topos cannot be created in such a case. So, when the new dynamic neighbors trying to be created in such a scenario are rejected, the symptom occurs. An exception has to be made for dynamic neighbors.
  2. The second issue is applicable for all peer-group members, not just dynamic neighbors. The bgp_neighbor_send_multisession_cap_allowed() returns “true” only if the multisession capability is configured on the neighbor. If the multisession is configured on the peer-group, and then members do not inherit this property, even though the member accepts the multisession neighbor capability, when the neighbor sends the capability, a single session cap is sent. The peer router keeps rejecting with unsupported capability notification and hence the neighbor never comes up. So peer-group flags should also be considered when any member is checked in cap_allowed function.

- CSCti22091

  Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

Conditions: The symptom is observed when PfR is configured with the following conditions:

1. list > application > filter > prefix-list
2. Learn > traffic-class: keys
3. Learn > traffic-class: filter > ACL

Workaround: There is no workaround.

- CSCti22544

  Symptom: IKE fails to come up while using RSA signature. PKI debugs show the following message:

  ```
  PKI-4-CRL_LDAP_QUERY: An attempt to retrieve the CRL from
  ldap://yni-u10.cisco.com/CN=nsca-r1 Cert Manager,O=cisco.com using LDAP has failed
  ```

  Conditions: This symptom is observed when the VRF-aware IPsec feature is used and vrf-label is configured under trustpoint; for example,

  ```
  crypto pki trustpoint yni-u10 enrollment url http://yni-u10:80 vrf coke
  ```

  Workaround: There is no workaround.

- CSCti25319

  Symptoms: A directly connected subnet that is covered by a network statement is not redistributed into another routing protocol, even if a redistribute Open Shortest Path First (OSPF) is configured.

  Conditions: This symptom occurs only for those configurations in which a network mask covers multiple supernets. For example, for the following network statement, router ospf 1 network 192.168.0.0 0.255.255.255 area 0 the above mentioned symptom occurs if the interfaces are configured with IP addresses as follows: ip address 192.168.0.1 255.255.255.0 ip address 192.168.1.1 255.255.255.0 and so on.

  Workaround: Enable OSPF using the interface command “ip ospf <AS> area.”

  Alternate Workaround: Configure multiple network statements with mask/wildcard equal to supernet as shown in the example below:

  ```
  router ospf 1 network 192.168.0.0 0.0.0.255 area 0 network 192.168.1.0 0.0.0.255 area
  0
  ```

  and so on.

- CSCti28710

  Symptoms: Chunk memory leak is observed on oer_mc_nfc_add_template and oer_mc_nfc_get_source

  Conditions: This symptom occurs on oer_mc_nfc_add_template and oer_mc_nfc_get_source.

  Workaround: Change the border IP address.

- CSCti31984

  Symptoms: Router crashes.

  Conditions: This symptom occurs when “Show stats” is used to show auto Ethernet monitor operation.

  Workaround: There is no workaround.

- CSCti32641

  Symptom: A Cisco ASR 1004 (RP2) router is not able to establish an LDP session to a 3rd-party device and receives an Error Notification (0x07) Bad TLV Length message from that device.

  Conditions: This symptom is observed on a Cisco ASR 1004 with Cisco IOS Release 15.0(1)S when LDP ICCP capability TLV (0x405) is supported on the router.

Workaround: There is no workaround.

Further Problem Description: It seems that Cisco ASR 1004 routers send to the peer a malformed ICCP capability TLV (0x405).

- CSCti34396

  Symptoms: The router distributes an unreachable nexthop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

  Conditions: The symptom is seen when "next-hop-unchanged allpaths" is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is an unreachable.

  Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the nexthop is set to a visible address, you would configure:

  ```
  route-map static-nexthop-rewrite permit 10 match source-protocol static set ip
  next-hop <router ip address> ! router bgp <asn> address-family ipv4 vrf <vrf name>
  redistribute static route-map static-nexthop-rewrite exit-address-family exit exit
  ```

  Workaround 2: Instead of configuring static routes with a next-hop, specify an interface name.

  For example, if you had:

  ```
  ip route x.x.x.x 255.255.255.0 y.y.y.y
  ```

  And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with:

  ```
  ip route x.x.x.x 255.255.255.0 interface serial2/0
  ```

  Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration "set ip next-hop self" is added to route-maps.

  When used in conjunction with the newly added configuration:

  ```
  router bgp <asn> address-family vpnv4 unicast bgp route-map priority
  ```

  The "set ip next-hop self" will override "next-hop unchanged allpaths" for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti34968

  Symptoms: ACL with QoS is crashing the router, if one of the ACEs is evaluate or reflect.

  Conditions: The symptom is observed if the pure ACL used under a class-map is also a reflexive ACL. It is observed only in a pure QoS class-map configuration which has only access-group match filter. It is not seen with an impure QoS class-map configuration which has access-group as well as other filters like DSCP.

  Workaround: Do not use reflexive ACL under QoS. It is not a good practice.

- CSCti36310

  Symptom: A Cisco ASR 1000 Series Aggregation Services router is leaking memory when IKE attributes are pulled by SNMP.

  Conditions: This symptom is observed on a Cisco ASR 1000 Series Aggregation Services router with SNMP enabled. The leak has been observed with the asr1000rp1-adventerprisek9.03.01.00.S.150-1.S and asr1000rp1-adventerprisek9.02.06.01.122-33.XNF1 images.

  Workaround: There is no workaround.

- CSCti36423

  Symptoms: Cisco IOS ASR router memory leaks when NHRP, SNMP, and DMVPN are configured.

Conditions: This symptom is observed in Cisco IOS ASR routers running the asr1000rp1-adventerprisek9.03.01.00.S.150-1.S image.

Workaround: There is no workaround.

- CSCti39902

  Symptoms: An RRI route is still seen on the UUT via router1 after the deletion of the IPsec SA.

  Conditions: Configure RRI on the UUT.

  Workaround: There is no workaround.

- CSCti40660

  Symptoms: The following message is seen:

  ```
  %FW-4-GLOBAL_SESSIONS_MAXIMUM: Number of sessions for the firewall exceeds the
  configured global sessions maximum value 2147483647
  ```

  Conditions: This symptom is observed when IP SLA is configured along with self zones

  Workaround: Do not configure these features together.

- CSCti49472

  Symptoms: System “accounting off” record is seen with suppress-CLI enabled.

  Conditions: This symptom is observed with AAA CLI for suppressing system accounting records on switchover enabled when “Accounting OFF” is sent from a Cisco 7600 router.

  Workaround: There is no workaround.

- CSCti51145

  Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

  Conditions: In order to see this problem, ALL of the following conditions must be met:

  – The non-reloading device must have a “neighbor x.x.x.x transport connection-mode passive” configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword “established” or “eq bgp”

  – It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload

  – When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages

  – Both peers must be multisession capable

  – “transport multi-session” must not be configured on either device, or enabled by default on either device

  – “graceful restart” must not be configured

  Workarounds:

  1. Remove the configuration “neighbor x.x.x.x transport connection-mode passive” or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
  2. Configure “neighbor x.x.x.x transport multi-session” on either the device or its neighbor.
  3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command.

4. Configure graceful restart using the command **neighbor x.x.x.x ha-mode graceful-restart**.
5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

Further Problem Description: This is a day-one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where "neighbor x.x.x.x transport single-session" is configured and NSF is not configured.

