Caveats for Cisco IOS Release 15.2(1)T

Caveats

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

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

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

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

This document contains the following sections:

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

Resolved Caveats—Cisco IOS Release 15.2(1)T4

- CSCtj10515

  Symptoms: Crash seen in IGMP input process.

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

  Workaround: There is no workaround.

- CSCtj95182

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

  Conditions: Network scanner run against a 3750 running 12.2.55.SE.

  Workaround: There is no workaround.

  Additional Information: Vulnerable versions:

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

  First fixed in: 12.2(55)SE5, 15.0(1)EX, 15.1(1)SG, 15.2(1)E, 15.2(4)M, 15.3(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

- CSCtq14253

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

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

  Workaround: Reload all routers in the setup.

- CSCts08224

  Symptoms: Expected ACL/sessions not found for most of the protocols.

  Conditions: The symptom is observed with expected ACL/sessions.

  Workaround: There is no workaround.

- 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 warm reboot feature).

- CSCtu08373

  Symptoms: Router crashes at various decodes including fw_dp_base_process_pregen and cce_add_super_7_tuple_db_entry_common.

  Conditions: IOS firewall is configured and traffic is flowing through the router.

  Workaround: There is no workaround.

- CSCtu28696

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

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

  Workaround: There is no workaround.

- CSCtw78539

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

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

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

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

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

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

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

- CSCtx56174

  Symptoms: Cisco router hangs until a manual power cycle is done. If the **scheduler isr-watchdog** command is configured, the device will crash and recover instead of hanging until a power cycle is done.

  Conditions: This is seen with websense URL filtering enabled and with zone based firewalls.

  Workaround: Disable URL-based filtering.

- CSCtz35999

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

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is available at the following link:

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

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

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

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

- 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.

- 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.

- CSCtz71084

  Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.

  Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:

  ```
  CE0---------PE0---------RR | | | | CE1---------PE1---------|
  ```

  Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.

  This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix: no network x.x.x.x mask y.y.y.y

  Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external, and is day 1 issue with all.

  Workaround: Hard clear.

- CSCua12317

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

  Conditions: This symptom is observed with the following conditions:

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

  Workaround:

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

- CSCua15292

  Symptoms: Router may crash unexpectedly with crypto in running-configuration.

Conditions: The symptom is observed with a router running at normal operation. When it crashes, the error message below is found in the crashinfo file:

```
%CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=172.8.9.8, prot=50, spi=0xE8FB045F(3908764767), srcaddr=10.0.100.1, input
interface=GigabitEthernet0/0
```

Workaround: There is no workaround.

- CSCua39390

  Symptoms: The PRI configuration (voice port) is removed after a reload:

```
interface Serial1/0:23          ^
% Invalid input detected at '^' marker.
no ip address
% Incomplete command.
encapsulation hdlc
   ^
% Invalid input detected at '^' marker.
isdn incoming-voice voice
       ^
% Invalid input detected at '^' marker.
no cdp enable
        ^
% Invalid input detected at '^' marker.
voice-port 1/0:23
           ^
% Invalid input detected at '^' marker.
```

  Also getting trace back:

```
%SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "Init", ipl= 3, pid= 3 -Traceback=
0x607EE41Cz 0x630F0478z 0x607F72C0z 0x60722F38z 0x6070A300z 0x6070A9CCz 0x603E1680z
0x6029541Cz 0x60298F6Cz 0x6029AD48z 0x6029D384z 0x6062BC68z 0x60632424z 0x60635764z
0x60635CE0z 0x60877F2Cz %SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "Init",
ipl= 3, pid= 3 -Traceback= 0x607EE41Cz 0x630F04E4z 0x607F7154z
```

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T and Release 15.1(4)M4. The issue is not occurring with Cisco IOS Release 12.4(24)T6 or lower. The issue occurs after reload.

  Workaround: Reapply configuration after router comes back up.

- CSCua40273

  Symptoms: The ASR1k crashes when displaying MPLS VPN MIB information.

  Conditions: Occurs on the ASR1K with version 15.1(02)S software.

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

- CSCua55629

  Symptoms: SIP memory leak seen in the event SIPSPI_EV_CC_MEDIA_EVENT.

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

```
Adding blocks for GD...

                I/O memory

Address    Size   Alloc_pc  PID  Alloc-Proc       Name

                Processor memory

Address    Size   Alloc_pc  PID  Alloc-Proc       Name
```

```
 286E144     6128  8091528  398  CCSIP_SPI_CONTR CCSIP_SPI_CONTROL
```

Workaround: There is no workaround.

- 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.

- 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

- CSCub69976

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

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

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

- CSCuc07799

  Symptoms: The router crashes while booting with Cisco IOS Release 15.2(4)M weekly images.

  Conditions: This symptom occurs when the ISM-VPN Module is inserted in the router. WCCP and RG-Infra features are also enable.

  Workaround: There is no workaround.

- CSCuc56259

  Symptoms: A Cisco IOS router (so far only seen on 15.1 and newer), 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
  Delivery Ack could not be sent due to lack of buffers.
  ```

  and/or

  ```
  %SYS-6-STACKLOW: Stack for process IP Input running low, 0/12000
  ```

  Conditions: This happens when a media loop is created (which is due to misconfiguration or some other call forward/transfer scenarios).

  Workaround: Check the configurations for any misconfigurations, especially with calls involving CUBE and CUCM.

- CSCuc67033

  Symptoms: A Cisco IOS router with the ISM VPN encryption module enabled can experience memory corruption-related crashes.

  Just before the crash, the router may display some syslog error messages related to the ISM VPN module:

```
Aug 21 15:55:22: !!! Cannot find Revt counters struct for flowid: 0x4400012A
Aug 21 15:55:24: !!! Cannot find Revt counters struct for flowid: 0x4400012A
Aug 21 15:55:24: !!! Cannot find Revt counters struct for flowid: 0x4400012A
```

Here, the word "Revt" is specific for the ISM VPN module.

Also, some generic syslog error messages related to memory allocation failures may be displayed the crash:

```
Aug 21 15:55:33: %SYS-3-BADBLOCK: Bad block pointer DD7D7D0
-Traceback= 23B9EA7Cz 23BA1A44z 23BA1E24z 23B712B8z 23B7129Cz
Aug 21 15:55:33: %SYS-6-MTRACE: mallocfree: addr, pc
 352791C4,22DB4A50 352791C4,3000006C 38808760,2627EDF0 34C91824,262724A8
 352791C4,22DB6214 352791C4,22DB4A50 352791C4,3000006C 352791C4,22DB6214
Aug 21 15:55:33: %SYS-6-MTRACE: mallocfree: addr, pc
 352791C4,22DB4A50 352791C4,3000006C 352791C4,22DB6214 3875D9C4,600002CA
 3875D5E0,2627EDF0 35092ACC,262724A8 352791C4,22DB4A50 352791C4,3000006C
Aug 21 15:55:33: %SYS-6-BLKINFO: Corrupted next pointer blk DD7D7D0, words
32808, alloc 214E636C, InUse, dealloc 0, rfcnt 1
```

Conditions: This symptom is observed with the following conditions:

- The ISM VPN crypto acceleration module is installed, enabled, and used for crypto operations (IPsec, etc.).
- Cisco IOS supports ISM VPN (Cisco IOS Release 15.2(1)T1 or later releases).

Workaround: Disable the ISM VPN module. The crash is specific to ISM VPN.

- CSCuc82992

  Symptoms: The router crashes upon execution of "no crypto engine slot 0", when RG-infra feature is enabled.

  Conditions: This symptom occurs when RG-Infra and ISM-VPN are configured and when issuing "no crypto engine slot 0".

  Workaround: There is no workaround.

- CSCud02361

  Symptoms: Sequence number of spoofed ACK sent to the server has a 0x00 value.

  Conditions: Once the max-incomplete high is reached, when the next SYN packet is sent from the client, the UUT sends a SPOOFED-ACK after getting the SYN-ACK from the server. When this ACK packet is observed at the server pagent with the packets tool, the sequence number is found to be 0x00.

  Workaround: There is no workaround.

- CSCue94880

  Symptoms: 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).

Resolved Caveats—Cisco IOS Release 15.2(1)T3a

Cisco IOS Release 15.2(1)T3a is a rebuild release for Cisco IOS Release 15.2(1)T. The caveats in this section are resolved in Cisco IOS Release 15.2(1)T3a but may be open in previous Cisco IOS releases.

- CSCub16372

Symptoms: In extremely rare cases, Cisco ISR-G2 cannot boot up with certain ROMMON versions with the error “Signature did not verify”.

So far, only one image is found to have this problem: c3900-universalk9-mz.SPA.152-1.T3.bin.

Conditions: The issue will happen when the following conditions are met at the same time:

1. The platform is affected.
2. The ROMMON version running at the router is within the affected ROMMON version range.
3. The first calculated hash value is 0 during the Cisco IOS image building process.

Since it is extremely rare that the third condition will happen, so far only one image is found to have this problem.

Workaround: There is no workaround.

Upgrading ROMMON to the latest version of Cisco IOS 15.0(1r)M16 or 15.1(1r)T5 will fix the issue completely.

The ROMMON upgrade can be done using one single CLI command in the router's enable mode:

Router# upgrade rom-monitor file flash:<ROMMON_file_name>

<ROMMON_file_name> is the ROMMON file name for the specific platform that is downloadable from cisco.com. For example, C3900_RM2.srec.SPA.150-1r.M16 is the latest ROMMON version for Cisco C39xx platforms located at the cisco.com download site:

http://www.cisco.com/cisco/software/release.html?mdfid=282774222&flowid=7437&softwareid=280805687&release=15.0%281r%29M16&relind=AVAILABLE&rellifecycle=&reltype=latest

Resolved Caveats—Cisco IOS Release 15.2(1)T3

Cisco IOS Release 15.2(1)T3 is a rebuild release for Cisco IOS Release 15.2(1)T. The caveats in this section are resolved in Cisco IOS Release 15.2(1)T3 but may be open in previous Cisco IOS releases.

- CSCtj48387

  Symptoms: After a few days of operation, a Cisco ASR router that is running as an LNS box, crashes with DHCP related errors.

  Conditions: This symptom occurs when DHCP enabled and sessions get DHCP information from a RADIUS server.

  Workaround: There is no workaround.

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

- CSCtl73132

  Symptoms: Router may crash and reset when the **show ipc hog- info** or **show tech-support ipc** commands are run repetitively on either the switch processor or route processor.

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

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

- CSCtl90292

  Symptoms: 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 on EOBC buffers list for really long time like weeks or more.

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.

- 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.

- 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: Disable Flexible NetFlow on all interfaces.

- 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 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.

- 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.

- CSCto70391

  Symptoms: Under policy-map when bandwidth CLI is removed and switch-over, the standby reboots continuously.

Conditions: The standby continuously reboots.

Workaround: There is no workaround.

- CSCto77352

  Symptoms: Standby cannot reach HOT sync state with active. Standby RP will keep resetting. The following messages are printed:

  ```
  %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 a Cisco ASR 1000 series router is configured with ISG as DHCP server and with low DHCP lease timer.

  Workaround: There is no workaround.

- CSCtq14817

  Symptom: Traceback or crash might happen when PPTP related traffics were passing through NAT configured device.

  Conditions: A race condition when PPTP packets were subjected to NAT, that might cause NAT to behave improperly and cause the issue.

  Workaround: There is no workaround.

- CSCtq20168

  Symptoms: Chunk leak is seen at ipc_init_message_system.

  Conditions: This symptom is seen with the **test ipc port send 0 0 rpc type 0 1 1** command.

  Workaround: There is no workaround.

- CSCtq24557

  Symptoms: Router crash after deleting multiple VRFs. This happens very rarely.

  Conditions: The symptom is observed in a large scale scenario.

  Workaround: There is no workaround.

- 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. 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 packetization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq57742

  Symptoms: Router crashes for corrupted chunk memory when BGP neighbor is shutdown.

  Conditions: This symptom is seen with BGP and IPv6 configuration.

  Workaround: There is no workaround.

- 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 “ip routing protocol purge interface”.

- CSCtq60703

  Symptoms: The device crashes and traceback is seen when executing **write network**.

  Conditions: The symptom is observed when the command **write network** is used with no URL specified.

  Workaround: Specify a URL.

- 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.

- CSCtq85564

  Symptoms: The fix of CSCto77352 may cause a data corruption problem.

  Conditions: This symptom is seen when two processes are calling the same function that is raising the race condition.

  Workaround: There is no workaround.

- 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.

- CSCtq91305

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

%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.

- CSCtq97883

  Symptoms: Traceback is shown. The root cause is a null pointer.

  Conditions: The symptom is observed during longevity testing of Cisco IOS Release 12.4(24)GC3a and Release 15.1(2)GC.

  Workaround: There is no workaround.

- CSCtr45287

  Symptoms: Router crashes in a scale DVTI scenario.

  Conditions: The symptom is observed when the IPsec tunnel count reaches around 2500.

  Workaround: Use fewer tunnels or use a different platform.

- 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

- CSCtr53944

  Symptoms: IPv6 unicast packets are dropped.

  Conditions: The symptom is observed when there is a breakage in VMI fastpath when passing IPv6 unicast packets.

  Workaround: There is no workaround.

- CSCtr54327

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

  Conditions: This symptom is observed on a voice gateway that is configured with transcoding and fax passthrough. When a fax call comes in for a codec, but is not configured for a codec, then the “a=silenceSupp:off” option is set in SDP.

  Workaround: Disable fax by going into the “voice service voip” mode and configuring the **fax protocol none** command.

- 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.

- CSCtr86328

  Symptoms: A device that is running Cisco IOS might reload when the web browser refreshes or reloads the SSL VPN portal page.

  Conditions: This symptom is observed on a Cisco IOS device that is configured for clientless SSL VPN.

  Workaround: There is no workaround.

  Further Problem Description: This problem has been seen when the stock Android browser visits the SSL VPN portal (after authentication) and refreshes (reloads) the page. However, the issue is not browser-specific and other browsers might trigger the issue too.

  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-2012-1344 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

- 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.

- CSCtr92202

  Symptoms: Compilation failure is seen with version gcc.c4.2.1.

  Conditions: This symptom occurs when compiling images using gcc.c4.2.1.

  Workaround: There is no workaround.

- 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.

- 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
```

- 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.

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

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

- CSCts68541

  Symptoms: In IPsec scaling test, when CPE is keeping reload, all IPsec sessions will be torn down and reestablished. During the session flapping, RP reset is observed sometimes.

  Conditions: This symptom is seen with CPE reloading continually.

  Workaround: There is no workaround.

- 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.

- CSCts72911

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

  Conditions: The symptom is observed after an SSO switchover in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the non-restarting router does not send back the corresponding VPN prefixes towards the restarted router.

  Workaround: There is no workaround.

- CSCtt02313

  Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.

  Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.

  Workaround: There is no workaround.

- CSCtt26074

  Symptoms: Memory leak with IP SLAs XOS Even process.

  Conditions: The symptom is observed with IP SLA configured.

  Workaround: There is no workaround.

- CSCtt26692

  Symptoms: Router crashes due to memory corruption. In the crashinfo you may see:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk xxxxxxx data
  xxxxxxxx chunkmagic xxxxxxxx chunk_freemagic EF4321CD -
  Process= "CCSIP_SPI_CONTROL", ipl= 0, pid= 374
  chunk_diagnose, code = 1
  chunk name is MallocLite
  ```

  Conditions: Router is configured for SIP. When a translation-rule is configured to translate a number to one with more digits, the router may crash when the translation takes effect, such as when a call is forwarded.

  Workaround: Configuring “no memory lite” configurations can be used as a workaround in some cases (depending on the length of the phone numbers), but will cause the router to use more memory. If the translation-profile is configured to translate forwarded calls, then avoid or disable the option to forward the call.

- 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.

- CSCtt37516

  Symptoms: Line card crash with priority traffic when QoS policy is applied. The defect impacts the distributed system, 7600, with line card using software data plane implementation, Enh Flex or SIP200, when priotiy feature is enable with mlppp/mlpFR interleaving.

Conditions: The symptom is observed with the QoS priority feature. When interleaving is enabled, add/remove/modify priority feature will trigger this defect with live traffic.

Workaround: There is no workaround.

- CSCtu32301

  Symptoms: Memory leak may be seen.

  Conditions: This is seen when running large **show** commands like **show tech-support** on the line card via the RP console.