The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

Note that the fix does not solve the problem when interacting with Cisco IOS 12.2(33)SB-based releases if the Release 12.2(33)SB router is the one not reloading.

- CSCti59562

  Symptoms: DHCP accounting stop does not clear IP initiated sessions and radius-proxy sessions.

  Conditions: This symptom occurs when VRF mapping is being used.

  Workaround: There is no workaround.

- CSCti61949

  Symptoms: Unexpected reload with a `"SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header"` and `"chunk name is BGP (3) update"` messages.

  Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

  Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti62801

  Symptoms: When both Caller-ID (CID) and Call-Waiting (CW) features are enabled on SIP analog endpoint, repetitive Call-Waiting (CW) tone is not played every 10 seconds until call is answered.

  Conditions: The symptom is observed with a SIP analog endpoint on IAD243x, when the Device Service Application (DSAPP) is enabled on the gateway to provide supplementary features using SIP for the phone connected to the FXS port.

  Workaround: There is no workaround.

- CSCti66076

  Symptoms: A standby HSRP router could be unknown after reloading the ES20 module that configured HSRP.

  Condition: This symptom is observed under the following conditions:

  - HSRP version 1 is the protocol that must be used
  - Use HSRP with sub-interfaces on ES20 module
  - Reload the ES20 module

  Workaround: Change to HSRPv2, which is not exposed to the issue.

  Alternate Workarounds:

  1. Reconfigure HSRP on all subinterfaces

2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode).

- CSCti66153

  Symptoms: A Cisco 7200 series router with VSA in GETVPN deployment is logging the following error:

  ```
  %VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption error, Selector checks.
  ```

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

  – A Cisco 7200 series router with VSA in receive-only mode
  – Keyserver in receive-only mode
  – Other GM in passive mode (that is encrypting outbound traffic) sending traffic to the "inside" of the Cisco 7200
  – Traffic matching a keyserver delivered crypto ACL matching L4 ports (e.g.: **permit tcp any any eq 23**).

  Workaround: Relax any of the conditions above as follows:

  1. Use VAM2+ instead of VSA
  2. Use GETVPN ACL without l4 ports (e.g.: **permit ip any any**)
  3. Have the Cisco 7200 in passive mode as well
  4. Not using receive-only mode on the keyserver.

- CSCti67102

  Symptoms: Tunnel disables due to recursive routing loop in RIB.

  Conditions: The symptom is observed when a dynamic tunnel which by default is passive in nature is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

  Workaround: There is no workaround.

- CSCti67832

  Symptoms: Cisco 3900e platform router reloads while try to enable GETVPN Group Member (GM) all-features debugs.

  Conditions: The symptom is observed on a Cisco 3900e router that is running Cisco IOS interim Release 15.1(2.7)T and while trying to enable the debug **debug crypto gdoi gm all-features**.

  Workaround: There is no workaround.

- CSCti68721

  Symptoms: The output of **show performance monitor history interval** <*all* | *given #*> will appear to have an extra column part way through the output.

  Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

  Workaround: If the symptom occurs, repeat the command.

- CSCti69008

  Symptoms: When dampening is configured for many VRFs, doing full vpnv4 radix tree walk and the proposed fix improves convergence by doing subtree walk based on VRF/RD.

  Conditions: This symptom is observed with dampening configuration changes for VRFs.

Workaround: There is no workaround.

- CSCti69990

  Symptoms: A router crashes after unconfiguring IPv6 and then reconfiguring.

  Conditions: The symptom is observed only under the following specific conditions:

  - Router has IPv6 configured on a number of interfaces
  - Router has GLBP configured
  - IPv6 configuration is removed from all interfaces and then re-applied.

  Workaround: There is no workaround.

- CSCti75666

  Symptoms: Calls from CUCM through H.323 to SIP CUBE get disconnected when remote AA does transfer.

  Conditions: The symptom is observed on CUCM 4.1.3 and 6.1.3. It is seen on a Cisco ISR gateway that is running Cisco IOS Release 12.4(24)T2.

  Workaround: Convert the H.323 leg to SIP.

- CSCti77879

  Symptoms: When the traffic to encrypt matches the first sequence of a crypto map, starting its crypto ACL with a deny statement, the traffic is dropped whether or not this deny statement is a subset of the permits contained in that crypto ACL or not.

  Also, the limitation of 14 denies in an ACL due to the jump behavior does not seem to be present.

  Conditions: The symptom is observed in a VSA installed in a Cisco 7200 series router that is running Cisco IOS Release 15.0(1)M3.

  Workaround: There is no workaround.

  Further Problem Description: As the configuration guide states, the **crypto ipsec ipv4-deny {jump | clear | drop}** command should help to avoid this problem, but this command is not available for the VSA, only for VPN SPA.

- CSCti79442

  Symptoms: One-way voice.

  Conditions: The symptom is observed on a Cisco AS5400 MGCP controlled by PGW, SIP to PSTN call, with echo cancellation enabled. You see the RTP RX/TX counters increment with the **show call active voice brief** command.

  Workaround: Explicitly define the MGCP codec type: **mgcp codec g711ulaw packetization-period 20**.

- CSCti82141

  Symptoms: The following symptoms are observed:

  1. The “none” option will be missing in the **show run** output after “ntp pps-discipline none inverted stratum <#value>” is configured.
  2. “Invalid input detected” error message will be thrown during the bootup and the configured “ntp pps-discipline none inverted stratum <#value>” will vanish after a reload.

  Conditions: The symptom is observed when the “inverted” option is included in the “ntp pps-discipline” CLI.

  Workaround: Configure the CLI without the “inverted” option.

- CSCti84762

  Symptoms: Update generation is stuck with some peers held in refresh started state (SE).

  Conditions: This is seen with peer flaps or route churn and with an interface flap.

  Workaround: Do a hard reset of the stuck peers.

- CSCti85446

  Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

  Conditions: The symptom is observed under the following conditions:

  1. Configure a nexthop static route with permanent keyword
  2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface)
  3. Change the configuration in such a way that nexthop is reachable
  4. Configure a new static route through the same nexthop IP address used in step 1.

  Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti87502

  Symptoms: CP Express does not launch. A blank or garbage characters appear in the browser.

  Conditions: This symptom is observed when attempting to launch CP Express.

  Workaround: A power cycle fixes the issue temporarily.

- CSCti88897

  Symptoms: When configuring the interface cellular 0 on a Cisco 880 series router that is running Cisco IOS Release 15.1(1)T1 or up to Release 15.1(2) T1, the command **service-policy output QOS_CUST_BASIC_OUT** disappears when the router is reloaded or power cycled.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(1)T1 or up to Release 15.1(2)T1.

  Workaround: There is no workaround.

- CSCti91036

  Symptoms: Performance drop has been seen between Cisco IOS Release 15.1(1)T and Release 15.1(2)T.

  Conditions: The symptom is observed when you upgrade from Cisco IOS Release 15.1(1)T to Release 15.1(2)T.

  Workaround: There is no workaround.

- CSCti93175

  Symptoms: NAT router does not translate address of the last TCP ACK in the 3-way handshake.

  Conditions: The symptom is observed with the following conditions:

  - VRF NAT is involved
  - “ip nat outside source translation” has to exist.
  - NAT flow-entries are disabled by **no ip nat create flow-entries**.