  Workaround: Do not run the show commands frequently.

- CSCtu40028

  Symptoms: The SCHED process crashes.

  Conditions: The issue occurs after initiating TFTP copy.

  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.

- CSCtv36812

  Symptoms: Incorrect crashInfo file name is displayed during crash.

  Conditions: The symptom is observed whenever a crash occurs.

  Workaround: There is no workaround.

- CSCtw45055

  Symptoms: A Cisco ASR 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:

```
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
%BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold
time expired) x bytes
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification
received
```

```
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session  Neighbor deleted
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session  Neighbor deleted
%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. When the **no ntp server** *hostname* command is issued later on the active, the standby reloads because the configuration was not added.

  Conditions: When the device is reloaded or when the DNS name is not resolved, the configuration is not added. It is seen after the standby sync failure, then issuing the **no ntp server** *hostname*.

  Workaround: Use IP/IPv6 addresses instead of the hostname for NTP configurations. The IP/IPv6 address can be found by pinging the hostname.

- CSCtw46229

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

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

  Workaround: Ensure all your PPP connections stay stable.

- CSCtw55976

  Cisco IOS Software contains a vulnerability in the Intrusion Prevention System (IPS) feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if specific Cisco IOS IPS configurations exist.

  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-20120926-ios-ips

- CSCtw61872

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

  Conditions: The symptom is observed when executing a complex sort with top- talkers on a show command from multiple CLI sessions (note that normal show commands without top-talkers are fine):

sh flow monitor QoS_Monitor cache sort highest counter packets top 1000 sh flow monitor QoS_Monitor cache sort highest counter packets top 10000

Workaround: Do not execute complex sorts with top-talkers on the show output from multiple CLI sessions.

- CSCtw62310

  Symptoms: The **cells** keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service- policy”.

  Conditions: The symptom is observed when removing the policy-map from map-class.

  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw71564

  Symptoms: Not all data packets are accounted for in the “show stats” output of the video operation.

  Conditions: The symptom is observed with heavy load on the responder caused either by many video sessions or other processes.

  Workaround: Reduce processor load on device running the responder.

- CSCtw84664

  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

- CSCtw88094

  Symptoms: The standby management processor reloads during configuration sync when there is a mismatch in the IP SLA configuration.

  Conditions: This symptom occurs shortly after the “ip sla schedule X start specific_start_time” command is issued multiple times on the same probe instance. Hence, when the configuration is synced to the standby management processor, a PRC error occurs. The PRC error causes a reload of the standby management processor.

  Workaround: Unschedule the probe before rescheduling for a specific start time.

- CSCtx01604

  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.

  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.

  Workaround: Do not use any dynamic network interface IP address as CNS ID.

- 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.

- 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. Insure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- 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.

- 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 on Cisco IOS 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.
  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

- 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.

- CSCtx56174

  Symptoms: Cisco router hangs until a manual power cycle is done. If the scheduler **isr-watchdog** command is configured, the device will crash and recover instead of hanging until a power cycle is done.

  Conditions: This is seen with websense URL filtering enabled and with zone based firewalls.

  Workaround: Disable URL-based filtering.

- CSCtx57784

  Symptoms: Device crashes while configuring “logging persistent url”.

  Conditions: Occurs when the destination file system has zero free bytes left.

  Workaround: There is no workaround.

- CSCtx66804

  Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFREQ.

  Conditions: The symptom is observed with the following conditions:

  – “ppp lcp delay 0” is configured.
  – The symptom can be seen on Cisco IOS Release 15.0(1)M5.

  Workaround: Set delay timer without 0.

- CSCtx68100

  Symptoms: On a system having SP-RP, the reload reason is not displayed correctly. Once the system crashes, in all subsequent reloads the last reload reason is displayed as crash.

  Conditions: The symptom is observed on a system having SP-RP. The reload reason is shown wrongly when the **show version** CLI is executed.

  Workaround: There is no workaround.

- CSCtx74342

  Symptoms: After interface goes down or is OIRed, in a routing table you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next hop interface set to the interface that is down.

  Conditions: The symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 sec default).

  Workaround: Configuring SPF throttle timer can change the interval.

  Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

```
Router show ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
```

```
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/64 [110/10]
     via Ethernet0/0, directly connected
```

- CSCtx86539

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

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

  Workaround: There is no workaround.

- 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.

- CSCty05092

  Symptoms: EIGRP advertises the connected route of an interface which is shut down.

  Conditions: This symptom is observed under the following conditions:

  1. Configure EIGRP on an interface.
  2. Configure an IP address with a supernet mask on the above interface.
  3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.

  Workaround 1: Remove and add INTERFACE VLAN xx.

  Workaround 2: Clear ip eigrp topology x.x.x.x/y.

- CSCty05150

  Symptoms: After SSO, an ABR fails to generate summary LSAs (including a default route) into a stub area.

  Conditions: This symptom occurs when the stub ABR is configured in a VRF without “capability vrf-lite” configured, generating either a summary or default route into the stub area. The issue will only be seen after a supervisor SSO.

Workaround: Remove and reconfigure “area x stub”.

- 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.

- CSCty32232

  Symptoms: BRI interface is not showing as monitored.

  Conditions: The issue occurs after performing an on-line insertion/removal of an NM-16ESW module.

  Workaround: Reload the router.

- CSCty32851

  Symptoms: A Cisco router may unexpectedly reload due to software forced crash exception when changing the encapsulation on a serial interface to “multilink ppp”.

  Conditions: The symptom is observed when the interface is configured with a VRF.

  Workaround: Shut down the interface before making the encap configuration change.

- CSCty41067

  Symptoms: Router crashes while doing an SSO without any configurations.

  Conditions: The symptom is observed while doing an SSO.

  Workaround: There is no workaround.

- CSCty54434

  Symptoms: ISRG2 with ISM VPN is not bringing up more than one tunnel in a crypto map-based scenario. This can happen with either certificates or PSK.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T and Cisco IOS Release 15.2(2)T.

  Workaround: Configure IKEv2 fragmentation so that the fragmentation/reassembly is handled by IKE code rather than by IPsec.

- 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.

- CSCty65189

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

  Conditions: The symptom is observed when ZBFW is configured.

  Workaround: There is no workaround.

- CSCty65334

  Symptoms: Unconfigured crypto ACL causes the Cisco 3900 router to crash.

Conditions: This symptom is observed with a Cisco 3900 image with ISM crypto engine installed and enabled. This may also affect the Cisco 2900 and Cisco 1900 routers with ISM crypto engine installed and enabled.

Workaround: When changing the crypto ACL configuration, disable the ISM crypto engine first using the **no crypto engine** *slot 0* command, and then change the ACL. After changing the ACL, reload the router with ISM enabled.

- 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(1)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.

- CSCty80553

  Symptoms: Multicast router crashes.

  Conditions: The symptom is observed when multicast traffic is routed through an IPsec tunnel and multicast packets are big causing fragmentation.

  Workaround: Make sure that multicast packet sizes do not exceed tunnel transport MTU.

- CSCty86039

  Symptoms: Shut down the physical interface of tunnel source interface. The router crashes with traffic going through some of the tunnels.

  Conditions: This symptom is seen with tunnel interface with QoS policy installed.

  Workaround: There is no workaround.

- CSCty94289

  Symptoms: The drop rate is nearly 1 Mbps with priority configuration.

  Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.

  Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

- CSCty96052

  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

Conditions: It is an extreme corner case/timing issue. Has been observed only once on release image.

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

- CSCty97961

  Symptoms: Device configured with SSLVPN crashes.

  Conditions: Device configured with SSLVPN and **functions svc-enabled** or **functions svc-required** and **svc dtls** and has an outbound ACL on one of the devices 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 outbound ACL, or **no svc dtls** if running Cisco IOS Software that has a fix for Cisco bug ID CSCte41827.

  Further Problem Description: This bug covers configurations that have DTLS enabled on the device. A corresponding Cisco Bug ID CSCte41827, deals with a similar vulnerability but when the device does not have DTLS configured.

  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-2012-3924 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

- CSCty98834

  Symptoms: The Cisco c2900, c3900, and c1900 IOS with the ISM VPN crypto engine might crash after some time when you run out of memory on the ISM VPN engine as there are memory leaks during rekey.

  Conditions: This symptom occurs when the ISM VPN crypto engine is enabled.

  Workaround: Disable the ISM VPN module using the **no crypto engine** *slot 0* command.

- 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 on a device that 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

- CSCtz13465

  Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.

  Conditions: This symptom is observed with an interface with a policy installed.

  Workaround: There is no workaround.

- CSCtz13818

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

  Conditions: The symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.

  Workaround 1: Refresh the updated route-target to use **clear ip route vrf** *vrf-name net mask*.

  Workaround 2: Hard clear the BGP session with the peer.

- CSCtz25364

  Symptoms: GM to GM communication between ISM VPN and the Cisco ASR 1000 series router with TBAR enabled is broken.

  Conditions: This symptom occurs when ISM VPN and the Cisco ASR 1000 series router are GMs and TBAR is enabled.

  Workaround: Disable ISM VPN or disable TBAR and switch to counter-based anti-replay.

- CSCtz26735

  Symptoms: SDP process to provision CVO router is broken in Cisco IOS Release 15.2(3)T.

  Conditions: This symptom is seen when we start the SDP process. The connection immediately breaks after the username and password are entered.

  Workaround: There is no workaround.

- 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.

- CSCtz44989

  Symptoms: A EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.

  Conditions: The issue is seen with IPv6 link-local nexthop. When the EIGRP route is redistributed to BGP VRF, it clears the nexthop information (it become 0.0.0.0). Now this route becomes invalid and BGP is not able to export to another VRF.

  Workaround: There is no workaround.

- CSCtz51773

  Symptoms: High CPU seen on routers equipped with an ISM-VPN module. The output of **show process cpu** shows that the process "REVT Background" is using around 70% of the CPU cycles.

  The ISM-VPN module is not visible in **show diag**, and the output of **show crypto engine configuration** indicates that the module status is DEAD.

  Conditions: The symptom is observed with an ISM VPN with a few IPSec tunnels. This can take between a day and a week.

  Workaround 1: Reload the router.

  Workaround 2: For a longer-run workaround and if the traffic volume is not too high, switch to the onboard crypto hardware using the configuration **no crypto engine slot 0**.

- CSCtz58719

  Symptoms: Watchdog timeout under interrupt or process

  Conditions: The 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

- 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.

- 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: Router may crash with breakpoint exception.

  Conditions: The symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.

  Workaround: Disable SNMP IPv6 polling.

- CSCua39107

  Symptoms: In a FlexVPN Spoke to Spoke setup, Resolution reply goes via the Tunnel interface to the Hub.

  Conditions: This symptom is only observed when NHO is added for the V-Access, overriding an existing route. This issue is not seen when H route is added.

  Workaround: Distribute the summarized address from the Hub, thus avoiding addition of NHO at the Spokes. The Spokes will then add H route instead of NHO.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

  Conditions: The issue is seen on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua47570

  Symptoms: The **show ospfv3 event** command can crash the router.

  Conditions: The symptom is observed when "ipv4 address family" is configured and redistribution into OSPFv3 from other routing protocols is configured.

  Workaround: Do not use the **show ospfv3 event** command.

- CSCua67998

  Symptoms: System crashes.

  Conditions: This symptom occurs after adding or removing a policy-map to a scaled GRE tunnel configuration.

  Workaround: There is no workaround.

- CSCub17794

  Symptoms: Cisco 819G routers with HSPA+ modems (8705 modems) will crash on bootup.

  Conditions: This symptom is observed in Cisco IOS interim Release 15.2(1)T2.8.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(1)T2

Cisco IOS Release 15.2(1)T2 is a rebuild release for Cisco IOS Release 15.2(1)T. The caveats in this section are resolved in Cisco IOS Release 15.2(1)T2 but may be open in previous Cisco IOS releases.

- CSCtc96631

  Symptoms: Packet drops occur in downstream devices every 4ms burst from shaper.

  Conditions: The symptom is observed when shaping at high rates on very fast interface types with low memory buffer devices downstream.

  Workaround: Use ASRs instead of ISR.

- CSCtj30238

  Symptoms: WRED counters are wrongly updated. The default counter should be 0, but the counter is wrongly updated. All the WRED subclasses show the same count. Counters are shown for WRED subclasses for which there are no traffic matches in the class.

  Conditions: This issue is seen on the Cisco 7600 router with ES+ line card only. The Es+ line card does not support per WRED class based counters. There was a recent breakage due to the Transmit packets/bytes column that started showing up for the Es+ line card. This is wrong. As ES+ writes same value to WRED transmit count (not the per subclass base count, but total count), this value does not make sense.

  Workaround: Do not use WRED subclass Transmit packets/bytes counters for ES+ line card on the Cisco 7600 router.

- CSCtk00181

  Symptoms: Password aging with crypto configuration fails.

  Conditions: The symptom is observed when Windows AD is set with “Password expires on next log on” and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Auth failure.

  Workaround: There is no workaround.

- CSCtl04112

  Symptoms: Switch/router reloads whenever NAS receives a state attribute in a COA request.

  Conditions: While parsing a COA request, a state attribute is decoded twice and the original pointer is moved ahead so that the next attribute type and length are wrong. This causes a loop which never exits.

  Workaround: Ensure state attribute is not received in a COA request.

- CSCtl52854

  Symptoms: Client does not receive multicast traffic when it is connected to an EHWIC port in access mode.

  Conditions: The 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.

- 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.

- 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.

- 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

- 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.

- 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.

- CSCtq17082

  Symptoms: Router reloads.

  Conditions: The symptom is observed with at least 2000 IPSec tunnel sessions by automatic script to remove a QoS configuration from Virtual Template.

  Workaround: Session teardown before you remove the QoS configuration.

- CSCtq21234

  Symptoms: Label is not freed.

  Conditions: The symptom is observed after shutting down the link.

  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.

- CSCtq32282

  Symptoms: Chunk leaks observed on various platforms.

  Conditions: The issue seen while testing the ipsec_unity_solaris functionality.

  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

- CSCtq61128

  Symptom: 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

- 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

- CSCtq68778

  Symptoms: After an ISSU, the reload reason string is missing in the newly- active session.

  Conditions: The symptom is observed after an ISSU.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCtr01750

  Symptoms: The command **clear ip nat translation *** is not working as expected.

  Conditions: Issue is seen with a Cisco 7200 platform that is running the Cisco 15.2 (0.19)T0.1 image. This issue is specific to the NAT translations created for ICMP traffic sent with port number 0.

  Workaround: There is no workaround.

- 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.

- CSCtr11469

  Symptoms: CNS configurations might crash the HA system, especially on the standby side.

  Conditions: The symptom is observed when CNS features run on any HA system.

  Workaround: Do not use CNS features on HA system.

- CSCtr14675

  Symptoms: The line card crashes after removing the child policy in traffic.

  Conditions: This symptom occurs after the child policy is removed in traffic.

  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.

- CSCtr25386

  Symptoms: BFDv6 static route association fails after reenabling interfaces.

  Conditions: This symptom is observed after interfaces are reenabled.

  Workaround: There is no workaround.

- CSCtr31496

  Symptoms: The line card crashes after switchover with the multilink configurations.

  Conditions: This symptom occurs after switchover with the multilink configurations.

  Workaround: There is no workaround.

- 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.

- CSCtr35740

  Symptoms: QoS queuing hierarchy not moved to current active link when the previously active link goes down.

  Conditions: The symptom is observed when the DMVPN tunnel active link goes down.

  Workaround: There is no workaround.

- CSCtr45978

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

  Conditions: Device configured with Cisco IOS WAAS, and crafted FTP packets or real HTTP user traffic to internet sites is 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

- 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.

- 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.

- 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.

- 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.

- CSCtr79905

  Symptoms: Error message seen while detaching and reattaching a service policy on an EVC interface.

  Conditions: The symptom is observed when detaching and reattaching the service policy on an EVC interface when port shaper is configured on the interface.

  Workaround: There is no workaround.

- CSCtr81559

  Symptoms: The PPP session fails to come up occasionally on LNS due to a matching magic number.

  Conditions: This symptom is observed during LCP negotiation, when the random magic number generated on the client matches the magic number generated on the LNS. PPP assumes it to be a loopback and disconnects the PPP session. This condition occurs rarely.

  Workaround: To avoid this, renegotiate the LCP. Configure the client using the **retry** command. This may cause the next session to come up correctly.

- CSCtr87740

  Symptoms: A router may crash due to a bus error.

  Conditions: The symptom seems to be related to high traffic and an ongoing rekey taking place.

  Workaround: There is no workaround.

- 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.

- 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

- CSCts11344

  Symptoms: Upon a reload, a router will crash during bootup.

  Conditions: The symptom is observed on a Cisco 3900 series router with “no cry eng slot 0” configured then the configuration is saved in the startup config file. The issue is seen upon a reload.

Workaround: Do not save “no cry eng slot 0” in the config file. If you want to turn off the crypto engine, do it after router boot up.

Further Problem Information: To recover from the crash, first reload an image build before 07/07/2011. Remove “no cry eng slot 0” from the startup configuration then reload the image you are going to use. After the router boots up, configure “cry eng slot 0” to turn off the engine.

- 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.

- 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.

- 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”.

- CSCts55371

  Symptoms: OSPF will not flood link state updates over an interface. The command **show ip ospf flood-list** will show interface entries similar to:

  ```
  Interface Tunnel1, Queue length 181
  Link state retransmission due in 1706165974 msec
  ```
  Note the high value for the retransmission timer.

  Conditions: The symptom is observed with some newer S and T releases including Cisco IOS Release 15.1(2)S, Release 15.1(3)S, and Release 15.2(1)T.

  The issue can occur on interfaces where OSPF has not flooded updates for more than 24 days. This can include interfaces that are newly configured for OSPF if the router has been up longer than that. Interfaces that flood LSAs at least once every 24 days will not be affected.

  Workaround: To clear a hung interface use **clear ip ospf process**.

- CSCts57108

  Symptoms: Standby reloads continuously after ISSU RV.

  Conditions: The symptom is observed during a downgrade scenario where the active is running Cisco IOS Release 15.1 and the standby is running Release 12.2. Cisco IOS Release 15.1 will be syncing “snmp-server enable traps ipsla” keyword to the standby, but the standby does not understand the new keyword.

  Workaround: Remove references to “snmp-server enable traps ipsla” and then perform the downgrade.

- CSCts62082

  Symptoms: Router generates the following message:

  ```
  %NHRP-3-QOS_POLICY_APPLY_FAILED: Failed to apply QoS policy 10M-shape mapped to NHRP
  group xx on interface Tunnelxx, to tunnel x.x.x.x due to policy installation failure
  ```
  Conditions: The symptom is observed when “per-tunnel” QoS is applied and there are more than nine DMVPN spokes. (Up to eight spokes, with QoS applied is fine.)

  Workaround: There is no workaround.

- CSCts63973

  Symptoms: Router configured with ScanSafe can crash with high session testing. This happens very rarely and is not seen frequently.

  Conditions: The symptom is observed when ScanSafe is configured and HTTP sessions are created at a high rate.

  Workaround: There is no workaround.

- 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 disable-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”.

- CSCts67423

  Symptoms: On the Cisco ASR1k and ISR G2 only, call failures occur in the CUBE enterprise with interoperability to third-party SIP devices due to a trailing comma in the Server and User-Agent fields. For example:

  ```
  User-Agent: Cisco-SIPGateway/IOS-15.1(3)S,
  Server: Cisco-SIPGateway/IOS-15.1(3)S,
  ```

  You might see this with Cisco IOS Release 15.2(1)T or other versions. If the trailing comma is present it can cause interoperability issues. If there is no trailing comma, then this defect is not applicable.

  Conditions: This symptom is observed when there is an interoperability problem between the CUBE enterprise and a third-party SIP device. The trailing comma is invalid against RFC 2616 and the third-party SIP device ignores SIP messages from the CUBE.

  Workaround: On both inbound and outbound dial peers, apply a SIP profile similar to the one below, or add the four lines to an existing SIP profile in use.

  ```
  voice class sip-profile 1
   request ANY sip-header User-Agent modify "-15.*," ""
   response ANY sip-header User-Agent modify "-15.*," ""
   request ANY sip-header Server modify "-15.*," ""
   response ANY sip-header Server modify "-15.*," ""

  dial-peer voice 1 voip
   voice-class sip profiles 1
  ```

- 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.

- 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.

- CSCts85459

  Symptoms: Upon a reload, the cellular interface will not negotiate if a crypto map is applied to it.

  Conditions: The symptom is observed on a Cisco 881 router that has a cellular interface which dials to get an IP address and also acts as the VPN gateway. When we reload the router, the cellular interface does not connect if a crypto map is applied and we see IPsec fails to initialize because we do not have an IP address.

  Workaround: This situation remains until we manually remove the crypto map from the cellular interface. Then we see the chat-script starting and the whole dialing procedure starts, then the cellular link is up with an IP address. Then we re-apply the crypto map again and the tunnel works fine.

- CSCts88467

  Symptoms: Drops happen earlier than expected.

  Conditions: This symptom occurs if the queue-limit is incorrectly calculated.

  Workaround: Configure a queue-limit explicitly to fix this issue, then remove and reapply the policy. Configuring queue-limit in parent policy automatically triggers calculation based on the parent queue-limit value on the child queue-limits based on bandwidth allocated to various classes.

- CSCtt05316

  Symptoms: Under **show content-scan sessions active**, the usergroup information is printed over and over.

  Conditions: The symptom is observed when the TCP SYN is retransmitted.

  Workaround: There is no workaround.

- 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.

- 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.

- 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

- CSCtt17762

  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.

  Conditions: The symptom is observed on an IP PIM multicast network.

  Workaround: There is no workaround.

- 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.

- CSCtt19027

  Symptoms: When ACL is applied to the serial interface or Gigabit interface, ping failure seen even though the permit statement is there.

  Conditions: The symptom is observed when ACL is configured on the serial interface or Gigabit interface.

  Workaround: Enable EPM by installing the security license.

  Further Problem Description: This is seen with those images where EPM is not supported and because of that an EPM call always gives a return value as “deny” due to registry call.

- 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.

- CSCtt28703

  Symptoms: VPN client with RSA-SIG can access a profile where his 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

- CSCtt33158

  Symptoms: If WRED is already present and the queue limit is configured in packets then WRED thresholds become 0.

  Conditions: Use the below mentioned config to repro the problem.

```
policy-map parent
class class-default
shape aver 2000
service-policy child

policy-map child
class class-default
random-detect

int g0/0/0
service-policy out parent

policy-map child
class class-default
queue-limit 2000
```

  Workaround: Remove WRED and reattach it.

- CSCtt43843

  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.

  Conditions: It is occurring with a Cisco 7200 platform loaded with the 15.2 (1.14)T0.1 image.

  Workaround: There is no workaround.

- CSCtt45381

  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

- 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
  ```

- CSCtu16809

  Symptoms: Deny entries in the KS ACL are not downloaded to the GM when the GM has an ISM VPN card.

  Conditions: The GM is using an ISM VPN card.

  Workaround: Use deny entries on a local ACL on the GM, or disable the ISM VPN.

- 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.

- 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.

- CSCtu24740

  Symptoms: A Cisco ISR router may unexpectedly reload due to bus error or Segv Exception or experience a spurious access.

  Conditions: The symptom is observed when NAT and dampening are configured on the same interface while the device is running Cisco IOS Release 15.2(1)T or a later release.

  Workaround 1: Remove dampening from the configuration.

  Workaround 2: Downgrade to Cisco IOS Release 15.1(4)M or earlier release.

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

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

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

- CSCtu33956

  Symptoms: The dialer with PPP encapsulation is seen when DSL is the WAN interface. L2PT does not work.

  Conditions: This symptom is observed under the following conditions:

  - The PPPoE dialer client needs to be configured on the physical SHDSL interface.
  - The GRE tunnel destination interface should point to the dialer interface.
  - The MPLS pseudowire should go over the tunnel interface.
  - After the PPPoE session is set up, the GRE tunnel traffic gets dropped at the peer end of the PPPoE session.

  Workaround: There is no workaround.

- CSCtu38244

  Symptoms: After bootup, the GM cannot register and is stuck in “registering” state. Issuing the **clear crypto gdoi** command is required for a successful registration to the keyserver.

  Conditions: The symptom is observed upon router bootup.

  Workaround: Do a **clear crypto gdoi** after a reload.

- CSCtu52820

  Symptoms: A memory leak is observed under HTTP PROXY Server process.

  Conditions: Device is configured with Cisco ISR Web Security with Cisco ScanSafe and has User Authentication NTLM configured.

  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 7.1/5.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2011-4661 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

- 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

- CSCtv52031

  Symptoms: Router crashes while accessing the usergroup database.

  Conditions: The symptom is observed with performance testing.

  Workaround: There is no workaround.

- CSCtw50141

  Symptoms: Incremental leaks at __be_ber_get_stringa pointing to LDAP process.

  Conditions: The symptom is observed when NTLM authentication is being used with an LDAP server and with the router acting as the NTLM proxy.

  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.

- CSCtw60333

  Symptoms: HTTP process hangs. This impacts the webauth authentication scaling factor.

Conditions: The symptom is observed when the **clear ldap server** *server-name* command issued or the connection is closed during any outstanding LDAP. Transactions are in progress or are waiting for an LDAP response from the LDAP server.

Note: it is not only related to the secure-server. It is also applicable with an IP HTTP server. So generally it is applicable if you are using webauth with LDAP as the authentication server.

Workaround: Do not issue **clear ldap server** when any LDAP transactions for web authentication are in progress.

- CSCtw71620

  Symptoms: ISM VPN module cannot handle SSL records of a size greater than 1500 bytes. It will lead to SSL record encrypt/decrypt operation failure and result in a packet drop.

  Conditions: The symptom is observed with ISM VPN and SSL records of a size greater than 1500 bytes.

  Workaround: Disable the ISM VPN module with **no crypto engine slot 0**.

- CSCtw76044

  Symptoms: Need IGMP/MLD information to make IGMP/MLP snooping work.

  Conditions: The symptom is observed under all conditions.

  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.

- CSCtx06018

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

  Conditions: The symptom is observed when performing WAAS performance test.

  Workaround: Increase interface input queue hold size.

- CSCtx06801

  Symptoms: Certain websites may not load when content-scan is enabled. Delays of up to a few seconds may be seen.

  Conditions: The symptom is observed when content-scan is enabled.

  Workaround: Though not always, refreshing the page sometimes helps.

  Further Problem Description: The problem is due to GET request being segmented. For example, a huge get request of 1550 may come from the client in two different packets such as 1460+90=1550.

- CSCtx12216

  Symptoms: I/O pool memory goes low.

  Conditions: The symptom is observed with Scansafe configured. A small buffer is not getting freed.

  Workaround: There is no workaround.

- CSCtx16040

  Symptoms: ISM VPN card will crash when used in combination with SSL-AO of WAAS express. In theory, this can also happen in normal VPN-SSL.

  Conditions: The symptom is observed with high numbers of SSL connections.

  Workaround: Disable the ISM VPN card.

- CSCtx37680

  Symptoms: All the ports on the ISR are used up. After this we may see a crash.

  Conditions: The symptom is observed with ports on the ISR.

  Workaround: Ensure that not all the TCP ports on the ISR are allocated.

- CSCtx46741

  Symptoms: ISM VPN module crashes for SSL records between 1800 bytes to 1840 bytes.

  Conditions: The symptom is observed with an ISM VPN module + SSLVPN or ISM VPN + WAAS SSL AO.

  Workaround: Disable ISM VPN module and fallback to onboard/SW crypto engine.

- CSCtx47493

  Symptoms: NTLM authentication does not work.

  Conditions: The symptom is observed when “ip admission ntlm rule” is configured on the interface.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(1)T1

Cisco IOS Release 15.2(1)T1 is a rebuild release for Cisco IOS Release 15.2(1)T1. The caveats in this section are resolved in Cisco IOS Release 15.2(1)T1 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.

- CSCtd15853

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

  Conditions:

  - mVPN is configured on the PE router.
  - Both Pre-MDT SAFI and MDT-SAFI Cisco IOS software is running in a Multicast domain.

  Multicast VPN: Multicast Distribution Trees Subaddress Family Identifier

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

  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.

- 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: The issue occurs during the peer (standby RP) reset or switch- over.

  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.

- 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.

- 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.

- 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.

- CSCtn39950

  Symptoms: An IPsec session will not come up.

  Conditions: This symptom occurs if a Cisco ISR G2 has an ISM VPN accelerator and slow interfaces such as BRI-PRI. Crypto plus ISM VPN module plus slow interfaces will not work.

  Workaround: Disable the ISM VPN module and switch to the onboard crypto engine.

- 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 that “no logging console” is configured.

- 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.

- 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.

- 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
  ```

- 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.

- 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.

- CSCtq31898

  Symptoms: Web traffic is not getting redirected to ScanSafe towers.

  Conditions: Having dual WAN links to reach the ScanSafe tower and the source interface used as a loopback.

  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.

  “show 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.

- 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.

- CSCtq71344

  Symptoms: Sometimes HTTPS sessions may fail when they are redirected via a ScanSafe tower.

  Conditions: This symptom is observed when multiple HTTPS sessions are being redirected to ScanSafe towers by the content-scan feature.

  Workaround: White-list the HTTPS traffic not to be redirected to ScanSafe towers by applying an ACL in the content-scan configuration.

- 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.

- 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.

- CSCtq83468

  Symptoms: 302 Page Moved to url: https://<virtual-ip>/login.html?redirect- url=<actual-url> does not happen, and the client is directly presented with the login page.

  Conditions: The Proxy Auth method and ip admission virtual-ip should be configured.

  Workaround: Unconfigure ip admission virtual-ip.

- CSCtq90577

  Symptoms: A router crashes when removing NetFlow.

  Conditions: The symptom is observed when removing NetFlow.

  Workaround: There is no workaround.

- 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.

- CSCtr09142

  Symptoms: Poor throughput is observed with content-scan.

  Conditions: This symptom occurs when content-scan is enabled.

  Workaround: There is no workaround.

- CSCtr10577

  Symptoms: 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.

- 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.

- 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.

- CSCtr19922

  Symptoms: Lots of output printed by **show adjacency** [*key of adj*] *internal dependents* followed by a crash.

  Conditions: The symptom is observed with the existence of midchain adjacencies, which will be created by IP tunnels, MPLS TE tunnels, LISP, and similar tunneling technologies.

  Workaround: Do not use the **show adjacency** [*key of adj*] *internal dependents* command. Specifically, it is the “dependents” keyword which is the problem. If the dependents keyword is not used there is no problem.

- 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.

- 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

- CSCtr34965

  Symptoms: An SSL WebVPN page does not come up when ISM-VPN is used.

  Conditions: When an attempt is made to bring up an SSL session with ISM-VPN, the page does not load.

  Workaround: There is no workaround.

- CSCtr40091

  Symptoms: A call is not recorded.

  Conditions: This symptom is observed after a few days of load.

  Workaround: There is no workaround.

- 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”.

- 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.

- CSCtr54907

  Symptoms: A router crashes.

  Conditions: This symptom is observed when an ISM VPN accelerator is used as the crypto engine.

  Workaround: Disable the ISM VPN accelerator.

- CSCtr59314

  Symptoms: A router reloads when the **clear crypto session** command is issued with 4000 sessions up.

Conditions: This symptom is observed only under load conditions.

Workaround: There is no workaround.

- CSCtr63462

  Symptoms: A router crashes at bootup.

  Conditions: This symptom is observed with a Cisco 3900 that has an ISM VPN module installed and no HSECk9 license installed.

  Workaround: Boot with a pre-15.2(1)T image, load an HSECk9 license, and then boot with a 15.2(1)T image.

- CSCtr83542

  Symptoms: When content-scan functionality is enabled, the throughput drastically comes down and CPU utilization approaches 100 percent.

  Conditions: This symptom is observed when content-scan is enabled and web traffic is subjected to redirection.

  Workaround: Disable content-scan functionality.

- CSCtr85537

  Symptoms: The content-scan feature was not available in the v152_1_t throttle before this DDTS was committed.

  Conditions: All ISRG2 images.

  Workaround: There is no workaround.

- CSCtr87249

  Symptoms: A Cisco 2900 router crashes while it is reloaded with a 15.2(1.6)T image.

  Conditions: This symptom occurs when an ISM-VPN card is installed on the Cisco 2900 and when there is no HSECK9 license installed.

  Workaround: When the HSECK9 license is installed on the Cisco 2900, the crash is not seen.

- 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.

- CSCtr89882

  Symptoms: Platform-related error messages are seen during an LDP flap in an ECM scenario.

  Conditions: This symptom is observed with LDP with ECMP paths and during flapping of LDP sessions.

  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

- CSCtr91890

  Symptoms: An RP crashes sometimes when the router is having PPPoX sessions.

  Conditions: If a PPPoX session is terminated in the middle of session establishment and ip local pool is configured to pick the IP address for the peer and the version that the router is running has the fix for CSCtr91890.

  Workaround: There is no known workaround.

- CSCtr94887

  Symptoms: Using MRCP v1, VXML script with ASR operation will always receive no input event.

  Conditions: The symptom is observed with Cisco IOS Release 15.2(1)T.

  Workaround: There is no workaround.

- CSCts06776

  Symptoms: Requests hang when NAT is enabled.

  Conditions: This symptom is observed when content scan and NAT are enabled.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCts64483

  Symptoms: Incorrect packet lengths are received at ISM VPN.

  Conditions: Buffer alignment in Cisco IOS software.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(1)T

All the caveats listed in this section are open in Cisco IOS Release 15.2(1)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCso41274

  Symptoms: The router has enough DSP resources to set up 14 signaling channels. While trying to configure a ds0-group for 16 time-slot, an error message is received that not enough DSP resources are available.

  Immediately after that the router spits the following 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

  % 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

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

- CSCta22221

  Symptoms: A frame-relay client triggers the reload of a standby router.

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

Workaround: There is no workaround.

- CSCtb51244

  Symptoms: Spurious memory access is seen when deleting a policy map.

  Conditions: The symptom is observed on a Cisco 7200 series router running Cisco IOS interim Release 12.4(24.6)PI11u.

  Workaround: There is no workaround.

- CSCth38565

  Symptoms: A router crashes after traffic stops and the WE router is unconfigured. This problem is intermittent and very difficult to reproduce.

  Conditions: This symptom is observed when the WE is configured for full optimization, traffic is passed, and then the WE router is unconfigured. The type of traffic being passed does not seem to affect the crash.

  Workaround: There is no workaround.

- 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.

- 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, whereas the other interface is one hop away.

  Workaround: There is no workaround.

- CSCti85075

  Symptoms: Customer running cat4500-ipbasek9-mz.122-31.SGA9.bin on a cat4500 has reported the following log messages whenever an snmpset is performed:

  ```
  %SCHED-3-SEMLOCKED: SNMP ENGINE attempted to lock a semaphore, already locked by
  itself -Traceback= 10DB0624 10C9FCD0 10C76964 10C6A300 10C901D0 10626B80 1061E388
  ```

  The traceback may vary.

  Conditions: This symptom is observed if the snmp engine is shut down during the processing of an snmpset. Entering the command **no snmp-server** in config mode is one way that the snmp engine can be shut down. The likely hood of the snmp engine being shut down during the processing of an snmpset is very small.

  This problem will affect other devices, not just the Cat4500.

  Workaround: There is no workaround other than to reboot the device.

- 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 Release 12.4(15)T14.

Workaround: Remove CEF.

- CSCtj69620

  Symptoms: An IPIPGW memory-related crash (double free) occurs at ccsip_update_srtp_caps.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtk33149

  Symptoms: A router crashes when making SIP trunk calls along with Cisco IOS Firewall.

  Conditions: This symptom is observed with the Cisco UBE and the Cisco IOS Firewall configured as co-located, and with the Cisco IOS Firewall doing SIP inspection.

  Workaround: There is no workaround.

- CSCtk35917

  A service policy bypass vulnerability exists in the Cisco Content Services Gateway - Second Generation (CSG2) which runs on the Cisco Service Application Module for IP (SAMI). This vulnerability could allow in certain configurations:

  – Customers to access sites that would normally match a billing policy to be accessed without being charged to the end customer.

  – Customers to access sites that would normally be denied based on configured restriction policies.

  Additionally, Cisco IOS Software release 12.4(24)MD1 on the CSG2 contains two vulnerabilities that can be exploited remotely, via an unauthenticated attacker resulting in a denial of service of traffic through the CSG2. Both these vulnerabilities require only a single content service to be active on the CSG2 and are exploited via crafted TCP packets. A three way hand-shake is not required to exploit either of these vulnerabilities.

  No workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110126-csg2

- CSCtk76648

  Symptoms: An rpcdump operation takes more time with WEXP.

  Conditions: This symptom is observed when WEXP is configured and an rpcdump occurs.

  Workaround: There is no workaround.

- CSCtk98248

  Symptoms: The Fa8 line proto is down after the connected device is reloaded.

  Conditions: This symptom is observed on the following platforms:

  – A Cisco 892 running Cisco IOS Release 15.0(1)M3 or a previous version

  – A Cisco 892 (only Fa8 port and set to 10/full)

  – A Cisco 3750/Cisco 2960 running Cisco IOS releases other than Cisco IOS Release 12.2(37)SE

  Workaround:

  - Fa8 set to 100/full or auto
  - On the Cisco 892, upgrade to Cisco IOS Release 15.0(1)M4
  - On the Cisco 3750/Cisco 2960, run Cisco IOS Release 12.2(37)SE

- CSCtl20181

  Symptoms: Incorrect behavior is seen in MPPC compression.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtl55502

  Symptoms: Any parser command with a pipe option used in an http URL is not working properly and is giving the help option instead of actual output.

  Conditions: This symptom is observed when a parser command is used with a pipe option in an http URL. For example, http://<ipadd>/level/15/exec/show/runn/|/i/http/CR will not give proper output.

  Workaround: When using the router through a browser, enter the command through the text field instead of including it in the URL.

- CSCtl79666

  Symptom: A Cisco 1801 router configured with zone-based firewall causes Memory Leak.

  Conditions: The symptom is observed with zone-based firewall configured on a Cisco 1801 router with traffic.

  Workaround: There is no workaround.

- CSCtl87463

  Symptoms: The queue length becomes negative.

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

  Workaround: There is no workaround.

- CSCtn04277

  Symptoms: Time-based WRED does not work.

  Conditions: This symptom is observed when time-based WRED is used.

  Workaround: There is no workaround.

- CSCtn14074

  Symptoms: Ingress traffic passes through an unauthorized switch port.

  Conditions: This symptom is observed on a Cisco ISR G2 platform with an EHWIC-ESG module, and with ingress traffic initiated from an unauthorized supplicant port. To hit the scenario, supplicant should be authenticated and have a successful traffic flow. After that, simulate an UNAUTHORIZED state of supplicant, but traffic flow should not be stopped. Now, perform shut/no shut on the interface or reload the router to see that the traffic is continuing to go.

  Workaround: There is no workaround. However, if traffic is stopped prior to the symptom occurring, it will not be seen.

- CSCtn16855

  Symptoms: A Cisco 7200, PA-A3 cannot ping across an ATM pvc.

  Conditions: This symptom is observed when a high traffic rate output policy is applied under the pvc.

Workaround: Remove the policy.

- CSCtn17800

  Symptoms: Main ATM interface statistics cannot be obtained using SNMP. This symptom is not observed for ATM subinterfaces/PVCs configured under subinterfaces or any other type of interfaces on a Cisco 3900 device.

  Conditions: This symptom is observed on a Cisco 3900 series running Cisco IOS Release 15.1T1.

  Workaround: There is no workaround.

- CSCtn24305

  Symptoms: The software version in “call home” messages has a trailing comma for the released images, which is causing a backend processing failure when the software version is needed.

  Conditions: This symptom is observed with all “call home” messages on all released images.

  Workaround: The backend can check to remove this trailing comma if it is present.

- CSCtn28941

  Symptoms: The PVDM2-24DM connection sequence stops at the debug output of “CSM: (CSM_PROC_WAIT_FOR_CARRIER)<--CSM_EVENT_MODEM_SETUP”, and therefore it cannot establish the connection with the TA, though NM-30DM can.

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

  Workaround: There is no workaround.

- CSCtn65519

  Symptoms: After a call connects through an MGCP-controlled gateway and DTMF is issued for a phone system to route a call, DTMF digits are not interpreted correctly.

  Conditions: This symptom is observed on an MGCP-controlled gateway.

  Workaround: Use H323.

- CSCtn84572

  Symptoms: A Cisco 2801 running Cisco IOS Release 12.4(24)T4 has good performance, but when upgraded to Cisco IOS Release 15.1(3)T, the performance may degrade.

  Conditions: This symptom is observed on a Cisco 2801 on both Cisco IOS images without any features configured.

  Workaround: There is no workaround.

  Further Problem Description: Without any features configured, both Cisco IOS versions tested the same (no performance decrease vs. each other). Then we added some basic features: a) named access list and b) nat. The access list was permitting all test traffic. Nat was not actively natting any packets.

  On Cisco IOS Release 12.4(24)T4, there was no packet droppage and thruput was as expected. On Cisco IOS Release 15.1(3)T, there was packet droppage (as seen on a traffic generator and also on the router in the form of “ignored” packets). Thruput was diminished by at least 10%.

- CSCtn87834

  Symptoms: Platform: Cisco devices crash during normal operation with the following message:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 7669B0C data B0D0B0D
  chunkmagic 0 chunk_freemagic 100 -Process= "<interrupt level>", ipl= 1,
  ```

  Conditions: This symptom is observed on Cisco 7200 devices running Cisco IOS 12.4(24)T4.

  Workaround: There is no workaround.

- CSCtn97267

  Symptoms: Router crash in CCE code

  Conditions: This symptom occurs on an ISRG2 during normal operation.

  Workaround: There is no workaround.

- CSCtn98633

  Symptom: IP phones lose registration with CUCME on a Cisco IAD887 after some usage.

  Conditions: This symptom is observed when transfer, call waiting, and other scenarios that involve MoH are present.

  Workaround: Disable MoH.

- CSCto08904

  Symptoms: RTP operations fail to run when using multiple operations.

  Conditions: When more than 16 RTP operations are running, operations start failing due to scaling issues.

  Workaround: There is no workaround.

- CSCto10485

  Symptoms: Mediatrace fails to activate all the sessions.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- 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. The same symptom occurs with a blind transfer to external destinations.

  Conditions: This symptom is observed when the **voice-class codec X offer all** command and transcoders are used with the Cisco UBE.

  Workaround:

  - Use the **codec XXXX** command instead of the **voice-class codec X offer all** command
  - Perform a consultative transfer instead of a blind transfer.

- CSCto31255

  Symptoms: A router crashes at fair-enqueue.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCto38553

  Symptoms: Iosips sends rst to a client on some http sessions with a printer after working for a few hours. Once the symptom occurs, it continues until the iosips configuration is removed from the interface.

  Conditions: This symptom is observed on a Cisco 3945 with an iosips configuration.

  Workaround: Remove and reapply the iosips config on the interface.

- CSCto52353

  Symptoms: Multilink bundles are not removed after clearing the vpdn session in LAC.

Conditions: This symptom is observed when a VPDN/L2TP tunnel is established between the client and the LNS.

Workaround: There is no workaround.

- CSCto52575

  Symptoms: A Cisco 7200 router crashes after unconfiguring tcp and rtp under the iphc-profile.

  Conditions: This symptom is observed on a Cisco 7200 running Cisco IOS Release 15.2(0.11)T.

  Workaround: There is no workaround.

- CSCto53119

  Symptoms: The VC stays down.

  Conditions: This symptom is observed after the following sequence:

  4. xconnect is configured on an SVI and the EoMPLS VC is up
  5. remove xconnect, remove SVI
  6. add the same vlan on VPLS VC via V-E

  Workaround: Remove and add back the VLAN in “down” state using the **switchport allowed vlan** command.

- CSCto54850

  Symptom: IP Phones fail to register with SRST GW after CCM Fallback to GW while testing call-forward and call-transfer scenarios.

  Conditions: This symptom is observed on an SRST GW running with failed image.

  Workaround: There is no workaround.

- CSCto55852

  Symptoms: A Cisco 2821 router crashes due to block overrun.

  Conditions: This symptom is observed when the router is acting as a fax gateway.

  Workaround: There is no workaround.

- CSCto63268

  Symptoms: A Cisco IOS router configured as a VoIP MGCP gateway interworking with Cisco Unified Communications Manager (CUCM - Callmanager) may experience an unexpected reload.

  Conditions: This symptom has been observed

  - in Cisco IOS Release 15.1T while attempting to parse the ccm config being pushed down
  - when using a digital (T1/E1) module interface when the MGCP PRI configuration is being pushed to the gateway from CUCM using the **ccm-manager config** command.

  Workaround: Either disable the T1/E1 configuration from CUCM or remove the **ccm-manager config** command. It may be possible to manually configure the MGCP with the PRI backhaul commands.

- CSCto63809

  Symptoms: A Cisco 3945 router is unable to receive updates from another router.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCto70421

  Symptoms: Throughput performance drops between Cisco IOS Release 15.1(3)T and Release 15.1(4)M.

  Conditions: The symptom is observed when you upgrade from Cisco IOS Release 15.1(3)T to Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCto76888

  Symptoms: A PSTN user calls up on a specific number which is directed to the IVR response via the Cisco 2800 GW router, but the PSTN user cannot hear anything due to the codec payload mismatch.

  Conditions: This symptom is observed when the first preference sent to a Cisco 2851 for an IVR announcement is the G.729ab codec.

  Workaround: Change the preference of the codecs so that G.729a is the preferred codec from the MGX.

- CSCto83077

  Symptoms: IPIPGW is not found in zone, though registered, when invia outvia is used for remote zone.

  Conditions: This symptom is observed with the incoming LRQ to GK with IPIPGW from the remote zone.

  Workaround: There is no workaround.

- CSCto84268

  Symptoms: TCP connections will take a longer time or will not work if PAT is enabled with two dialer links.

  Conditions: PC---fa0/1-7200-Vi1.1---DSLAM---Di0---1841-f0/0---PC -Vi1.2---DSLAM---Di1--|

  The Cisco 1800 router has two dialer interfaces and NAT will point to Dialer 0 interface as the source address, but packets will leave the Dialer 1 interface with a source address of Dialer 0. If the ISP has enabled RPF check, then it will drop the packets coming out of the Dialer 1 interface.

  Workaround: Shut down one of the dialer interfaces.

- CSCto85479

  Symptoms: A Cisco 3945 router running EHWIC-4ESG claims itself to be the STP root for all active vlans. The Cisco 3945 router is not participating in STP root bridge election.

  Conditions: This symptom is observed on a Cisco 3945 router running Cisco IOS Release 15.1(4)M. Interfaces gi0/3/0-1 are on an EHWIC-4ESG card. The symptom was observed on an EHWIC-4ESG; data is not available for other HWIC cards.

  Workaround: There is no workaround.

- CSCto96445

  Symptoms: A router reloads while unconfiguring/configuring “call-router h323-annexg.”

  Conditions: This symptom is observed when “neighbor ip address” is configured.

  Workaround: There is no workaround.

- CSCtq06497

  Symptoms: Prefix not received at the remote end even after radius passes.

  Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtq12007

  Symptoms: When removing tunnel protection from one tunnel, other tunnels sharing the same profile and the same source interface stop working.

  Conditions: This symptom affects multipoint GRE over IPsec tunnels (DMVPN) tunnels that are sharing the same ipsec profile (with keyword “shared” at the end of the tunnel protection statement), and are using the same interface as a source.

  Workaround: There is no workaround.

- CSCtq15936

  Symptoms: A Cisco 3845 with chronic high CPU interrupts with Cisco IOS Release 12.4(24)T2 and Release 15.0(1)M4.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(24)T2 and Release 15.0(1)M4.

  Workaround: There is no workaround.

- CSCtq17444

  Symptoms: A Cisco AS5400 crashes when performing a trunk call.

  Conditions: This symptom is observed in Cisco IOS Release 15.1(3)T and on Cisco routers acting as voice gateways for H323.

  Workaround: There is no workaround.

- CSCtq21234

  Symptoms: A label is not removed after shutting down the link.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtq22924

  Symptoms: WSMA code does not allow more namespaces to be added to the SOAP envelope. Namespaces should be in the SOAP envelope in order for the CWMP agent to interwork with third-party ACS servers.

  Conditions: This symptom is observed with interworked third-party ACS servers that expect a dslforum namespace in the SOAP envelope. As per the TR-069 standard, the SOAP message must carry a private namespace in the SOAP envelope (xmlns:cwmp="urn:dslforum-org:cwmp-1-0">.

  Workaround: There is no workaround.