  Workaround: There is no workaround.

- CSCti95511

  Symptoms: The command **no buffer header permanent** does not restore the default number of header buffers.

Conditions: This symptom is observed under the following conditions:

- Only when configuring header/fast switching buffers
- Buffers need to be created for this pool.

Workaround: Configure the buffer CLIs carefully. This issue could be avoided by:

1. Not configuring “buffer header permanent” with a high value when available memory is low.
2. Not configuring “no buffer header permanent” when the number of buffers in the free list is less than the minimum value.

- CSCti97810

  Symptoms: A `“%SYS-2-FREEBAD”` memory traceback is seen on an HA router.

  Conditions: The symptom is observed on an HA router approximately 3-4 minutes after loading the image on an HA router.

  Workaround: There is no workaround.

- CSCti97896

  Symptoms: A Cisco ISR router with 512MB of memory and iomem set to 25% may crash and hang at bootup.

  Conditions: The symptom is observed when booting a Cisco IOS 15.0 image with iomem set at 25% and 512MB of RAM.

  Workaround: Do not configure “memory-size iomem 25". To restore from the hang you will need to physically reload the router, break to rommon, and issue the following rommon command: **iomemset smartinit**. Check that you have smartinit enabled using the rommon command **meminfo** which would show you “Smart Init is enabled."

- CSCti98219

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat

- CSCti98347

  Symptoms: DMVPN Phase 3 traffic flows stop and do not recover when the primary spoke loses WAN connectivity. NHRP entry on hub router continues to try to use NHRP mapping to spoke router that goes offline.

  Conditions: This symptom occurs on routers running the asr1000rp1-adventerprisek9.02.06.02.122-33.XNF2.bin. image. Primary DMVPN Phase 3 spoke goes offline or loses connectivity and the NHRP mapping on the hub router doesn’t get updated.

  Workaround: Clear IP route for the network(s) on the hub router.

  Further Problem Description:

```
Hub3#sho ip route next-hop-override | section % + - replicated route, % - next hop
override
D % 10.2.1.0 [90/2588672] via xxx.xx.x.x, 19:07:03, Tunnel2 [90/2588672] via
xxx.xx.x.x, 19:07:03, Tunnel2 [90/2588672] via xxx.xx.x.x, 19:07:03, Tunnel2
[NHO][90/1] via xxx.xx.x.x, 19:52:03, Tunnel2 <<---- This is Tunnel IP that is
shutdown.
Sho ip nhrp cache 10.2.1.0 10.2.1.0/24 via xxx.xx.x.xx <<----- Pointing to redundant
spoke - this one should be used. Tunnel2 created 00:22:21, expire 00:04:03 Type:
dynamic, Flags: router used NBMA address: 10.1.12.12
```

- CSCtj00039

  Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

  Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

  Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj01235

  Symptoms: A crash is seen when running the command **debug crypto isakmp** during ISAKMP profile selection. The crashinfo file shows that the crash is happening during MM_KEY_EXCH as it receives the certificate from the remote peer.

  Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router that is running Cisco IOS Release 15.0(1)S.

  Workaround: There is no workaround.

- CSCtj04278

  Symptoms: In a DMVPN setup that is running the code of Cisco IOS Release 15.1TPI15, it is possible that NHRP Registrations are not sent by the box. This is seen if crypto is not configured using tunnel protection.

  Conditions: This symptom occurs when tunnel protection is not configured.

  Workaround: perform a shut/noshut of the tunnel interface.

- CSCtj04672

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCtj05198

  Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

  Conditions: This symptom is observed when there are two EIGRP router processes.

  Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj05903

  Symptoms: Some virtual access interfaces are not created for VT, on reload.

  Conditions: This symptom occurs on scaled sessions.

  Workaround: There is no workaround.

- CSCtj06302

  Symptoms: Cisco IOS ASR1000 SBC box crashes when it is trying to configure “media-address pool ipv4” CLI under SBC against the XNF2 image.

  Conditions: This symptom occurs when “media-address pool ipv4” CLI is configured.

  Workaround: There is no workaround.

- CSCtj08368

  Symptoms: Router software crash at process_run_degraded_or_crash.

  Conditions: The symptom is observed when the allocated memory block is freed.

  Workaround: There is no workaround.

- CSCtj10592

  Symptoms: DVTI GRE IPv4 mode fails to create virtual-access for IKEv2 connections.

  Conditions: The symptom is observed with a simple SVTI to DVTI connection.

  Workaround: There is no workaround.

- CSCtj16291

  Symptoms: Voice router crashes due to memory corruption.

  Conditions: The symptom is observed when multiple SIP Register are received. The response causes a Send Error.

  Workaround: There is no workaround.

- CSCtj17316

  Symptoms: EIGRP flaps up and down in a large scale network, when there is a lot of data to be sent.

  Conditions: In an EIGRP network that has a large number of peers on a single interface, EIGRP might stop sending data to peers. This causes a flap due to packets not being acknowledged.

  Workarounds:

  1. Find the instability in the network and fix the interface
  2. Summarize more routes
  3. Change more routers to stub
  4. Upgrade to rel7 of EIGRP.

- CSCtj17545

  Symptoms: Immediately after a switchover, the restarting speaker sends TCP-FIN to the receiving speaker, when receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.

  Conditions: The symptom can occur when a lot of BGP peers are established on different interfaces.

  Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

  ```
  template peer-session ce-v4 transport connection-mode passive
  ```

- CSCtj21696

  Symptoms: The virtual access interface remains down/down after an upgrade and reload.

  Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

```
Router1#sho inv NAME: "chassis", DESCR: "2801 chassis" PID: CISCO2801 , VID: V04 , SN:
FTX1149Y0KF
NAME: "motherboard", DESCR: "C2801 Motherboard with 2 Fast Ethernet" PID: CISCO2801 ,
VID: V04, SN: FOC11456KMY
NAME: "VIC 0", DESCR: "2nd generation two port EM voice interface daughtercard" PID:
VIC2-2E/M= , VID: V , SN: FOC081724XB
NAME: "WIC/VIC/HWIC 1", DESCR: "4 Port FE Switch" PID: HWIC-4ESW , VID: V01 , SN:
FOC11223LMB
NAME: "WIC/VIC/HWIC 3", DESCR: "WAN Interface Card - DSU 56K 4 wire" PID:
WIC-1DSU-56K4= , VID: 1.0, SN: 33187011
NAME: "PVDM 1", DESCR: "PVDMII DSP SIMM with one DSP with half channel capacity" PID:
PVDM2-8 , VID: NA , SN: FOC09123CTB
```

  Workaround: Do a shut/no shut on the serial interface.

- CSCtj24453

  Symptoms: The following traceback is observed when **clear ip bgp *** is entered:

```
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 5905A0A8
chunkmagic 120000 chunk_freemagic 4B310CC0 -Process= "BGP Scanner", ipl= 0, pid= 549
with call stack 0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
0x403A4E84:bgp_scanner(0x403a4c50)+0x234
```

  Conditions: This symptom is rarely observed, but can occur when **clear ip bgp *** is entered with a lot of routes and route-map-cache entries.

```
Router# show ip bgp sum
BGP router identifier 10.0.0.1, local AS number 65000 BGP table version is 1228001,
main routing table version 1228001 604000 network entries using 106304000 bytes of
memory 604000 path entries using 31408000 bytes of memory 762/382 BGP path/bestpath
attribute entries using 94488 bytes of memory 381 BGP AS-PATH entries using 9144 bytes
of memory 382 BGP community entries using 9168 bytes of memory 142685 BGP route-map
cache entries using 4565920 bytes of memory
```

  The **clear ip bgp *** command is not a very common operation in the production network.

  Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the issue will not be observed.

- CSCtj27251

  Symptoms: A router may crash when modifying a QoS class-map.

  Conditions: The symptom is observed when modifying a QoS class-map which is being referenced by two or more policy-maps while traffic is matching the class-map and traversing the router.

  Workaround: Remove the policy-maps that match the class-map to be modified by issuing **no service-policy input/output** *policy-map name*, make changes to the class-map, then re-apply the policy-maps by issuing **service-policy input/output** *policy-map name*.

- CSCtj28747

  Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an "Exit Mismatch" message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

  Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

Workaround: There is no workaround.

- CSCtj32574

  Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

  ```
  router eigrp 1 redistribute connected no redistribute connected
  ```

  The **no redistribute connected** command is not being backed up to the standby.

  Conditions: The symptom is observed with any redistribute-related commands.

  Workaround: There is no workaround.

- CSCtj33003

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

- CSCtj35106

  ```
  Symptoms: Spurious memory access seen:
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61CBC400z reading 0x70
  %ALIGN-3-TRACE: -Traceback= 0x61CBC400z 0x631A1ABCz 0x63156BA0z 0x631A508Cz
  0x631A5600z 0x62B75A10z 0xFFFF95C0z 0xFFFF95C0z
  0x61CBC400:ipv6_enqueue(0x61cbc3dc)+0x24
  0x631A1ABC:fw_dp_insp_send_rsts(0x631a00b8)+0x1a04
  0x63156BA0:fw_dp_tcp_inactivity(0x631567ac)+0x3f4
  0x631A508C:fw_dp_insp_handle_sis_idle_timeout(0x631a4c64)+0x428
  0x631A5600:fw_dp_insp_handle_timer_event(0x631a554c)+0xb4
  0x62B75A10:tw_notify(0x62b75944)+0xcc
  ```

  Conditions: The symptom is observed with any self-generated IPv6 traffic.

  Workaround: There is no workaround.

- CSCtj36521

  Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

  Conditions: The symptom is observed only if IPv6 CEF is enabled at the same time.

  Workaround: Make sure IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj38234

  Symptoms: IPSec IKEv2 does not respond to INVALID_SPI informational message. It should respond with another INFORMATIONAL IKE message.

  An INVALID_SPI may be sent in an IKE INFORMATIONAL exchange when a node receives an ESP or AH packet with an invalid SPI. The notification data contains the SPI of the invalid packet. The INVALID_SPI message is received within a valid IKE_SA context.

  Conditions: The symptom is observed when an IKEv2 peer sends an INFORMATIONAL IKE message notifying about an INVALID_SPI (IPSec).

Workaround: There is no workaround.

- CSCtj38346

  Symptoms: Router crash is seen when configuring the **default transmit-interface** command.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.1(2.19)T.

  Workaround: There is no workaround.

- CSCtj39558

  Symptoms: Sub-interface queue depth cannot be configured.

  Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.

  Workaround: There is no workaround.

- CSCtj40564

  Symptoms: Cisco ASR 1000 router disallows incoming Internet Key Exchange (IKE) connection that matches a keyring. This issue occurs after the router is reloaded.

  Conditions: This symptom occurs when a crypto keyring, which has a local-address defined as an interface, is used.

  ```
  crypto keyring keyring_test pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted> local address Loopback2104
  ```

  Workaround: Use an IP address.

  ```
  crypto keyring keyring_test pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted> local address <ip address>
  ```

- CSCtj41194

  Cisco IOS Software contains a vulnerability in the IP version 6 (IPv6) protocol stack implementation that could allow an unauthenticated, remote attacker to cause a reload of an affected device that has IPv6 enabled. The vulnerability may be triggered when the device processes a malformed IPv6 packet.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6.

- CSCtj41867

  Symptoms: A Cisco 2900 Integrated Service router that is running Cisco IOS Release 15.1(2)T exhibits increased memory utilization over time.

  Conditions: The symptom is observed when a Cisco 2900 Integrated Services router that is running Cisco IOS Release 15.1(2)T is configured as a branch router that has an VPN WAN connection, Quality Of Service (QoS) classification configured (“qos pre-classify”), and WAAS Express enabled on a several interfaces with MLPPP enabled.

  Workarounds:

  1. Disable QoS classification on VPN tunnel interface
  2. Disable WAAS Express on VPN tunnel interface
  3. Reduce the number of serial interfaces down to one.

  Further Problem Description: The symptom is not observed when QoS classification is not configured or when MLPPP is not configured or when WAAS Express is not enabled.

- CSCtj47736

  Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

  Conditions: The symptom is observed when the neighbor is learned, then a max-service limit is added on an address family, then a shut/no shut is done on the interface.

  Workaround: There is no workaround.

- CSCtj47829

  Symptoms: A buffer leak is experienced with “traffic-export” configured.

  Conditions: The issue seen when you export traffic to an interface and to an NME-APPRE-502-K9. All conditions are not completely known yet.

  Workaround: Disable the traffic-export functionality, for example:

  ```
  Traffic export configs ip traffic-export profile axp-netscout interface
  Integrated-Service-Engine1/0 bidirectional mac-address 0080.8c00.0001
  interface FastEthernet0/0.99 encapsulation dot1Q 99 ip address xxx.xxx.xxx.xxx
  255.255.255.0 ip traffic-export apply axp-netscout
  Remove the configs interface fa0/0.99 no ip traffic-export apply axp-netscout no ip
  traffic-export profile axp-netscout
  ```

- CSCtj48629

  Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC-1CE1T1-PRI.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCtj48913

  Symptoms: Track does not recognize when an HTTP IP SLA probe’s status changes to OK.

  Conditions: The symptom is observed with an HTTP IP SLA probe and with a tracker.

  Workaround: There is no workaround.

- CSCtj52077

  Symptoms: Policy at subinterface is not accepted with CBWFQ.

  Conditions: This symptom is observed when policy is used in Ethernet subinterface.

  Workaround: There is no workaround.

- CSCtj53363

  Symptoms: Router hangs and console does not respond indefinitely.

  Conditions: The symptom is observed with the following conditions:

  - AIM-VPN in ISR + ZBFW; or,
  - A Cisco 2811/2821 Onboard VPN + ZBFW.

  Once traffic starts, router hangs within minutes.

  Workaround: If running a Cisco 2811/2821, use sw crypto + ZBFW.

  Alternate Workaround: If running Cisco 2851 and higher ISRs, use onboard crypto + VPN instead of AIM-VPN + ZBFW.

- CSCtj55624

  Symptoms: A Cisco router crashes upon entering the **show crypto ruleset** command.

  Conditions: This symptom is observed when v6 crypto maps are configured.

Workaround: Do not enter the **show crypto ruleset** command.

- CSCtj56019

  Symptom: Mibwalk dot1dBridge using mst context does not return correct info.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtj61284

  Symptoms: NAT overload does not work for non-directly connected destinations in MPLS-VPN configurations.

  Conditions: The symptom is observed with NAT overload configured to NAT traffic coming over an MPLS VPN to internet (via a VRF-enabled interface).