- CSCtq23708

  Symptoms: An active PGW crashes when deleting pdp, due to low mem with service records.

  Conditions: This symptom is observed when the pdp are cleared using the **clear** command and the SCU timeout happens.

  Workaround: There is no workaround.

- CSCtq24733

  Symptoms: A VXML gateway crashes with an unexpected exception to CPU: vector C.

  Conditions: This symptom is observed when MRCP is enabled.

  Workaround: There is no workaround.

- CSCtq26270

  Symptoms: HSRP packets are forwarded on STP blocked ports.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtq30376

  Symptoms: An SGW reloads for a dual APN with multiple MCBs under one user when the DDN message is tied to one of the MCBs. If this MCB is deleted, the crash occurs after n3t3 timeout.

  Conditions: This symptom is observed when the DDN message has been sent for the pdp.

  Workaround: There is no workaround.

  Further Problem Description: Since the DDN message is a user-level message, it should not be tied to any one MCB because that MCB can be freed before the DDN Ack is received or the n3t3 timeout occurs.

- CSCtq36192

  Symptoms: Cisco IOS with Zone Based Firewall crashes the router.

  Conditions: The issue is seen when modifying the parameter map as shown below:

  ```
  parameter-map type regex slim no pattern [^x80]
  ```

  Workaround: There is no workaround.

- CSCtq36742

  Symptoms: DmVPN DCHP does not work with a tunnel interface configured under a VRF on spoke.

  Conditions: This symptom is observed when vrf is configured.

  Workaround: There is no workaround.

- CSCtq38474

  Symptoms: A router running Cisco IOS may crash due to a bus error.

  Conditions: This crash is related to the forwarding of MPLS traffic. Additional conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtq39602

  Symptoms: The DMVPN Tunnel is down with IPSEC configured. The **show dmvpn** from the spoke shows that the state is “IKE.”

  Conditions: This symptom is observed after heavy traffic pumps from the DMVPN hub to the spoke for a period of time ranging from a few minutes to a couple of hours.

  Workaround: There is no workaround.

- CSCtq40469

  Symptoms: EEM policy registration fails.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtq41512

  Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/No Shut will bring the PRI layer 1 to “Active” and layer 2 to “Multi-frame established.”

Conditions: This symptom is observed 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.

- CSCtq48481

  Symptoms: The following syslog and traceback are observed under high stress conditions with 300k subscriber sessions with MEF functionality enabled on the gateway and a QoS-profile (MBR/GBR):

  ```
  SAMI 4/8: 000056: Jun 8 23:10:31: %SAMI-4-UNEXPECTED: Unexpected condition: Could not
  delete Hash-Entry -Process= "GTP Management", ipl= 0, pid= 124, -Traceback=
  0x461C9520z 0x461D0A18z 0x461D3014z 0x45DCFD00z 0x45DD1678z 0x45DD1888z 0x461DD820z
  0x461DD890z 0x45DCAEF8z 0x45DCD4D0z 0x45DCDEC0z 0x442FC234z 0x4598BB78z 0x4598F27Cz
  ```

  Conditions: This symptom is observed while maintaining the rate profile for given MBR/GBR values with a granularity of 2.7kbps for all subscriber sessions. The rate profile reference count (num_of_pdps) will wrap around after creating 65535 under each PPC (TCOP). When PDP are deleted after wrapping around the reference count, the syslog and traceback will be observed.

  Workaround: Disable MEF functionality on the gateway or under an access-point configuration.

- CSCtq49325

  Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

  Conditions: This symptom is observed only when there are 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. If they are required and if mutual redistribution is done, then while performing a graceful shutdown, sufficient time should be given for one process to be shut down completely before executing the second **shutdown** command. This should resolve the problem.

  Problem Description: In a normal scenario, a zombie drdb or path entry (a temporary drdb entry that is deleted as soon as processing of the packet is complete) would be created only for the reply message. Due to redundancy in the LAN and the EIGRP processes in this scenario, a query sent on one interface comes back on the other interface, 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, 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; the flow continues and the prefix itself is deleted. This causes a dangling path to exist without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to a crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths before deletion. Similar conditions will occur if the packetization timer expiry is not kicked in immediately to send the drdbs threaded to be sent, and a topology shutdown flow executes first.

- CSCtq51271

  Symptoms: The web pages may not load, and the browser displays the following error: “Internet Explorer cannot display the webpage.” The following display is seen on the console:

  ```
  *May 23 13:12:13.734: %FW-6-DROP_PKT: Dropping tcp session <X.X.X.X:80>
  <Y.Y,Y.Y:port> with ip ident 0
  ```

  Conditions: This symptom is observed in Cisco IOS with the URL trend filter enabled.

  Workaround: Refresh the webpage, or remove the IP of the specific website from being inspected.

- CSCtq51554

  Symptoms: A Cisco 881 router crashes during normal operation, but not much information is available in the crashinfo.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(2)T3 and earlier versions.

  Workaround: There is no workaround.

- CSCtq55173

  Symptom: A Cisco device crashes with NAT configured. SIP appears to be translated trough NAT. However, some cases report that the crash is still present after redirecting SIP traffic elsewhere.

  Conditions: This symptom is observed 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. Entering “sh proc mem sorted” shows continuous increase in memory held by the CCSIP_SPI_CONTROL process even when the average number of calls at the gateway are constant.

  Conditions: This symptom is observed when the SIP trunk in Cisco Unified Communications Manager points to the gateway, is configured with DTMF signaling type as “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 Cisco Unified Communications Manager SIP trunk configuration that is pointing to the SIP gateway.
  2. Configure “dtmf-relay rtp-nte” at the SIP gateway dial-peer configuration instead of “sip-kpml.” The Unified Communications Manager is configured with “no preference.”

  In order to recover from the crash, the gateway router must be reloaded.

- CSCtq57330

  Symptoms: A Cisco device crashes while processing calls.

  Conditions: This symptom is observed when H323 is being used.

  Workaround: There is no workaround.

- CSCtq58364

  Symptoms: NBAR sees IPsec packets on a DMVPN tunnel interface.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtq59326

  Symptoms: Flexible NetFlow stops working after some time.

  Conditions: This symptom is observed on a Cisco 3945 running Cisco IOS Release 15.1(3)T with Flexible NetFlow.

  Workaround: Reload the router.

  Further Problem Description: The “high watermark” value becomes 4294967295 with “current entries” close to that; “flows added” minus “flows aged” is close or equal to “cache size.”

- CSCtq59923

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

  Conditions: This symptom is observed when running multiple OSPF processes and with filtered mutual redistribution between the processes. When pulling the cable on one OSPF process, the OSPF database will clear, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

  Workaround: Configure “ip routing protocol purge interface.”

- CSCtq60799

  Symptoms: A Cisco router crashes due to a memory corruption with the following error,

  ```
  %SYS-2-CHUNKBADREFCOUNT: Bad chunk reference count
  ```

  Conditions: This symptom is observed when using a hardware crypto accelerator (VSA module).

  Workaround: There is no workaround.

- CSCtq62069

  Symptoms: A Cisco gateway crashes during CVP load testing.

  Conditions: This symptom is observed when a CVP Mixed Call-Flow test is run with 900 calls. The gateway crashes and a crash file is produced.

  Workaround: There is no workaround.

- CSCtq63625

  Symptoms: A WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4, is not getting trained with third-party DSLAMs unless the “line rate” is configured manually.

  Conditions: This symptom is observed on a WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4.

  Workaround: There is no workaround.

- CSCtq63838

  Symptoms: A Cisco 2921 router crashes with the following traceback:

  ```
  May 1 20:50:00.513: ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528:
  unkn -Traceback= 0x24A19810z 0x24A5DC8Cz 0x24A4A560z 0x24DF6618z 0x24DF6BBCz
  0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z

  May 1 20:50:00.553: ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528:
  unkn -Traceback= 0x24A19810z 0x24A5DC8Cz 0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz
  0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z

  May 1 20:50:00.553: %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 a Cisco router running Cisco IOS Release 15.0(1)M3 and with the DSMP process

  Workaround: There is no workaround.

- CSCtq64153

  Symptoms: When a PPPoE service-name is configured on an ATM interface or subinterface, the CLI is accepted but not applied.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtq67517

  Symptoms: gh-sip.jar missing in locale-ja_JP-Japanese-8.6.2.4.tar

  Conditions: This symptom is observed when applying the Japanese locale in the Cisco SIP IP Phone 8961. gh-sip.jar file is missing in the CME-locale-ja_JP-Japanese-8.6.2.4.tar.

  Workaround: There is no workaround.

- CSCtq70847

  Symptoms: A Cisco 2900 series device fails to transmit a DCS message for T38 to RightFax.

  Conditions: This symptom is observed when T38 v0 is configured on the gateway, and with the following topology: PSTN---T1 CAS---2950---T38/SIP---RightFax IOS: c2951-universalk9_npe-mz.SPA.151-3.T1

  Workaround: There is no workaround.

- CSCtq74389

  Symptoms: When using an SVI interface as an L2TPv3 termination, the SVI interface unexpectedly floods an unknown unicast packet.

  Conditions: This symptom is observed when an SVI interface is used as an L2TPv3 termination.

  Workaround: Use a routed port instead of an SVI.

- CSCtq74610

  Symptom: A PGW crashes while sending the “modify command failure” message.

  Conditions: This symptom is observed when the Modify Bearer Command procedure is exercised under a load of 200 create-session-requests per second, and 200 **modify bearer** commands per second are performed simultaneously, with a lag of 60 seconds in between for a specific session.

  Workaround: There is no workaround.

- CSCtq75008

  Symptoms: A Cisco 7206VXR crashes due to memory corruption.

  Conditions: This symptom is observed under the following conditions:

  – the device is working as a server for L2TP over IPSec
  – encryption is done using a Cisco C7200-VSA
  – more than two clients are connected

  If client sessions are kept up for about a day, the router would crash.

  Workaround: There is no workaround.

- CSCtq76005

  Symptoms: Configuring “atm route-bridge ip” on MPLS-enabled ATM interface forces the router to punt all incoming MPLS packets to the CPU.

  Conditions: This symptom is observed when RBE is configured on an MPLS-enabled ATM interface.

  Workaround: Remove RBE.

- CSCtq77024

  Symptoms: Metrics collection fails due to an 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:

1. remove and reschedule the mediatrace session
2. remove and reconfigure the mediatrace responder

- 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.

- CSCtq84313

  Symptoms: A router hangs and then crashes due to a watchdog timer expiry.

  Conditions: This symptom is observed when IP SLA probes are configured, and then the configuration is replaced with one that has no IP SLA probes.

  Workaround: Reset the ip sla.

- CSCtq84350

  Symptoms: High memory utilization occurs in the IPS process.

  Conditions: This symptom is observed when Cisco IOS Release 12.4(24)T3 is upgraded to Cisco IOS Release 12.4(24)T5. Even with the same IPS configuration, the IPS process is utilizing 11 Mb more memory.

  Workaround: There is no workaround.

- CSCtq85327

  Symptoms: CCM-CCM Call forward cases fail when the Cisco UBE is in flow-around mode.

  Conditions: This symptom is due to a glare condition when the Cisco UBE receives and sends UPDATE message at the same time.

  Workaround: Disable “update caller-id” under “voice service voip.”

- CSCtq85728

  Symptoms: An EHWIC-D-8ESG card is causing an STP loop.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtq85875

  Symptoms: A device crashes in ipsec_dp_delete_sa when **clear cry sess** is entered.

  Conditions: This symptom is observed with a flexvpn configuration.

  Workaround: There is no workaround.

- CSCtq89267

  Symptoms: A router crashes or gets stuck.

  Conditions: This symptom is observed when the “debug ccsip messages” is enabled and call transfer is performed on a sip phone.

  Workaround: Avoid using “debug ccsip messages.”

- CSCtq90054

  Symptoms: A Cisco IOS router fails to recognize Skype-application traffic.

  Conditions: This symptom is observed after configuring PfR to control Skype traffic.

Workaround: There is no workaround

- CSCtq90577

  Symptoms: The router crashes when removing netflow.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtq92650

  Symptoms: A DMVPN Tunnel is not selecting the right source interface.

  Conditions: The symptom is observed when Multi-link Frame-relay creates more than one subinterface with the same name.

  Workaround: There is no workaround.

- CSCtq92655

  Symptoms: A DSP reset occurs with c5510_NO_RING_DESCRIPTORS errors.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

  Further Problem Description: A DSP crash-dump showed that Cisco IOS is either not taking packets from DSP, or there is corruption of the HPI buffer pointer update.

- CSCtq92940

  Symptoms: An active FTP transfer initiated from a Cisco IOS device used as a client may hang.

  Conditions: This symptom is observed when an active FTP connection is used (for example, “no ip ftp passive” is present in the configuration) and there are device configuration or communication issues between the Cisco IOS device and the FTP server that, while allowing control connections to work as expected, stop the data connection from reaching the client.

  Workaround: Use passive FTP (default) by configuring “ip ftp passive.”

- CSCtq94509

  Symptoms: A memory leak occurs in the “Dead” process.

  Conditions: This symptom is observed on a Cisco 3845 running Cisco IOS Release 12.4(24)T5 or Release 12.4(24)T1.

  Workaround: None to stop the leak. However, monitoring “show memory stat” (processor pool, free column) will show free memory. Reload the router before the memory drops too low.

  Further Problem Description: “Show proc mem sorted” may show the “Dead” process holding more and more memory. In at least one case, the leak rate was 20-40Mb/day.

- 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.

- CSCtq97723

  Symptoms: A Cisco 3945 router may have performance issues (lower throughput) due to overruns.

  Conditions: This symptom is observed with a steady bi-directional 64-byte ICMP stream. With Cisco IOS Release 15.0(1)M2, at 283Mbps = 37.16% wire rate of 1 gig, overruns began to increment. With Cisco IOS Release 15.1(4)M, at 206Mbps = 27.09% wire rate of 1 gig, overruns began to increment.

  Workaround: There is no workaround.

- CSCtq97991

  Symptom: An ADSL interface fails to re-train when the command line “dsl enable-training-log” is configured.

  Conditions: This symptom is observed in the following:

  1. Cisco 800, 1900, and 2900 devices, but the symptom could affect other software platforms
  2. Cisco IOS Release 15.1(2)T, Release 15.1(2)T1 and Release 15.1(3)T3, but not in Cisco IOS Release 15.0(1)M4.

  Workaround: The symptom is resolved after removing “dsl enable-training-log.”

  Further Problem Description:

  1. When “dsl enable-training log” is not configured, the HWIC trains up to the DSLAM with no problem; even after unplugging the cable and reconnecting it, the HWIC still comes up.
  2. When “dsl enable-training log” is configured, after unplugging the cable and reconnecting it, the HWIC fails to come up. The CD LED does not blink and the following error message appears:

  ```
  “No retrain. sleep 20 seconds”
  ```

- CSCtr00381

  Symptoms: A PRI interface goes down and cannot make a call after reload.

  Conditions: This symptom is observed when the **modem firmware location** command is configured for using specific firmware for PVDM2-24DM.

  Workaround: Re-insert the cable and shut/no shut the controller; this might clear the symptom temporarily. Or, delete the **modem firmware location** command.

- CSCtr01595

  Symptoms: A Cisco AS5350XM router experiences a “software forced crash.”

  Conditions: This symptom is observed on a Cisco AS5350XM used as a VXML Gateway and running Cisco IOS Release 15.1(3)T.

  Workaround: Keep the number of active calls to 150 or less.

- CSCtr03624

  Symptoms: An incorrect “calling-station-id” is displayed during DHCP accounting.

  Conditions: This symptom is observed when accounting is triggered by the DHCP relay. It is not seen when accounting is triggered using the DHCP server.

  Workaround: Use a DHCP server to start accounting.

- CSCtr07471

  Symptoms: The following symptoms are observed:

  – on a Cisco 2800 router with HWIC cards and 2 ports connected to a Cisco 2960 switch (one in an STP blocking state), after 4-5 days of operation (more or less), the HWIC hangs and no traffic is forwarded via the card.

  – “show cdp neighbor” entered on the router displays the Cisco2960 switch, whereas when the same is entered on the switch, no neighbors are shown.

  – a shut/no shut on either the switch interface or the HWIC ports does not resolve the issue.

  Conditions: These symptoms are observed under the following conditions:

  – speed and duplex are matching on both sides (the issue is found even when the speed and duplex are set to auto)

  – the output rate for the interface on the HWIC card towards the switch shows 0 packet rate

  Workaround: Reload the router.

- CSCtr07508

  Symptoms: A crash is observed several times for a period of time. This crash occurs after enabling WAAS on the interface.

  Conditions: Conditions are not determined. Router is reloaded, no traffic is flowing through the router, or special configuration is done. This is seen several times in regression during a period of time, then ceases to happen in newer versions. Crash may be released with previous configuration on the router. It is not consistent.

  Workaround: There is no workaound.

- CSCtr11030

  Symptoms: An SGW reloads.

  Conditions: This symptom is observed when an SGW and a PGW are out of sync with respect to default bearers. Multiple Modify Bearer Responses are received from the PGW with a “Context Not found” error.

  Workaround: There is no workaround.

- CSCtr11274

  Symptoms: A backup clock is missing.

  Conditions: After the primary clock switches over, the new primary clock does not have a backup clock.

  Workaround: There is no workaround.

- CSCtr11620

  Symptoms: In a simple HSRP setup with Cisco 2900 devices, ping to a virtual IP intermittently fails.

  Conditions: This symptom is observed with a Cisco 2911 device.

  Workaround: Replace the Cisco 2900 series device with a Cisco 1800 series or a Cisco 1941.

- CSCtr13172

  Symptoms: Using the **configure replace** command causes the router to crash.

  Conditions: This symptom is observed when mediatrace and performance monitoring along with DMVPN are configured on the router.

  Workaround: There is no workaround.

- CSCtr14227

  Symptoms: Peer1 current-data metric set to default is not matching baseCost.

  Conditions: This issue is seen in routers loaded with Cisco IOS 15.1(2)T3.1

  Workaround: There is no workaround.

- CSCtr15040

  Symptoms: MCID is not clearing DSP resources when it receives the ISDN disconnect with PI.

  Conditions: Conditions are unknown at this time.

  Workaround: Remove the MCID script to release the DSP resources.

- CSCtr15518

  Symptoms: One-way audio occurs after transfer by the Cisco Unity auto attendant or IP phone SIP (PSTN) -- CUBE -- SIP -- CUCM -- Unity AA -- IP phone or SIP (PSTN) -- CUBE -- SIP -- CUCM -- IP phone -- blind transfer -- IP phone

  Conditions: This symptom is observed when a SIP trunk from the PSTN returns an IP address 0.0.0.0 when the connection is made inactive.

  Workaround: Enable pass-thru content sdp under voice service voip/sip.

- CSCtr16857

  Symptoms: Windowing in IKEv2 is broken.

  Conditions: This symptom is observed due to an error condition in auth exchange that causes the delete message to not be sent because of incorrect windowing:

  ```
  "No room in peer window request is throttled: Current Req = 2 Next Req = 1"
  ```

  Workaround: There is no workaround.

- CSCtr18559

  Symptoms: An unallocated/unassigned number is received from the PBX but, as a response, the gateway sends a network congestion notice back to the PBX. The gateway rejects the call with 4#, when it should send a 7#.

  Conditions: This symptom is observed only when the country “Brazil” is configured. When the country is set to “itu,” 5# is sent, which is correct for an unallocated/unassigned number.

  Workaround: There is no workaround.

- CSCtr18574

  Symptom: H323-H323 video calls fail with cause code 47; 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
  ```

  Conditions: This symptom is observed when H323-H323 video calls fail to establish an H245 media connection.

  Workaround: There is no workaround.

- CSCtr18985

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

  Conditions: This symptom is observed after reloading the router.

  Workaround: Flap the serial interface, or disable CEF on the serial interface or globally.

- CSCtr20300

  Symptoms: An SA negotiation test is failing for ipsec_core script; the SA should enter idle state after entering the **show crypto isakmp sa** command.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtr20762

  Symptoms: When the router is reloaded, the following tracebacks are seen:

  ```
  *Jun 14 11:34:05.188: %TUN-3-L3VPN_GROUP: Tunnel L3VPN Groups: attempting to delete
  PE: failed to translate handle to group -Traceback= 1B99250 CFDC7C CFE560 D27CFC
  D8D374 D8EB60 CEA4B4 CEA994 CEB080 4A63F0 4A63EC
  ```

  Conditions: This symptom is observed with L3 VPN encapsulation IP. When the **aaa accounting system default** command is not used, the symptom does not occur.

  Workaround: Clear ip bgp * or disable the aaa accounting system.

- CSCtr21296

  Symptoms: The following messages are seen continuously on the router console:

  ```
  Jun 28 22:56:53.551: [ipsec_dp_expand_sa]Invalid data cipher info Jun 28
  22:56:53.551: [ipsec_dp_expand_action]No memory to allocate SA for decrypt action
  ```

  and the GETVPN Group Member tries to register continuously even after successful registration.

  Conditions: The issue is seen after disabling the hardware crypto engine.

  Workaround: There is no workaround

- CSCtr22683

  Symptoms: The EIGRP flaps.

  Conditions: This symptom is observed when tunnel protection is configured on a GRE tunnel.

  Workaround: There is no workaround

- CSCtr25127

  Symptoms: When switching between ATM and 3G interfaces, the following traceback is observed.

  ```
  %ALIGN-3-CORRECT: Alignment correction made at 0x23D242DCz reading 0xE85C77B
  %ALIGN-3-TRACE: -Traceback= 0x23D242DCz 0x23CDE700z 0x23CFDF50z 0x225C0594z
  0x225C1368z 0x22DD4564z 0x21F88D28z 0x2173449Cz
  %ALIGN-3-CORRECT: Alignment correction made at 0x23D2430Cz writing 0xE85C77B
  %ALIGN-3-TRACE: -Traceback= 0x23D2430Cz 0x23CDE700z 0x23CFDF50z 0x225C0594z
  0x225C1368z 0x22DD4564z 0x21F88D28z 0x2173449Cz
  ```

  Conditions: This symptom is observed when switching between ATM and 3g interfaces.

  Workaround: There is no workaround.

- CSCtr25734

  Symptoms: A router crashes.

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

Workaround: There is no workaround.

- CSCtr26018

  Symptoms: A Key Server crashes while unconfiguring VRF.

  Conditions: This symptom is observed during the removal of access-lists.

  Workaround: There is no workaround.

- CSCtr26117

  Symptoms: An authorized client gives its user credentials, but the password expiry rejects the pin and prompts the client to resubmit the pin.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtr26144

  Symptoms: The UUT 5 second output packet rate falls out of 70/130% range while testing the PPPoE/VMI feature.

  Conditions: This issue is seen in routers running Cisco IOS Release 15.2(0.19)T0.1

  Workaround: There is no workaround.

- CSCtr26373

  Symptoms: An interface bounces and after coming back up, hangs and does not pass traffic. The Rx ring is stuck and all packets coming into the interface are counted as “input errors.” The interface will still show “up/up” in the “show interface” output.

  Conditions: This symptom is observed on a Cisco 3900. This may be seen at random times and has thus far occurred after an interface bounce.

  Workaround: Bounce the interface again to restore service.

- CSCtr26681

  Symptoms: QoS pre-classify fails for vpn traffic classification.

  Conditions: This symptom is observed when classification is based on an inner IP header.

  Workaround: Configure classification using ToS.

- CSCtr28594

  Symptoms: Load calculation fails on a VMI interface with high CDR, High traffic occurs while testing the PPPoE/VMI feature.

  Conditions: This issue is seen in routers running Cisco IOS Release 15.2(0.19)T0.1

  Workaround: There is no workaround.

- CSCtr28701

  Symptoms: A local server does not get an ip address from the remote server via IPCP.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtr29460

  Symptoms: The dead memory on a Cisco 3845 router is holding up memory. The memory being held is constantly increasing.

Conditions: “sh memory dead” reveals significant amount of memory allocated for:

- SSH Process
- State Machine Instance
- TCP Remote Shell

Workaround: There is no workaround.

- CSCtr29914

  Symptoms: A Cisco 3945 crashes.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCtr31153

  Symptoms: Packet decryption seems to fail with manual crypto maps configured on an interface.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.2(0.19)T0.1

  Workaround: There is no workaround.

- CSCtr31578

  Symptoms: Variable and inaccurate NTP sync results occur on 3945 and 3945E , leading to a few-second time drift every 24 hours.

  Conditions: This symptom is observed on the Cisco 3945/3945E under normal operation.

  Workaround: Configure "no ntp."

- CSCtr32498

  Symptoms: Input/output packet counts display double the expected value on “show interface output.”

  Conditions: This symptom is observed with an NM-16ESW card and not on the ports on the motherboard.

  Workaround: There is no workaround.

- CSCtr33856

  Symptoms: Tracebacks and/or crash occurs @ mace_monitor_waas_command:

  ```
  Jul 5 21:08:54.635: %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 or watchdog crash
  following the above, with decodes pointing to mace_monitor_waas_command
  ```

  Conditions: This symptom is observed after on-the-fly changes to mace policies and classes.

  Workaround: There is no workaround.

  CSCtr35456

  Symptom: A router crash occurs at datalist_next while configuring mld proxy with PIM disabled.

  Conditions: This symptom is observed on Cisco IOS Release 15.2(1.2)T.

  Workaround: Start PIM (e.g., enable ipv6 multicast-routing) before configuring mld host-proxy.

- CSCtr35913

  Symptoms: 200 OK response is deferred at incoming SIP leg. Possible Tracebacks due to accessing NULLl memory.

  Conditions: Applicable for SIP-SIP calls in Cisco IOS images where the bad code fix CSCto72992 is present.

  Workaround: There is no workaround.

- CSCtr38330

  Symptom: A Cisco router may reload after configuring and unconfiguring ATM PVCs several times.

  Conditions: This symptom is observed on a Cisco 3825 running Cisco IOS Release 15.1(3)T1.

  Workaround: There is no workaround.

- CSCtr40091

  Symptoms: A call is not recorded.

  Conditions: This symptom is observed after a few days of the load.

  Workaround: There is no workaround.

- CSCtr40568

  Symptoms: Blind transferring an incoming call from PSTN back out to another PSTN number via a Cisco UBE results in one-way audio.

  Conditions: This symptom is observed in Cisco IOS Release version 15.1(2)T.

  Workaround: Revert to Cisco IOS Release 15.0(1)M1ES.

- CSCtr41626

  Symptoms: A Cisco 1941 and Cisco 2911 with 512MB memory fail to netboot via FTP due to Address Error (load or instruction fetch) exception following verification of the digital signature.

  Conditions: This symptom is observed on a Cisco 1941 or Cisco 2911 with 512MB memory and flash, and running Cisco IOS Release 15.1(4)M.

  Workaround: Boot the image directly from flash.

- CSCtr41941

  Symptoms: A DSP crash on occurs on a Cisco 3945 gateway when sending T38 fax with ECM disabled.

  Conditions: This symptom is observed on PVDM3 with ECM enabled, and in Cisco IOS Release 15.1.3T1

  Workaround: There is no workaround.

- CSCtr42341

  Symptoms: A crash occurs at task_execute_prep.

  Conditions: This symptom is observed on a Cisco 800 series router configured with BFD.

  Workaround: There is no workaround.

- CSCtr43255

  Symptoms: HWIC-3G-CDMA-V will not activate.

  Conditions: This sympto is observed with OTASP activation.

  Workaround: There is no workaround.

- CSCtr43993

  Symptoms: A router is crashing with CPUHOG messages and WATCHDOG TIMEOUT

  Conditions: This symptom is observed when Netflow is configured.

  Workaround: Disable Netflow.

- CSCtr45484

  Symptom: A router reloads while unconfiguring telephony service.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(03)T1.5

  Workaround: There is no workaround.

- CSCtr46004

  Symptoms: When changing the “match” command the router reloads with a bus error.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T10.

  Workaround: There is no workaround.

- CSCtr46577

  Symptoms: Dropped calls, informational (non-crash) MGCP tracebacks, ISDN signaling issues.

  Conditions: This symptom is observed with bad DSP hardware.

  Workaround: This issue is rarely seen. It results when there is a hardware problem with a DSP channel, and then signaling resources are assigned to the channel. There is currently no workaround except to replace the defective DSP module.

- CSCtr46815

  Symptoms: With some MACE CLI configurations, WAAS does not pick up any packets.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtr46854

  Symptoms: A PPP multilink between a Cisco ISR G2 and a Cisco ASR1K crashes the ISR.

  Conditions: This symptom is observed on a Cisco ISR G2.

  Workaround: Remove authentication on the serial interface on the Cisco ASR1K.

- CSCtr47084

  Symptoms: Changing zone from multilink interface and replacing config with test config crashes the router.

  Conditions: This symptom is observed when traffic is running.

  Workaround: There is no workaround.

- CSCtr48480

  Symptom: A Cisco router may crash after “show gateway” is entered.

  Conditions: This symptom is observed on a Cisco 3825 running Cisco IOS Release 12.4(24)T4. The problem is rare in that most instances this command will not trigger a crash.

  Workaround: Do not enter “show gateway.”

- CSCtr49868

  Symptoms: A Cisco UBE crashes.

Conditions: This symptom is observed when the Cisco UBE is a Cisco 3945 running Cisco IOS Release 15.1.4M1.

Workaround: There is no workaround.

- CSCtr50008

  Symptoms: A Cisco UBE does not pass the reason header.

  Conditions: This symptom is observed with the following topology:

  Phone - Multiple vendor switches - Cisco UBE - Cisco UBE - CUCM 8.6 - Phone

  Workaround: Configuration had both a copy option under sip-profiles as well as allowing the reason header pass-through. Removing the copy option and just using the pass-through corrected the problem. However, the resulting reason header is not formatted as expected.

  Further Problem Description:

  Call flow: Routine call from vendor phone A to Cisco UBE - Cisco UBE to Cisco phone A

  Flash Override Call from vendor phone B to Cisco UBE - Cisco UBE to Cisco phone

  A Routine call is preempted as expected between the Cisco phone A and vendor phone A, and the Flash Override call is up between Cisco phone A and vendor phone B

  However, Cisco UBE is not passing to vendor phone A a reason header for the call termination. CUCM is sending the reason code to the Cisco UBE, but the Cisco UBE is not sending it along.

- CSCtr50118

  Symptoms: A router crashes.

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

  Workaround: There is no workaround.

- CSCtr52047

  Symptoms: A one-way audio issue occurs in SRST mode.

  Conditions: This symptom is observed under the following conditions:

  - when a Cisco 3925 is in SRST mode
  - internal calls are not affected

  Workaround: There is no workaround.

  Further Problem Description: Call setup is working fine, but RTP packets are not sent to the IP phone from the Cisco 3925. The phones fall into SRST, and the caller from PSTN can hear voice from IP phone, but the IP phone cannot hear voice from the PSTN. From the trace, the voice packets get received by the ephone packet handler layer, but from the phone statistics, no voice packet is received.

- CSCtr53265

  Symptoms: ISDN layer 1 is in deactive state.

  Conditions: This symptom is observed with a WIC-1B-U-V2 card on a Cisco 2801.

  Workaround: There is no workaround.

- CSCtr53903

  Symptoms: One-way voice occurs, where POTS cannot hear VOIP.

  Conditions: This symptom is observed on a Cisco 3945 running Cisco IOS Release 15.1.2(T2) PVDM3 DSPware 26.8.1

Workaround: Reboot the router

- CSCtr54269

  Symptoms: Cisco UBE Sends RTCP Bye message to MS OCS R2, causing a loss of audio for about 20 seconds.

  Conditions: Cisco UBE sends RTCP BYE only upon reINVITE due to Session refresh timer.

  Workaround: Revert to Cisco IOS Release 12.4(22)YB.

- CSCtr55348

  Symptoms: A seemingly unending MIB walk occurs.

  Conditions: This symptom is observed when auto-generated IP SLA probes are present and a MIB walk encompassing either rttMonReactTriggerAdminStatus or rttMonReactTriggerOperTable is done.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(1)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.2(1)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsl74976

  Symptoms: When MPLS-tagged packets are punted to MSFC CPU at a high rate, incoming interface hold-queue can fill up, and interface will be throttled. No packets are processed from throttled interfaces (until interface is unthrottled). If control plane protocols are running on throttled interfaces (especially with aggressive short timeouts), frequent throttling can lead to instabilities (such as BGP session loss, OSPF adjacency flaps, HSRP failovers, BFD neighbor less, etc.).