  Workaround: There is no workaround.

- CSCtj61657

  ```
  Symptoms: IO memory leak is seen followed by TCP no buffer logs:
  %SYS-2-MALLOCFAIL: Memory allocation of xxxx bytes failed from 0xXXXXXXXX, alignment
  xxx Pool: I/O Free: xxxx Cause: Not enough free memory Alternate Pool: None Free: 0
  Cause: No Alternate pool -Process= "Pool Manager"
  %TCP-6-NOBUFF: TTY0, no buffer available -Process= "SCCP Application", ipl= 0, pid=
  XXX
  ```

  Conditions: The symptom is observed in the presence of VOIP phones using multicast applications with the **session protocol multicast** dial-peer configuration command.

  Workaround: There is no workaround.

- CSCtj65553

  Symptoms: The static route that is installed in the default table is missing.

  Conditions: This symptom is observed after Route Processor (RC) to Line Card (LP) to Route Processor transition on a Cisco Catalyst 3000 series switching module.

  Workaround: Configure the missing static route.

- CSCtj69577

  Symptoms: When congestion occurs on a QoS-enabled output interface, output rate significantly decreases.

  Conditions: The symptom is observed under the following conditions:

  1. 3945E outbound interface is connected to 100M link
  2. QoS (LLQ/Fair Queue) is configured on 3945E outbound interface
  3. Congestion occurs on outbound interface.

  Workaround: Reload the router.

  Further Problem Description: This issue is resolved after a reload but the shutdown/no shutdown commands can cause the same issue.

- CSCtj69886

  Symptoms: NTP multicast over multiple hops.

  Conditions: This symptom is observed when a multicast server is multiple hops away from multicast clients.

  Workaround: There is no workaround.

- CSCtj72730

  Symptoms: If an Enhanced Interior Gateway Routing Protocol (EIGRP) **address-family** configuration command is removed, any redistribution commands that refer to that address-family should also be removed. This defect documents a case where the redistribution command is not removed.

  Conditions: This issue occurs when the redistribution command is not removed after removing the corresponding EIGRP address-family configuration command.

  Workaround: Manually remove the redistribution commands that remain after the **address-family** command is removed.

- CSCtj76297

  Symptoms: Router hangs with interoperability of VM and crypto configurations.

  Conditions: The symptoms are seen only during interoperability between video-monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

  Workaround: Disable AIM and use onboard CE.

- CSCtj77004

  Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

  Conditions: The symptom is observed when “archive log config” is configured.

  Workaround: There is no workaround.

- CSCtj77285

  Symptoms: Router CPU becomes high tending towards 80%+ from normal operating conditions. The command **show mem | inc FNF OCE** will show multiple rows rather than just a couple of rows.

  Conditions: The symptom is observed with voice calls and VOIP in use. It is seen when Flexible NetFlow is configured.

  Workaround: Switch off Flexible NetFlow (although that leaves memory consumption in place and CPU higher than normal) or reboot the router.

- CSCtj77477

  Symptom: High delay in priority queue when using CBWFQ/LLQ. For example:

  ```
  EFM rate 2304 kbps
  888E Average delay: 42ms 888E Max delay: 63ms HWIC-4SHDSL-E Average delay: 216ms
  HWIC-4SHDSL-E Max delay: 361ms
  ```

  Conditions: The symptom occurs only on Cisco G.SHDSL EFM platforms 888E and ISR with HWIC-4SHDSL-E.

  Workaround: Configure hierarchical QoS on WAN G.SHDSL EFM interface. For example:

  ```
  EFM rate 2304 kbps
  policy-map CHILD class voice priority percent 25 class business bandwidth percent 50
  policy-map PARENT class class-default shape average 2100000 8400 0 service-policy
  CHILD
  ```

- CSCtj77963

  Symptoms: Resets are observed on low speed links.

  Conditions: The symptom is observed on low speed interfaces over the WAN that produce retransmissions, out of order segments, etc.

  Workaround: There is no workaround.

- CSCtj78966

  Symptoms: A Cisco ASR router crashes with thousands of IKEv2 sessions, after numerous operations on the IKEv2 session.

  Conditions: This symptom is observed when the IKEv2 SA DB WAVL tree is corrupted if we fail to insert the SA due to some error (for example, PSH duplication).

  Workaround: There is no workaround.

- CSCtj79368

  Symptoms: All keyservers crash after removing RSA keys before changing to new ones based on security concerns.

  Conditions: The symptom is observed when removing RSA keys.

  Workaround: Stay on the same RSA keys.

- CSCtj79750

  Symptoms: Multicast responses are not obtained.

  Conditions: This symptom is observed after a Multicast Listener Discovery (MLD) join.

  Workaround: There is no workaround.

- CSCtj79769

  Symptoms: An LC crashes.

  Conditions: This symptom is observed during unconfiguration.

  Workaround: There is no workaround.

- CSCtj81533

  Symptoms: The following error message is seen:

  ```
  np_vsmgr_modify_connection: invalid service id 11 passed
  ```
  No detrimental consequences or effects on the correct operation of the router are observed; however, thousands of these error messages may appear on the console.

  Conditions: This symptom is observed on Cisco AS5400 platforms during VoIP calls, and is more evident when the router is handling multiple calls.

  Workaround: There is no workaround.

- CSCtj82292

  Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.

  Conditions: This issue occurs when summary address is advertised as follows:

  ```
  ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
  ```
  Workaround: There is no workaround.

- CSCtj82387

  Symptoms: Config sync @ pppoe server remote-id

  Conditions: This symptom is observed on the Cisco 7600 platform with Cisco IOS Release_15.1(1.14)S.

  Workaround: There is no workaround.

- CSCtj84901

  Symptoms: Cisco routers crash when traffic passes from the MGF port of any module towards the router CPU with a PVDM module present in the router.

Conditions: This symptom is observed on Cisco 19xx, 2911 and 2921 routers with PVDM modules, as well as any other module that connects to the MGF backplane switch. The modules that currently connect to MGF are

1. Service Ready Engine modules (ISM and SM SRE)
2. Etherswitch modules (SM and EHWIC)

If any traffic from these modules flows over the MGF port towards the router CPU, then the router will crash.

This symptom is not observed on Cisco 2951, 39XX, or 39XXe routers.

Workaround: For the EHWIC Etherswitch module with PVDM on the router, there is no workaround.

For the Etherswitch SM modules and Service Ready Engine modules, as long as the MGF port on these modules is not configured to send traffic to the router, there will be no issue. For traffic between modules over MGF there is no issue. If the MGF port on these modules has to be used, then the PVDM would have to be removed from the router. There is no workaround if both the PVDM and the MGF port on these modules has to be used.

- CSCtj85333

  Symptoms: System may crash when config-template contains the config command **ip ips signature-category** and when the template is downloaded to the router using the CNS config feature commands **cns config retrieve** (exec command) and **cns config initial** (config command). This symptom may also occur when the config template is downloaded to the router using the device Config-Update operation of Config Engine.

  Conditions: This symptom is observed in normal mode operation, but will also occur when the CNS feature is used.

  Workaround: There is no workaround.

- CSCtj87180

  Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of `"SSS Manager Disconnected Session"`.

  Conditions: The symptom is observed when the LAC router receives the following message from the multihop peer:

  ```
  "Error code(9): Try another directed and Optional msg: SSS Manager disconnected
  session <<<< INVALID"
  ```

  Workaround: There is no workaround.