  Conditions: This symptom occurs when MPLS-tagged packets are punted to MSFC CPU at a high rate, incoming interface hold-queue can fill up, and interface will be throttled.

  Workaround: A certain level of stability can be gained by increasing hold queues on interfaces in questions. Also reducing the rates and duration of the traffic punting to MSFC CPU will help.

- CSCtb72734

  Symptoms: DHCP OFFER is not reaching the client when the unicast flag is set.

  Conditions: This symptom occurs only on ASR devices where creation or removal of the ARP entry does not maintain sequential ordering. As a result, the packet could arrive at the forwarding plane after the ARP entry has already been removed or before the ARP entry has been created.

  Workaround: There is no workaround.

- 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 or Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtd87072

  Symptoms: IOSD restart seen.

  Conditions: The symptom is observed when changing tunnel mode on scaled IPSec sessions.

  Workaround: There is no workaround.

- CSCtd90030

  Symptoms: A Cisco 2851 router may crash with a bus error.

  Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or 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 ############
  ```

- CSCth03648

  Symptoms: Cisco 2960 and 3750 series switches running Cisco IOS Release 12.2 (53)SE1 may crash.

  Conditions: This symptom is observed if two traps are generated by two separate processes, and if one process suspends and the other process updates some variables used by the first process.

  Workaround: Disable all snmp traps.

- 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

- 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.

- CSCti16649

  Symptoms: GETVPN GM reregisters.

  Conditions: This symptom is seen when any ACL is added or removed from the key server.

  Workaround: There is no workaround.

- CSCti48504

  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

- 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.

- 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.

- CSCtj14921

  Symptoms: During the stress test of EzVPN, many messages are observed on the console like the following:

  ```
  "%PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT: IOS thread disabled interrupt for 11 msec"
  ```

  The EzVPN server is configured for dVTI and dynamic crypto maps. The stress test consists of bringing up and tearing down close to 1700 EzVPN clients (1250 dVTI and 450 dynamic cmap) clients.

  Conditions: This symptom is seen on a Cisco ASR 1006 router with RP2/FP20 combo with EzVPN clients coming in on GigE interfaces and on the latest XE3.2 throttle build. Many messages are seen on the console followed by tracebacks.

Workaround: There is no workaround.

- CSCtj21045

  Symptoms: Header compression decodes RTP timestamp incorrectly.

  Conditions: This issue occurs mainly with IPHC format compression interacting with older IOS releases.

  Workaround: Use IETF format compression.

- CSCtj23189

  Symptoms: Packet drops on low rate bandwidth guarantee classes even if the offered rate is less than guaranteed rate.

  Conditions: This happens only when extremely high rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with 3 classes: one with 16kbps, second one with 1Mbps, and the third one with 99Mbps.

  Workaround: There is no workaround.

- CSCtj30155

  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

- CSCtj46670

  Symptoms: IPCP cannot complete after 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.

- CSCtj55624

  Symptoms: A router crashes upon entering the **show crypto ruleset** command.

  Conditions: This symptom is seen when version 6 crypto maps are configured.

  Workaround: Do not run the **show** command.

- CSCtj78966

  Symptoms: A Cisco ASR 1000 router crashes with thousands of IKEv2 sessions, after many operations on IKEv2 session.

  Conditions: This symptom is seen when IKEv2 SA DB WAVL tree is getting corrupted if we fail to insert the SA due to some error, for example, PSH duplication.

  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.

- CSCtj94510

  Symptoms: When sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and 4 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), one IKE session per VRF, and four SA dual per session.

  Workaround: There is no workaround.

- CSCtj94589

  Symptoms: With the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF and four SA dual per session, in unconfigured testbed after end of the IXIA traffic, crash happens at “no vrf” under “crypto isakmp profile”.

  Conditions: This symptom is seen 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.

- CSCtk12122

  Symptoms: A Cisco 7200 router may crash after clearing the SAs while using the IKE keepalive feature.

  Conditions: This symptom occurs when the IKE keepalive feature is turned on, and the user executes a **clear crypto session** command or a **clear crypto sa** command.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCtk74660

  Symptoms: The Network Time Protocol (NTP) tries to re-sync 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.

- CSCtk83638

  Symptoms: Client gets 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 a NAT router. When one client connection is broken and the server is not made aware of this, and the client reconnects with a different group, the IP address assigned is not from the correct pool.

  Workaround: There is no workaround.

- CSCtl00995

  Symptoms: A Cisco ASR1K with 1000 or more DVTIs may reboot when we do shut / no shut on the tunnel interfaces or the tunnel source interface.

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

  Workaround: Use a different tunnel source for each of the DVTIs. You can configure multiple loopback interfaces and use them as a tunnel source.

- CSCtl20993

  Symptoms: Router crashes during IPsec rekey.

  Conditions: The conditions for this crash are currently unknown.

  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.

- 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.

- 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.

- CSCtl73564

  Symptoms: The same address is allocated for multiple IAIDs.

  Conditions: This symptom is observed when a client has been configured to send multiple IAIDs in a single request.

  Workaround: There is no workaround.

- CSCtl78285

  Symptoms: In VRF configuration, we are not able to add rd 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
  ```

  After two hours, we try to add the rd again.

  ```
  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 VRF configuration and add again.

- 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.

- 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.

- CSCtl92210

  Symptoms: A router may crash when trying to show the sessions on responder while the session queue is being managed (removal).

  Conditions: This symptom occurs while new sessions are being provisioned or removed from mediatrace initiator side. The router can crash when trying to show the session objects on the responder while the session queue is being managed (removal) by first disabling the initiator using the **no mediatrace initiator force** command and then disabling responder with the **no mediatrace responder** command.

  Workaround: Do not disable initiator with the **no mediatrace initiator force** command and responder with the **no mediatrace responder** command in quick succession while the **show mediatrace responder session [brief | details]** command is not finished with output or in pause mode.

- CSCtl94813

  Symptoms: When using iLBC, the VG224 fails to play audio out the FXS port. The call uses iLBC when the analog 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: Revert to Cisco IOS Release 12.4(4)T8.

- CSCtl98132

  Symptoms: XDR CPU hog may cause system crash.

  Conditions: This symptom occurs when a double failure, such as SSO switch and FRR cutover, causes XDR CPU hog and crashes the system.

  Workaround: There is no workaround.

  Further Problem Description: The crash can be avoided if the system has no double failure.

- CSCtn02632

  Symptoms: A MAB supplicant never gets authenticated and remains in RUNNING state.

  Conditions: This symptom is observed when a MAB supplicant connected to FA1 port of a Cisco 890 router remains in RUNNING state indefinitely after issuing a warm reload of router.

  Workaround: Use other FE ports if a warm reload is issued.

- CSCtn04686

  Symptoms: When MHSRP is configured and the hello packets are passing through Etherchannel, and the cables connected to the Etherchannel port are unplugged/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.

- 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.

- 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.

- CSCtn18229

  Symptoms: A policy does not get suspended.

  Conditions: This symptom is observed if a policy is applied to fr-pvc, then the member link is flapped from the peer for mfr subint.

  Workaround: There is no workaround.

- CSCtn18437

  Symptoms: Crash seen @ qos_set_assign_pak_feature_object.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtn18784

  Symptoms: Interface Tunnel 0 constantly sends high-bandwidth alarms.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- 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 other than to avoid entering impacted **show** command.

- 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.

- 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.

- CSCtn22930

  Symptoms: PLATFORM_VALUE_EIGRP_TRACE_LOG_SIZE_IN_KB should not be hard coded to 20. The PLATFORM_VALUE_CRASH_BUFFER_SIZE is already defined as 20.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtn22961

  Symptoms: With the pseudowire redundancy, after performing "clear xconnect all" on the remote primary peer, the VCs that switchover to the backup PWs are now in the standby state on the primary peer. However, they are in down state on the local node instead of standby state.

  Conditions: This symptom occurs when performing "clear xconnect all" on the remote primary peer where initially all the VCs are in UP state.

  Workaround: There is no workaround.

- CSCtn29181

  Symptoms: SDP PassThru + IPv6 to IPv4 Conversion is not working.

Conditions: This symptom is observed with Cisco IOS Release 15.1(3.22)T and Release 15.1(3)T.

Workaround: There is no workaround.

- CSCtn31333

  Symptoms: CPU utilization is high due to the process Net Background.

  Conditions: This symptom is observed on a router used for LNS with an L2TP application after upgrading to Cisco IOS Release 12.4(24T).

  Workaround: There is no workaround.

- CSCtn36227

  Symptoms: Alignment errors are seen at ipv6_checksum.

  Conditions: This symptom is seen when the GRE tunnel is configured with IPv6 ping sweep going across.

  Workaround: There is no workaround.

- CSCtn39632

  Symptoms: RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.

  Conditions: This occurs on a Cisco ASR 1000 series 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.

- CSCtn41793

  Symptoms: With IP session and traffic after OIR/SSO, the downstream traffic is not flowing.

  Conditions: This symptom occurs after OIR/SSO.

  Workaround: There is no workaround.

- 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.

- CSCtn52270

  Symptoms: CWMP is not coming up.

  Conditions: This symptom is seen because of the “alcdsl_get_wan_dsl_link_config” function.

  Workaround: There is no workaround.

- CSCtn53794

  Symptoms: A multilink PPP interface stays down after SSO.

  Conditions: This symptom is observed when the serial interfaces on an 8xCHT1/E1 are configured to be a part of a ppp multilink group and a **redundancy force-switchover** command is entered.

Workaround: There is no workaround.

- 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.

- CSCtn55187

  Symptoms: Memory leaks are seen at ikev2_ipsec_add_proxy_to_list, ikev2_skeyseed_create, and ikev2_ios_get_ipv6_pak on the Cisco 2900 and Cisco 3900 platform routers respectively.

  Conditions: This symptom is seen after the test has been completed and while trying to check for the memory leaks when testing the Tunnel Protection for IPv6 feature.

  Workaround: There is no workaround.

- CSCtn61501

  Symptoms: CfmFlowRtpPayloadType does not return the correct value.

  Conditions: When CISCO-FLOW-MONITOR-MIB displays a flow carrying RTP information, it does not populate the correct value for the object cfmFlowRtpPayloadType.

  Workaround: Enter the **show performance monitor status** command. Entering this command will not make the object behave correctly, but it will provide an alternate way to see the value for the payload type.

- 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 keep alive 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.

- 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.

- CSCtn65130

  Symptoms: The “evaluate” statement on an IPv6 ACL in Cisco IOS cannot be added after the “sequence” statement; for example,

  ```
  %router(config)#ipv6 access-list test
  %router(config-ipv6-acl)#evaluate REFLECTOUT ? sequence Sequence number for this
  entry <cr> %router(config-ipv6-acl)#evaluate REFLECTOUT sequence 10 router
  (config-ipv6-acl)# %router(config-ipv6-acl)#sequence 10 ? deny Specify packets to
  reject permit Specify packets to forward remark Access list entry comment
  ```

  If configuring the reflexive ACL with the sequence command at the end of the statement, the ACL works fine. However, when saving the configuration, this gets translated into the startup-config as follows:

  ```
  %sequence 10 evaluate REFLECTOUT
  ```

  As this syntax is not accepted, when the router boots up this command is not applied, so it is lost on the running config.

  Conditions: This symptom is observed when configuring IPv6 reflexive ACL on Cisco IOS.

  Workaround: Manually re-enter the ACL with only the accepted syntax after boot.

- CSCtn68117

  Symptoms: The **session** command does not work on a Cisco 3000 series router that has become the master after a mastership change.

  Conditions: This symptom is observed upon fail-over to slave.

  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: IPSEC key engine crashes at sessions setup.

  Conditions: This symptom is seen 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 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/grandchild policy is used multiple times in the same parent.

Workaround: There is no workaround.

- CSCtn72939

  Symptoms: The L2tpv3 feature is not working on Cisco 1810 series platforms.

  Conditions: This symptom occurs with a Cisco 1812 running Cisco IOS Release 15.(0)M and later releases.

  Workaround: Configure bridge-group under that xconnect interface.

- CSCtn74169

  Symptoms: Crash by memory corruption occurs in the “EzVPN Web-intercept daemon” process.

  Conditions: This symptom is observed when EzVPN server pushes a long banner to the client after HTTP authentication using HTTP intercept.

  Workaround: Do not use long banner in HTTP intercept.

- 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

- 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.

- CSCtn79475

  Symptom: 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.

- CSCtn82089

  Symptoms: Connectivity loss to PCs in data vlan occurs when connected to ports on a EHWIC-D-8ESG-P. PCs do not get IP address from DHCP server.

  Conditions: This symptom is observed when the EHWIC-D-8ESG-P interface is configured in the following order (portfast prior to voice vlan):

  ```
  Router(config-if)#switchport access vlan 100 Router(config-if)#spanning-tree
  portfast Router(config-if)#switchport voice vlan 101
  ```

  Workaround: Remove the portfast and voice vlan configuration and re-apply voice vlan prior to portfast.

  Further Problem Description: If the router is reloaded, it is possible that the portfast is applied first, leading to the connectivity loss.

- CSCtn83520

  Symptoms: VOIP_RTCP related traceback is seen.

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

  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.

- 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.

- CSCtn90630

  Symptoms: Leaks occur at __be_udb_create_rtcg_p and __be_udb_remove_class_in_class_group or a crash occurs at __be_udb_pre_feature_unbind_child.

  Conditions: This symptom is observed with modification of complex 3 level QoS policy under certain scenarios.

  Workaround: There is no workaround.

- 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.

- CSCtn93891

  Symptoms: Multicast traffic is getting blocked.

  Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

  Workaround: There is no workaround.

- CSCtn95344

  Symptoms: After RPR downgrade from SRE2 CCO to SRE1 CCO, the standby RSP gets stuck in cold bulk and reboots every 50 minutes.

  Conditions: This symptom occurs after RPR downgrade from SRE2 CCO to SRE1 CCO.

  Workaround: Perform reload on the router.

- 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.

- CSCto00318

  Symptoms: SSH session that is initiated from a router that is running Cisco IOS Release 15.x may cause the router to reboot.

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.x.

  Workaround: For now, consider not initiating an SSH session from the Cisco router that is running a Cisco IOS Release 15.x train.

- 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.

- 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.

- CSCto02712

  Symptoms: DHCP client stops accepting IP address when ASR replies for arp packet of client's IP address obtained via DHCP.

  Conditions: Some of DHCP clients that check for duplicate IP addresses before configuring a DHCP assigned IP address may reject IP address assignment.

  Workaround: Configure "no ip proxy arp" on a dhcp server-facing interface.

  Further Problem Description: The above workaround would work if the DHCP server/relay agent is directly on the client's subnet and is not separated by an L2 technology that stops ARP (for example, a DSLAM).

- CSCto03506

  Symptoms: The Gigabit Ethernet 0/2 interface on Cisco 3900 platforms is not seen by applications using snmp.

  Conditions: This symptom is observed on Cisco 3900 platforms.

  Workaround: There is no workaround.

- 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.

- CSCto07586

  Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.

  Conditions: This symptom occurs under the following conditions:

  - Create an IOS image that does not IPV6 enabled
  - Enable BFD on an interface
  - 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.

- CSCto08754

  Symptoms: The crypto VTI interface with ip unnumbered VTI may experience input queue wedge. When the interface becomes wedged, all incoming traffic from the tunnel drops.

  Conditions: This symptom occurs when the crypto VTI interface becomes wedged.

  Workaround: There is no workaround.

- CSCto09161

  Symptoms: A Cisco router with MACE+NAT configuration crashes after a few hours of traffic.

  Conditions: This symptom is observed when both MACE+NAT are enabled on the interface.

  Workaround: There is no workaround.

- CSCto10165

  A vulnerability exists in the Smart Install feature of Cisco Catalyst Switches running Cisco IOS Software that could allow an unauthenticated, remote attacker to perform remote code execution on the affected device.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available to mitigate this vulnerability other than disabling the Smart Install feature.

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

- 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.

- CSCto12514

  Symptoms: After turning a member link, multilink goes to suspense mode and it will not come back even after the member comes back.

  Conditions: This symptom is observed with an MPOL configuration.

  Workaround: Remove the MPOL configuration.

- CSCto12825

  Symptoms: The multilink policy cannot be removed.

  Conditions: This symptom is observed with MPOL configured; when multilink goes to suspension, the policy cannot be removed.

  Workaround: There is no workaround.

- 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.

- CSCto15278

  Symptoms: Tracebacks are seen at managed_chunk_low.

  Conditions: This symptom occurs when sending multicast traffic and using the **show memory debug leaks chunks** command.

  Workaround: There is no workaround.

- CSCto15361

  Symptoms: 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.

- CSCto16319

  Symptoms: Traceback is thrown while starting Re-Auth timer and Re-auth always happens.

  Conditions: This symptom is observed when a Session-Timeout value from the RADIUS server is set to a high value which is rounded to a negative value in authenticator.

  Workaround: There is no workaround.

- CSCto16597

  Symptoms: When using the voluntary PPP feature with L2TP, a memory leak is seen. The leak is of AAA memory that is allocated on behalf of the voluntary PPP.

  Conditions: This symptom occurs when there is a disconnect of the L2TP or voluntary PPP connection.

  Workaround: There is no workaround.

- 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/read the static route that generates Type7.

  Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

  Workaround 3: Execute the **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.

- 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.

- 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.

- CSCto43683

  Symptoms: Suspended service policy is not re-enabled when MFR bundle link comes up.

  Conditions: This symptom is observed when the service policy is attached to MFR DLCI.

Workaround: There is no workaround.

- CSCto43776

  Symptoms: The “shared” keyword does not work as expected on the second tunnel interface on a HUB with the first tunnel interface connecting to a dmvpn spoke and the second tunnel interface to point-to-point GRE peer.

  Conditions: Conditions are unknown at this time.

  Workaround:

  1. Flap both T1 and T2
  2. For T2 use a different ipsec profile. This ipsec profile should be using a different transform set (either different encryption protocol or different hashing protocol)
  3. Configure the tunnel interfaces from scratch using the “shared” keyword

- CSCto43807

  Symptoms: The secondary tower will resume the IP Address of the primary tower when the secondary tower has been incorrectly configured.

  Conditions: This symptom is observed when the primary tower is incorrectly configured and is not up.

  Workaround: Configure the secondary tower with the correct DNS name or IP Address.

- CSCto44016

  Symptoms: After connectivity to the primary tower is lost, the secondary tower does not take over, and the following status is displayed:

  ```
  #sh content-scan summ
  Primary: <tower-primary-IP-address> (Up)*
  Secondary: <tower-secondary-IP-address> (Up)
  ```

  The primary tower is still showing as the active tower.

  Conditions: This symptom is observed when connectivity to the primary tower is lost.

  Workaround: Reload the router. After reload, the following status is displayed:

  ```
  #sh content-scan summ
  Primary: <tower-primary-IP-address>(Down)
  Secondary: <tower-secondary-IP-address> (Up)*
  ```

- CSCto44581

  Symptoms: The router crashes on high call volume.

  Conditions: This symptom occurs on high call volume.

  Workaround: There is no workaround.

- CSCto45019

  Symptoms: The router crashes when you remove the dialer interface and read 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 read 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 **config t no memory lite end,** one may start to see process “IP SLAs Responder” growing. 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: A memory leak occurs while running UDP echo operation.

  Conditions: This symptom is observed when an UDP echo operation successfully runs. Leak is seen on every 100th run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way is 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.

- CSCto55623

  Symptoms: A TCP session in listen state receiving invalid SYN packet fails for TCP-IPv6.

  Conditions: This symptom is observed in Cisco IOS Release 15.2(6)PI16.

  Workaround: There is no workaround.

- CSCto55708

  Symptoms: A build error occurs due to a missing quotation mark (‘"‘) in a printf statement, only in dsgs, due to compiler-specific issues.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCto60399

  Symptoms: Ping is not working if GETVPN is enabled

Conditions: This symptom is observed if icmp/ip acl are configured on KS.

Workaround: There is no workaround.

- CSCto61098

  Symptoms: Incremental SNMP chunk-leaks are observed.

  Conditions: This symptom is observed when GETVPN is enabled on the interface.

  Workaround: There is no workaround.

- CSCto63954

  Symptoms: A router with GETVPN configurations is continuously crashing.

  Conditions: This symptom is seen with GETVPN-related configurations with fail-close feature activated.

  Workaround: There is no workaround.

- CSCto65352

  Symptoms: System crashes randomly when the Apex module is in the system.

  Conditions: Conditions are unknown at this time.

  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 the 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).

- CSCto72932

  Symptoms: Traceback is seen at ephone_create_dn.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround

- CSCto73151

  Symptoms: An RP resets.

  Conditions: This symptom is observed when the **sh ip nhrp** is entered to check mixed dmvpn and svti.

  Workaround: There is no workaround

- 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.

- CSCto76018

  Symptoms: ASR1000-WATCHDOG crashed after clear crypto session on CES.

  Conditions: This symptom is observed when sessions setting up with the configuration of 1000 vrf, 1 IKE session per vrf and 4 IPSec SA dual per session, hit the crash on ASR1000-WATCHDOG process while CES clear crypto session on CES after all SAs had been established.

  Workaround: There is no workaround.

- CSCto77537

  Symptoms: Calls between SME and Cisco UBE fail due to no audio path when the originating leg is G729r8 and the Cisco UBE preferred codec list contains g729br8.

  Conditions: This symptom occurs under the following conditions:

  - Cisco UBE ISR: Cisco 3845 running Cisco IOS Release 15.1(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
  ```

  Cisco UBE codec configuration:

  ```
  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 the Cisco UBE to ensure that CUBE will offer only g729r8 in the outgoing offer.

Workaround 2: Change the Originating SME, SIP trunk to Originating Cisco UBE from DelayOffer to EarlyOffer.

Workaround 3: Configure a transcoder.

- CSCto79015

  Symptoms: If a connection fails to authenticate, the next http request sent by a client will sit in a redirect loop to the virtual IP for a URL whose authentication was previously aborted.

  Conditions: This symptom is observed when virtual-ip is configured and the first authentication fails.

  Workaround: There is no workaround.

- CSCto80032

  Symptoms: User group information sent to the ScanSafe tower is based on post-NATed IP.

  Conditions: This symptom is observed when configuring “content-scan out” on the egress interface.

  Workaround: There is no workaround.

- CSCto80719

  Symptoms: A Cisco 860 crashes.

  Conditions: This symptom is observed when applying tunnel protection on the tunnel interface.

  Workaround: Use a crypto map configuration.

- CSCto81814

  Symptoms: When SSH is attempted over an IKEv2 tunnel using ECDSA certificates, the router crashes.

  Conditions: This symptom is observed only when ECDSA certificates are used for IKEv2 and not with RSA certificates or with IKEv1.

  Workaround: There is no workaround.

- CSCto86833

  Symptoms: A router 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.

- 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.

- CSCto88581

  Symptoms: The standby RP crashes following an interface configuration change.

  Conditions: This symptom is observed only when “ospf non-stop routing” is configured.

  Workaround: There is no workaround.

- 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

- CSCto92123

  Symptoms: Continuous tracebacks occur at both the ce_sw_encrypt_ipsec_packet and the encrypt_process.

  Conditions: This symptom is observed when switching a traffic profile in Ixia and removing a service-policy under the interface.

  Workaround: There is no workaround.

- CSCto92586

  Symptoms: Chunk leak seen at ipsec_dp_init.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- 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.

- CSCto98742

  Symptoms: A typo may cause a main interface to be deleted when there is no subinterface of the port-channel:

  ```
  %7609(config)#no inter port-channel 1 .1
  ```

  The extra space between the interface and the subinterface numbers can cause all the port-channel 1 configurations to be deleted. Logical interface port-channel 1 and all sub-interfaces under this port-channel are deleted.

  Conditions: Conditions are unknown at this time.

  Workaround: Ensure the correct format is used with no extra spaces in the “no” form of the command.

- CSCto99523

  Symptoms: Convergence can take more time if there are a lot of vrf routes and aggregation is configured in many vrfs and massive route churn happens (for example, a session reset with RR).

  Conditions: Conditions are unknown at this time.

  Workaround: There is no functionality impact.

- 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.

- CSCtq04404

  Symptoms: The browser goes into a redirect loop without prompting for authentication.

  Conditions: This symptom is observed when ip admission, virtual-ip and Basic/NTLM authentication methods are configured.

  Workaround: Remove virtual-ip configurations.

- 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 the Cisco UBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1.3T1.

  Workaround: Upgrade to Cisco IOS Release 15.1.3T or Cisco IOS Release 15.1(M4).

- CSCtq06538

  Symptoms: RP crash due to bad chunk in MallocLite.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtq07222

  Symptoms: Non-RSVP to RSVP calls fail for iLBC codec in Voice class codec.

  Conditions: This symptom is observed with calls involving High density transcoding and Voice class codec with an iLBC codec.

  Workaround: Remove the iLBC codec from the Voice class codec.

- 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.

- CSCtq09542

  Symptoms: A Cisco UBE responds with “481/Transaction does not exist” for CANCEL message.

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

  Workaround: Use Tel URI instead of SIP URI.

  Further Problem Description: SP----(SIP)-----CUBE-----(SIP)---CUCM

  Basic Call Scenarios are working fine with one exception: Party A (outside SIP Network) is calling party B (CUCM Phone). B is ringing, A gets ring-back. Now A cancels the call (before B answers the call). A gets released, B continues ringing.

- CSCtq09712

  Symptoms: A Cisco ASR RP crashes due to L2TP management daemon:

  ```
  %Exception to IOS: Frame pointer 0xXXXXXXXXXXXX, PC = 0xZZZZZZZZ IOS Thread backtrace:
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = L2TP mgmt daemon
  ```

  Conditions: This symptom is observed with L2TP when clearing the virtual access interfaces.

  Workaround: There is no workaround.

- CSCtq09899

  Symptoms: The VXML gateway crashes.

  Conditions: This symptom occurs during the load test when the **show mrcp client session active** is used.

  Workaround: There is no workaround.

- 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.

- CSCtq14817

  Symptom: Traceback or crash might happen when PPTP related traffics were passing through NAT configured device.

Conditions: A race condition when PPTP packets were subjected to NAT, that might cause NAT to behave improperly and cause the issue.

Workaround: There is no workaround.

- 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.

- CSCtq21785

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS-XE 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.

- CSCtq24006

  Symptoms: DMVPN tunnels will not come up with an IPv6 address.

  Conditions: This symptom is observed if more than one tunnel is present on the spoke.

  Workaround: There is no workaround.

- 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.

- CSCtq26057

  Symptoms: Multicast ping fails after manual SA is fixed.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T.

Workaround: There is no workaround.

- CSCtq26892

  Symptoms: A Cisco UBE 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.

- CSCtq27180

  Symptoms: After a Cisco IOS upgrade, any permanent licenses are erased and eval licenses do not work.

  Conditions: This symptom is observed only on IOS internal releases.

  Workaround: There is no workaround.

  Further Problem Description: The following LOG messages and errors are found:

  ```
  Mar 30 01:27:38.003: %LICENSE-2-LIC_STORAGE: Storage validation failed -Traceback=
  604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z 63765DC8z Mar
  30 01:27:38.447: %LICENSE-2-VLS_ERROR:'VLSsetInstallLicenseStorage' failed with an
  error - rc = 136 - 'Error[136]: Specified license store doesn't exists.' -Traceback=
  604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z 63765DC8z
  ```

- CSCtq28151

  Symptoms: A bus error crash occurs.

  Conditions: This symptom is observed on a Cisco 3900 voice gateway running Cisco IOS Release 15.1(3)T1.

  Workaround: There is no workaround.

- 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.

- CSCtq30875

  Symptoms: A Cisco ISR G1 will display "March 11, 2011" when the **show clock** command is entered. This will effect functionality that depends on the clock to be accurate (for example, certificates to make secure connections or calls).

  Conditions: This symptom is observed only on Cisco ISR G1 routers running ISR licensing software.

  Workaround: The clock can be set manually via CLI.

- 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.

- CSCtq35297

  Symptoms: Cisco 880 images do not get compiled.

  Conditions: This symptom occurs during compilation of Cisco 880 images.

Workaround: There is no workaround.

- 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.

- CSCtq37579

  Symptoms: Enabling and disabling snmp-server traps crashes the UUT.

  Conditions: This symptom is observed when disabling the snmp-server, then performing a write memory.

  Workaround: There is no workaround.

- CSCtq38303

  Symptoms: A policy is rejected with an insufficient bandwidth percent guarantee.

  Conditions: This symptom is observed with bandwidth percentage guarantees.

  Workaround: Do not configure bandwidth in percentages.

- CSCtq42864

  Symptoms: A memory leak occurs @ sipSPI_ipip_UpdateSdpForPthru : Basic SDP Passthru Call.

  Conditions: This symptom is observed with SDP PassThru Calls.

  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

- CSCtq47428

  Symptoms: A Cisco router acting as an SRST may unexpectedly reload due to a bus error.

  Conditions: This symptom is observed with phones registered to the SRST.

  Workaround: There is no workaround.

- CSCtq48228

  Symptom: A Cisco UBE crashes: Translate Redirect + 302 Consumption +SDP PassThru Scenario

Conditions: Conditions are unknown at this time.

Workaround: Do not configure “SDP PASSTHRU.”

- CSCtq49408

  Symptoms: Analog phone calls (fxs) cannot be made with CME/SCCP.

  Conditions: This symptom occurs when SCCP support for FXS is missing in a Cisco IAD2435.

  Workaround: There is no workaround.

- CSCtq49860

  Symptoms: If an ISM VPN module is installed in the ISR G2 platform, we will exceed export limits without HSECk9 license installed.

  Conditions: This symptom is observed when an ISM VPN module is installed and enabled for crypto acceleration.

  Workaround: There is no workaround.

- CSCtq55723

  Symptoms: With Transport Control Protocol (TCP) and User Datagram Protocol (UDP), operations with VPN Routing and Forwarding (VRF) are not working.

  Conditions: This symptom occurs only with VRF.

  Workaround: Works without VRF.

- CSCtq59777

  Symptoms: A Cisco device crashes.

  Conditions: This symptom is observed when the **show mrcp client session history** command is entered.

  Workaround: Do not enter the **show mrcp client session history** command.

- 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.

- 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.

- CSCtq75045

  Symptoms: When a router is running FlexVPN-IKEv2 in auto-reconnect mode, IPSec SAs are not renegotiated properly after a **clear crypto session** command is entered. Entering the **show crypto ikev2 client flexvpn** command will indicate that the router is in a NEGOTIATING state.

  Conditions: This symptom is observed on a router running FlexVPN on IKEv2 in auto-reconnect mode.

  Workaround: Enter the **clear crypto ikev2 client flexvpn** command to clear the FlexVPN state and renegotiate the SAs successfully.

- CSCtq83257

  Symptoms: A Cisco 870 platform router crashes while booting with an advipservices image.

  Conditions: This symptom is observed on a Cisco 870 platform router running Cisco IOS Release 15.2(0.18)T and while booting with an advipservices image.

  Workaround: There is no workaround.

- CSCtq86500

  Symptoms: Crypto breaks non-encrypted traffic.

  Conditions: This symptom is observed after migration to Cisco IOS Release 15.0(1)M6.

  Workaround: Disable VSA and use software encryption.

- CSCtq96544

  Symptoms: Application id is limited to 100.

  Conditions: While configuring new applications, the application id allows values in the range 0-100 only.

  Workaround: There is no workaround.

- CSCtr01957

  Symptoms: The system crashes when “crypto engine slot 0" is entered.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtr06926

  Symptoms: CA Server goes to Disable State once Trustpoint authenticated.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtr25821

  Symptoms: Cisco 800 series routers crash with the **isdn leased-line BRI0 128** command:

  ```
  ----- Unexpected exception to CPU: vector 1000, PC = 0x0 , LR = 0x8155A310 -----
  ```

Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtr26531

  Symptoms: When we disable ISM VPN accelerator using no crypto engine slot 0, the ISM VPN module is not disabled. Also, under high load the ISM VPN firmware download will fail.

  Conditions: This symptom is observed with an ISM VPN module and during high traffic loads.

  Workaround: There is no workaround.

- CSCtr37099

  Symptoms: RTCP Passthru does not work for IPv4 to IPv6 calls with two interfaces. The Cisco UBE does not send RTCP packets from the IPv6 interface.

  Conditions: This symptom is observed with two interfaces, and is not seen with only one interface

  Workaround: Enable IPv6 on IPv4-only interface.

- CSCtr44686

  Symptoms: A crash occurs after matching traffic and resetting the connection using the 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: Conditions are unknown at this time.

  Workaround: Replace “reset” with “log.”