- CSCtj89941

  Symptoms: IOSd crash when using the command **clear crypto session** on an EzVPN client.

  Conditions: The symptom is observed under the following conditions:

  1. RP2+ESP20 worked as the EzVPN simulator, which is configured with over 1000 clients. Then simulator is connected to Cisco ASR 1004-RP1/ESP10 (UUT) with DVTI configured
  2. Use IXIA to generate 1Gbps traffic
  3. Wait until all the SAs have been established and traffic is stable
  4. Use CLI **clear crypto session** on EzVPN simulator.

  Workaround: There is no workaround.

- CSCtj90438

  Symptoms: Router crashes if “no switchport” is executed on /1 interface of Enhanced Etherswitch (ESW) or Service Ready Engine (SRE) module.

  Conditions: This symptom occurs while executing “no switchport” on the /1 interface of ESW or SRE module without HWIC-4ESW, HWIC-D-9ESW, HWIC-4ESW-POE, HWIC-D-9ESW-POE, NM-16ESW, and NM-16ESW-1GIG present.

  Workaround: Do not execute the **no switchport** command on the above mentioned modules as this command does not apply to these modules.

- CSCtj91190

  Symptoms: Non-queue same direction policy is not getting accepted.

  Conditions: This symptom is observed on post HQF images when the policy is used on both the ATM main and sub interfaces.

  Workaround: There is no workaround.

- CSCtj91764

  Symptoms: A Cisco UC560/UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to CPU.

  Conditions: This symptom is observed during a complete SNMP MIB walk.

  Workaround: The CISCO-CALL-APPLICATION-MIB can be excluded via configuration.

- CSCtj92692

  Symptoms: Path-confirmation failure seen with rtp-nte to out-of-band dtmf interworking.

  Conditions: This symptom is observed with the following setup:

  ```
  Callgen--OGW---H323----CUBE---H323----TGW---Callgen
  ```

  Workaround: Configure rtp-nte end to end.

- CSCtj94297

  Symptoms: “F” flag gets set in the extranet receiver MFIB forwarding entry, resulting in unexpected platform behavior.

  Conditions: The symptom is observed when the forwarding entry RPF transitions from a NULL/local interface to an interface belonging to a different MVRF.

  Workaround: Use the **clear ip mroute** in the affected mroute.

- CSCtj94617

  Symptoms: Memory leak is seen while issuing the **show running** or the **show ip access-lists** command even though we do not have any named ACL configured on the box.

  Conditions: This symptom is observed when issuing the **show running** command.

  Workaround: There is no workaround.

  Further Problem Description: The memory leak is in dynamic list that was created, which is not destroyed properly.

- CSCtj97823

  Symptoms: The 32-byte topology names are not handled correctly on bootup.

  Conditions: This symptom occurs when 32-byte topology names are not handled correctly on bootup.

  Workaround: Use topology names shorter than 32 characters.

- CSCtk02515

  Symptoms: Path confirmation fails for a basic call between SCCP and SIP endpoints.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3.7)T.

  Workaround: There is no workaround.

- CSCtk02547

  Symptoms: Informer router reloads @__be_gige_dsp_handle_voice_queue.

  Conditions: This symptom is observed on a Cisco router running a Cisco IOS 151-3.7.T image.

  Workaround: There is no workaround.

- CSCtk02647

  Symptoms: On an LNS configured for L2TP aggregation, it might be that per-user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).

  Conditions: This symptom is observed when LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL downloaded for PPP users via radius.

  Workaround: There is no workaround.

- CSCtk02666

  Symptoms: During a graceful restart event, the peer undergoes reconfiguration. This may result in stale labels on the RRP.

  Conditions: The symptom is observed with GR + SSO + peer reprovisioning.

  Workaround: Perform a **clear xconnect** or flap the local VC.

- CSCtk06548

  Symptoms: Using CCBU CVP solution, SIP calls are disconnected during stress test.

  Conditions: The symptom is observed when using a TCP connection. SIP messages are sporadically corrupted and cannot be framed correctly by SIP stack. It is seen with PI14 image testing.

  Workaround: Use PI12 image.

  Further Problem Description: The fundamental issue involves the selective ack (SACK) feature. An alternative workaround would be to disable the “SACK Permitted” option from the peer.

- CSCtk07576

  Symptoms: Routers reload while configuring the “station-role root.”

  Conditions: This symptom is observed while configuring the “station-role root” in the uclient with ssid killers.

  Workaround: There is no workaround.

- CSCtk10279

  Symptoms: A router configured for LISP may crash if it receives a LISP Map-Reply message with an IPv6 RLOC, when IPv6 routing is not enabled.

  Conditions: This symptom occurs when LISP is configured using the **ip lisp {itr | etr | proxy-itr | proxy-etr }** command, the router does not have IPv6 routing configured using the **ipv6 unicast-routing** command.

  Workaround: Enable the IPv6 routing by entering **ipv6 unicast-routing** command.

- CSCtk12122

  Symptoms: A Cisco 7200 router may crash after clearing the SAs while using IKE keepalive feature.

Conditions: This symptom is observed when the IKE keepalive feature is turned on and the user executes a “clear crypto session” or “clear crypto sa.”

Workaround: There is no workaround.

- CSCtk12608

  Symptoms: Route watch fails to notify the client when an RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

  Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, Release 15.1(2)T and Release 15.1(01)S and with the following configurations:

  Router 1: interface Ethernet0/0 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx !

  interface Ethernet1/0 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx ! router bgp 100 no synchronization bgp log-neighbor-changes neighbor xxx.xxx.xxx.xxx remote-as 200 neighbor xxx.xxx.xxx.xxx ebgp-multihop 255 no auto-summary !

  ip route 0.0.0.0 0.0.0.0 10.10.200.1 ip route xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx 10.0.12.2 ip route xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx

  Router 2: interface Loopback200 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx ! interface Loopback201 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx ! interface Ethernet0/0 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx !

  interface Ethernet1/0 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx ! router bgp 200 no synchronization bgp log-neighbor-changes network xxx.xxx.xxx.xxx neighbor xxx.xxx.xxx.xxx remote-as 100 neighbor 10.0.12.1 update-source Loopback201 no auto-summary ! ip route 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx !

  Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes”.

- CSCtk12681

  Symptoms: Enabling IP SLA trace for VoIP RTP causes a crash.

  Conditions: This symptom is observed when IP SLA TRACE is enabled for VoIP RTP probe.

  Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk15360

  Symptoms: Xauth userid mode http-intercept does not prompt for a password and the EzVPN session does not come up.

  Conditions: This symptom occurs when the EzVPN client x-auth is configured as http-intercept.

  Workaround: There is no workaround.

- CSCtk15410

  Symptoms: Spurious memory access is seen at rmon_int_command.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtk16310

  Symptoms: Timeout failure occurs due to “No socket” error.

  Conditions: This symptom occurs with Udp-jitter packet with VRF.

  Workaround: There is no workaround.

- CSCtk18607

  Symptoms: Router crashes at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

Conditions: This symptom occurs at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

Workaround: There is no workaround.

- CSCtk31401

  Symptoms: A Cisco router crashes when the SSH session from it is exited.

  Conditions: This symptom is observed when “aaa authentication banner” is configured on the router.

  Workaround: There is no workaround.

- CSCtk35650

  Symptoms: Router hangs while generating IP SLA auto schedule with maximum length.

  Conditions: This symptom occurs while generating IP SLA auto schedule.

  Workaround: There is no workaround.

- CSCtk36891

  Symptoms: Video conferencing through NAT may crash the router.

  Conditions: This symptom is observed when NAT is configured. Video conferencing with PVDM3 crashes the router.

  Workaround: Remove NAT configurations.

- CSCtk37395

  Symptoms: A Cisco 2921 cannot process fax calls and reports the following:

  ```
  %MSPI-1-NOMEMORY: Unit 770, no memory for mspi_on_xmit, disconnect connection
  ```

  Conditions: Conditions are not known. The symptom may occur when the processor’s free memory is more than 4GB/6.

  Workaround: Reduce slightly the processor memory while increasing the i/o memory and see if this is indeed what is causing the problem:

  - The command is “memory-size iomem 25” on systems with more than 1Gb
  - On systems with 1Gb io mem, you cannot take more than 10%. Instead, use logging buffer 200Mb to decrease free processor memory. This workaround helps to mitigate the issue.

- CSCtk46363

  Symptom: A device running Cisco IOS and acting as a DHCP server crashes.

  Conditions: This symptom is observed when a client requests a specific IP address.

  Workaround: Disable duplicate address detection check using the **ip dhcp ping packet 0** command.

- CSCtk53130

  Symptoms: You may be unable to configure pseudowire on a virtual PPP interface. The command is rejected with the following error:

  ```
  Incompatible with ipv6 command on Vp1 - command rejected.
  ```

  Conditions: The symptom occurs when an IPv6 address has already been configured on the virtual PPP interface.

  Workaround: There is no workaround.

- CSCtk54830

  Symptom: ARP entry is removed from the ARP table by DHCP.

  Conditions: This symptom is observed when replying back to the client Request/Inform.

Workaround: There is no workaround.

- CSCtk56570

  Symptoms: When there are some call loads on CUBE, one-way call occurs while call proceeding, after sending SIP CANCEL.

  Conditions: This symptom occurs when media transcoder-high-density is enabled on CUBE.

  Workaround: Disable media transcoder-high-density.

- CSCtk58732

  Symptoms: The router may crash if the following configuration is applied:

  ```
  ip sla 1 icmp-jitter xxx.xxx.xxx.xxx source-ip xxx.xxx.xxx.xxx num-packets 1 interval
  10 threshold 1000 timeout 1000 frequency 10
  ip sla schedule 1 start-time now life forever

  track 1 ip sla 1 reachability
  ```

  The following error message is displayed:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 10:49:31 UTC Mon Feb 21 2011 addr=0x1,
  pc=0x62D97F30z , ra=0x62D98848z , sp=0x67CE34D0
  10:49:31 UTC Mon Feb 21 2011: Address Error (store) exception, CPU signal 10, PC =
  0x62DA2E10
  ```

  Conditions: This symptom is observed in Cisco IOS Release 15.1(3)T. The router may continually reload following the crash.

  Workaround: Use the ICMP Echo operation instead, as shown below:

  ```
  ip sla 1 icmp-echo 192.0.2.1 source-ip 192.0.2.2 threshold 1000 timeout 1000 frequency
  10
  ```

- CSCtk61069

  Symptoms: The Cisco IOS router crashes.

  Conditions: This symptom occurs while entering “write memory” or “show running configuration” on the router after configuring “privilege exec level 15 show adjacency.”

  Workaround: Do not set the privilege exec level for any form of the **show adjacency** command.

- CSCtk62247

  Symptoms: IKEv2 session fails to come up with RSA sign authentication.

  Conditions: The symptom is observed with a hierarchical CA server structure.

  Workaround: Use non-hierarchical CA servers.

- CSCtk62626

  Symptoms: Memory leak could be observed after 802.1X or MAB authentication when using VLAN and DHCP assignment.

  Conditions: This symptom is observed on a Cisco 890 router configured for 802.1X authentication.

  Workaround: There is no workaround.

- CSCtk67073

  The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

  Cisco has released free software updates that address this vulnerability.

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipsla.

- CSCtk68647

  Symptoms: DMVPN stops allowing connections after operating for some time (based on number of connections). The **show crypto socket** command shows sockets are leaking and never decrease even when the SA is inactive.

  Conditions: This symptom occurs on Cisco ASR code prior to Cisco IOS Release XE 3.2.0. Multiple DMVPN tunnels are configured with tunnel protection shared.

  Workaround: Upgrade to Cisco IOS Release XE 3.2.0. Remove other DMVPN tunnels (or shutdown tunnels).

- CSCtk74970

  Symptoms: TE autoroute announced tunnel is not installed in the routing table.

  Conditions: The symptom is observed if you configure TE with one hop-LDP and then unconfigure. Then configure TE with one hop with non-LDP. The TE autoroute announced tunnel is not installed in the routing table.

  Workaround: Configure “no ip routing protocol purge interface”.

- CSCtk83638

  Symptoms: A client is assigned an ip address from an incorrect pool when it reconnects with a different profile.

  Conditions: This symptom is observed in a setup where two clients are behind an NAT router. When one client’s connection is broken, the server is not made aware of this, then the client reconnects with a different group, the IP address assigned is not from the correct pool.

  Workaround: There is no workaround.

- CSCtk84116

  Symptoms: A GETVPN ks crash may occur.

  Conditions: This symptom is observed when a split-and-merge occurs between the key servers.

  Workaround: There is no workaround.

- CSCtk98726

  Symptoms: ANCP shaper fails to be applied on ATM VC.

  Conditions: This symptom occurs after clearing and re-establishing the PPPoE session.

  Workaround: There is no workaround.

- CSCtl00467

  Symptoms: A Cisco router crashes while using conference call.

  Conditions: This symptom is observed when the conference call feature is used.

  Workaround: There is no workaround.

- CSCtl04285

  Symptoms: After provisioning a new BGP session, a BGP route reflector may not advertise IPv4 MDT routes to PEs.

  Conditions: The symptom is observed on a router running BGP, configured with new style IPv4 MDT and peering with an old style IPv4 MDT peer. Affected releases are Cisco IOS Release 12.2(33)SRE, Release 15.0M, Release 12.2(33)XNE, and later releases.

Workaround: There is no workaround.

- CSCtl05941

  Symptoms: CUBE crashes.

  Conditions: This symptom is observed when voice HA is configured on CUBE.

  Workaround: There is no workaround.

- CSCtl67195

  Symptoms: The following three BGP debug commands are not allowed to enable:

  debug ip bgp vpnv4 unicast
  debug ip bgp vpnv6 unicast
  debug ip bgp ipv6 unicast

  Conditions: The symptom is observed with the above BGP debug commands.

  Workaround: There is no workaround.

- CSCtl71478

  Symptoms: In an HA system, the following error message is displayed on the standby RP and LC:

  ```
  "OCE-DFC4-3-GENERAL: MPLS lookup unexpected"
  ```

  Conditions: This symptom is observed on standby/LC modules when you bring up both the RP and standby/LC routers with or without any configuration.

  Workaround: There is no workaround.

- CSCtl74163

  Symptoms: Some PPPoEoA PVCs that are configured with Auto VC feature may fail to disconnect after idle timeout timer expires.

  Conditions: The issue is observed on Cisco IOS ASR1006 router when the traffic generator creates 4000 PPPoEoA sessions for every ATM interface.

  Workaround: Perform shut and no shut to clear the VCs.

- CSCtl77735

  Symptoms: Saving a configuration to NVRAM may fail.

  Conditions: This symptom may be observed on a Cisco 2900 platform while saving the Cisco IOS configuration.

  Workaround: Erasing the startup configuration and saving again may recover the configuration.

- CSCtl87067

  Symptoms: Priority class will drop traffic before explicit police rate is reached.

  Conditions: This symptom is observed on Cisco ISR platforms when strict priority with explicit police is configured.

  Workaround: There is no workaround.

- CSCtl87879

  Symptoms: MGCP calls fail as the DTMF detection and reporting via NTFY message does not occur.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T5 but not in Cisco IOS Release 12.4(24)T4

  Workaround: There is no workaround.

- CSCtl88066

  Symptoms: A router reloads (seen with a Cisco ASR 1000 Series Aggregation Services router) or produces a spurious memory access (seen with most other platforms).

  Conditions: The symptom is observed when BGP is configured and you issue one of the following commands:

  show ip bgp all attr nexthop
  show ip bgp all attr nexthop rib-filter

  Workaround: Do not issue either of these commands with the "all" keyword. Instead, issue the address-family specific version of the command for the address family you are interested in.

  For example, the following are safe:

  show ip bgp ipv4 unicast attr nexthop
  show ip bgp attr nexthop
  show ip bgp vpnv4 vrf *vrfname* **attr nexthop**

  Further Problem Description: While the **show ip bgp all attr nexthop** has never done anything that **show ip bgp attr nexthop** did not do, the reload bug was introduced during the development of multi-topology routing. All versions of Cisco IOS which include multi-topology routing or which are derived from versions which included multi-topology routing, and where this fix is not integrated are impacted.

  The fix prevents the issuing of commands beginning with **show ip bgp all attr**.

- CSCtl92210

  Symptoms: A Cisco router may crash when trying to show the session objects while session queue is being managed (addition/removal).

  Conditions: This symptom is observed when new sessions are being provisioned or removed from mediatrace initiator side. The router may crash when trying to show the session objects while the session queue is being managed (addition/removal) or when the **no mediatrace responder** command is entered.

  Workaround: User can only avoid using show "mediatrace responder sessions" command if additions or removals are being done at Mediatrace responder node.

- CSCtl98270

  Symptoms: Changing the VC hold-queue under the PVC on a WIC-1ADSL card is not reflected correctly in the **show hqf interface** output.

  Conditions: The symptom is observed in Cisco IOS Release 15.1(2)T2 and later releases.

  Workaround: Execute a shut/no shut to fix the issue.

- CSCtn01047

  Symptoms: Firewall service-policy attachment failed.

  Conditions: This symptom is observed with Zone Based Firewall.

  Workaround: There is no workaround.

- CSCtn01832

  Symptoms: The following command sequence crashes the router at check syntax mode:

  config check syntax route-map hello match local-preference no match local-preference

  Conditions: The symptom is observed with the commands above.

  Workaround: There is no workaround.

- CSCtn09135

  Symptoms: MC5728V modem is not enumerated resulting in cellular interface not coming up.

  Conditions: This symptom occurs more often with USB flash attached and on DSL SKUs versus non-DSL SKUs.

  Workaround: Removing the USB flash solves the issue in some instances.

- CSCtn10922

  Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic and in some cases may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.

  Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.

  Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.

- CSCtn21154

  Symptoms: A crash occurs at mace_dp_update_post_mace_metrics.

  Conditions: This symptom is observed when MACE and NAT are configured together.

  Workaround: Do not configure NAT along with MACE.

- CSCtn27599

  Symptoms: The OIR of NM-1T3/E3 line card crashes the router.

  Conditions: This symptom is observed only on the Cisco 3945 router.

  Workaround: There is no workaround.

- CSCtn37743

  Symptoms: Egress interface is not correct as observed by Mediatrace responder. This can impact monitoring on perf-traffic and system profiles.

  Conditions: This symptom is observed on a node where it has both initiator and responder, when the responder has both high and low cost routes and when the interface is changed, the change is detected but the egress is not reflected.

  Workaround: Remove the original session and re-add it.

- CSCtn39632

  Symptoms: An RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.

  Conditions: This symptom is observed on a Cisco ASR router configured for RSA key encryption with a keyring name having more than 8 characters.

  Workaround: Modify the keyring name to be less than 8 characters.

- CSCtn46263

  Symptoms: Memory leaks are seen in ikev2_packet_enqueue and ikev2_hash.

  Conditions: This symptom is observed during retransmissions and window throttling of requests.

  Workaround: There is no workaround.

- CSCtn51740

  Symptoms: Memory leak is seen in EzVPN process.

Conditions: This symptom is seen when EzVPN connection is configured with split tunnel attributes.

Workaround: There is no workaround.

- CSCtn54985

  Symptoms: The status of a LSP health monitor with LSP discovery is shown as “unknown.”

  Conditions: This symptom is observed on “PE” routers in an MPLS VPN scenario when configured with LSP health monitors.

  Workaround: There is no workaround.

- CSCtn55187

  Symptoms: Memory leaks are seen at ikev2_ipsec_add_proxy_to_list, ikev2_skeyseed_create and ikev2_ios_get_ipv6_pak on Cisco 2900 and 3900 platform router, respectively.

  Conditions: This symptom is observed on Cisco 2900 and 3900 platform routers.

  Workaround: There is no workaround.

  Further Problem Description: Memory leaks are seen after the test has been completed and while trying to check for the memory leaks while testing the feature Tunnel Protection for IPv6 feature.

- CSCtn66356

  Symptoms: Sometimes AP802 Radio module may not be recognized by the AP IOS running on the second CPU core.

  Conditions: Conditions are not know at this time.

  Workaround: There is no workaround.

- CSCtn69929

  Symptoms: The DHCP Server will not assign any addresses to clients, even though Smart-install is configured with DHCP pool parameters.

  Conditions: This symptom is observed when Smart-install is configured to assign DHCP addresses.

  Workaround: Execute “show running-config” on the box once; after that, everything works fine.

- CSCtn74169

  Symptoms: Crash by memory corruption occurs in the process “EzVPN Web-intercept daemon.”

  Conditions: This symptom is observed with an EzVPN connection coming up after HTTP authentication using HTTP Intercept.

  Workaround: Do not use HTTP Intercept.

- CSCtn77154

  Symptoms: The Stateful Inspection Feature is enabled after reload when an “ip nat outside” statement is configured on two interfaces, which results in packets punted to the CPU. This results in overall performance degradation.

  Conditions: This symptom is observed when two outside NAT interfaces are configured.

  Workaround: Configure “ip nbar protocol discovery.”

- CSCtn84628

  Symptoms: A Cisco CGR2010 reports an over-temperature error message when the system is running in a 60C environment.

  Conditions: This symptom is observed when the environment is at 60C.

Workaround: Ignore the error message from the sys log.

- CSCto00318

  Symptoms: An SSH session initiated from a router running Cisco IOS 15.x releases may cause the router to reboot.

  Conditions: This symptom is observed with Cisco IOS 15.x releases.

  Workaround: Do not initiate SSE sessions; otherwise, there is no workaround.