Caveats for Cisco IOS Release 15.2(2)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(2)T4

Cisco IOS Release 15.2(2)T4 is a rebuild release for Cisco IOS Release 15.2(2)T. The caveats in this section are resolved in Cisco IOS Release 15.2(2)T4 but may be open in previous Cisco IOS releases.

- 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.

- CSCts60458

  Symptoms: There is a memory leak in PfR MIB.

  Conditions: This symptom occurs when PfR is configured.

  Workaround: There is no workaround.

- CSCtw52610

  Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary interface will be in OOP state.

  Conditions: The issue is seen when primary link is considered OOP based on utilization despite using the **no resolve utilization** command.

  Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR policy based on utilization is not needed, then configure “max-xmit-utilization percentage 100”.

- 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. For example:

  ```
  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”.

- CSCua05196

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

  Conditions: This symptom occurs when SSH traffic is sent.

  Workaround: Enable the warm reboot command.

- 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.

- CSCua55785

  Symptoms: Build breakage due to fix of CSCtx34823.

  Conditions: This issue occurs with CSCtx34823 fix.

  Workaround: CSCtx34823 change may be unpatched from the code-base.

- CSCua73191

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

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

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

  Workaround: Connecting via the portal might help.

- CSCua75069

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

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

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

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

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

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

  Older releases on these trains are not impacted.

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

- CSCua96354

  Symptoms: Reload may occur when issuing the **show oer** and **show pfr** commands.

  Conditions: This symptom is observed with the following commands:

  ```
  a. show oer master traffic-class performance
  b. show pfr master traffic-class performance
  ```

  Workaround: There is no workaround.

- CSCub90459

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

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

  Workaround: There is no workaround.

- CSCuc55634

  Symptoms: IPv6 static route cannot resolve the destination.

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

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

  Workaround: There is no workaround.

- CSCuc98021

  Symptoms: One-way voice audio issue is seen over CUBE after session reinvite is sent.

  Conditions: This symptom is observed with the following call flows:

  ```
  Signaling: Cisco IP phone ==> CUCM ==> CUBE ==> CCIPL ==> CCIPL IP phone Media: Cisco
  IP phone <=== sRTP ==> CUBE <== RTP ==> CCIPL IP phone
  ```

  Workaround: Do not use SRTP on the CUCM <-> CUBE leg.

- CSCud01502

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

  Conditions: This symptom occurs in CME.

  Workaround: There is no workaround.

- CSCud03273

  Symptoms: All the paths using certain next-hops under the route-map are marked inaccessible.

  Conditions: This symptom occurs under the following conditions:

  1. Configure peer groups.
  2. Apply BGP NHT with route-map (no BGP neighbors are created or added to peer groups).
  3. Configure the Prefix-list.
  4. Configure the route-map.

5. Configure the BGP neighbor and add them to peer groups.

Workaround: Configure “route-map permit <seq-num> <name>” or activate at least one neighbor in “address-family ipv4”.

- CSCud06887

  Symptoms: There is no sync of SADB on an active router when it reloads from the current standby router.

  Conditions: This symptom occurs when the active and standby routers are up. Whenever a session is up, there is a sync of SADB from active to standby. When active reloads and is up, there is no sync of SADB from the current active router.

  Workaround: Remove the isakmp-profile configuration under the crypto map.

- CSCud22222

  Symptoms: On a router running two ISIS levels and fast-reroute, the router may crash if “metric-style wide level-x” is configured for only one level.

  Conditions: Issue may happen if metric-style wide is configured for only one level on router running both levels, and fast-reroute is configured.

  Workaround: Configure metric-style wide for both levels (by default).

- CSCud41058

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

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

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

- CSCud62864

  Symptoms: When the Mid-call Re-INVITE consumption feature is active, CUBE consumes Re-INVITE which should change the media state from “sendonly” to “sendrcv”. This results in a one way or no way audio on the call.

  Conditions: This symptom occurs when the CUBE Mid-call Re-INVITE consumption feature is enabled.

  Workaround: There is no workaround.

- CSCud67779

  Symptoms: One-way audio is observed when a call goes through BACD and comes over SIP trunk.

  Conditions: This symptom occurs when a call comes through SIP trunk and is connected to an agent phone via BACD during the third call transfer, along with the “headset auto-answer” configuration in the ephone.

  Workaround: Remove the “headset auto-answer” configuration in the ephone configuration.

- CSCue06309

  Symptoms: A Cisco 2900 series router running IOS 152-4.M1 may generate the following error message:

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

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

Conditions: This symptom occurs when IGMP is enabled on the router and receives multicast traffic.

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

- CSCue36197

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

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

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

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

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

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

- CSCue55739

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

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

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

- CSCue65130

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

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

  Workaround: There is no workaround.

- 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).

- CSCuf09006

  Symptoms: Upon doing a **clear ip bgp * soft out** or **graceful shutdown** on a PE, all VPN v4 or v6 routes on an RR from this PE are purged at the expiry of enhanced refresh stale-path timer.

  Conditions: The symptom is observed with the following conditions:

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

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

- CSCug66784

  Symptoms: DSP Fails to Recover Using “Test DSP Device 0 All Reset”.

  Conditions: A crashed DSP (LSI PVDM3) fails to recover via the CLI command **test voice dsp device 0 all reset**.

  Workaround: A complete reload of the router is required to recover the DSP.

Resolved Caveats—Cisco IOS Release 15.2(2)T3

Cisco IOS Release 15.2(2)T3 is a rebuild release for Cisco IOS Release 15.2(2)T. The caveats in this section are resolved in Cisco IOS Release 15.2(2)T3 but may be open in previous Cisco IOS releases.

- CSCsq83006

  Symptoms: When some port-channels go down at the same time on a router, it can cause EIGRP SIA errors.

  Conditions: The symptom occurs with full mesh four routers which are connected via port-channels. Additionally, it occurs with over five routers which are connected via a partial mesh port-channel.

  Workaround: Use the port-channel interface settings below:

  ```
  (config)# interface port-channel <port-channel interface number>
  (config-if)# bandwidth <bandwidth value>
  (config-if)# delay <delay value>
  ```

  Further Problem Description: If a test is done with a physical interface, not a port-channel, this issue is not seen.

- CSCtj59117

  Symptoms: The following error message is seen and the router freezes and crashes:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle
  ```

  A reload is required to recover.

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

  Workaround: Remove CEF.

- 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 has 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

- CSCto32044

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

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

  Conditions: The conditions are unknown.

  Workaround: There is no workaround.

- 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.

- CSCtq17444

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

  Conditions: The following conditions are observed:

  - Affected Cisco IOS Release: 15.1(3)T.
  - Affected platforms: routers acting as voice gateway for H.323.

  Workaround: There is no workaround.

- CSCtq91063

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

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

  Workarounds:

  1. Remove MTU override from the tunnel interface; or
  2. Configure “service disable-ip-fast-frag”; or
  3. Reduce hold queue sizes such that the total size of the queues for all active interfaces in the system does not exceed 512.

- CSCtr70641

  Symptoms: When a router that is running a version before REL8, is rebooted with an IOS version having EIGRP REL8 onwards it does not show routes received from peer in EIGRP topology.

  Conditions: Initially all the devices are running EIGRP version before REL8 (**show eigrp plug** shows that). Now when a device is booted with newer EIGRP version (REL8 onwards) and it comes up before its hold down timer is expired on peers then this issue is hit.

  Workaround: There is no workaround.

- CSCts38674

  Symptoms: UUT/modem fails to make a call using external dialer interface.

Conditions: The symptom is observed when the cellular interface is configured with “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”.

- CSCts83046

  Symptoms: Back-to-back ping fails for P2P GRE tunnel address.

  Conditions: The symptom is observed when HWIDB is removed from the list (through **list remove**) before it gets dequeued.

  Workaround: There is no workaround.

- CSCtt17039

  Symptoms: UUT is reloaded with OSPFv3 IPsec authentication configured. The UUT has formed neighborship with two routers over port-channel.

  Conditions: The symptom is observed when the UUT is reloaded with OSPFv3 IPsec authentication configured.

  Workaround: There is no workaround.

- CSCtt97905

  Symptoms: Multiple demandNbrCallDetails traps generated.

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

  Workaround: There is no workaround.

- CSCtu08373

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

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

  Workaround: There is no workaround.

- CSCtu11013

  Symptoms: The router crashes when the SAF forwarder is enabled.

  Conditions: This symptom is observed when the SAF forwarder is enabled.

  Workaround: Disable the SAF forwarder.

- 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.

- 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.

- CSCtw48553

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

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

  Workaround: There is no workaround.

- CSCtw86793

  Symptoms: A Cisco router running Cisco IOS 15.2T will generate phase II rekeys using IKEv1 instead IKEv2.

  Conditions: The symptom is observed with an IKEv2 DVTI hub (tunnel mode GRE IP).

  Workaround: Anchor the IKEv2 profile into the IPsec profile.

- CSCtx45373

  Symptoms: Under **router eigrp virtual-name** and **address-family ipv6 autonomous-system 1**, when you enter **af-interface Ethernet0/0** to issue a command and exit, and later, under **router bgp 1** and **address-family ipv4 vrf red**, you issue the **redistribute ospf 1** command, the "VRF specified does not match this router" error message is displayed. When you issue the **redistribute eigrp 1** command, it gets NVGENd without AS number.

  Conditions: This symptom occurs under **router eigrp virtual-name** and **address-family ipv6 autonomous-system 1**, when you enter **af-interface Ethernet0/0** to issue a command and exit, and later, under **router bgp 1** and **address-family ipv4 vrf red**, you issue the **redistribute ospf 1** command.

  Workaround: Instead of using the **exit-af-interface** command to exit, if you give a parent mode command to exit, the issue is not seen.

- CSCty54695

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

  Conditions: This symptom is observed under the following conditions:

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

  Workaround: Clear the crypto session with the peer.

- CSCty61216

  Symptoms: CCSIP_SPI_Control causes leak with a Cisco AS5350.

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

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

Workaround: There is no workaround.

- CSCty82414

  Symptoms: A crash is seen.

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

  Workaround: Unconfigure IPS.

- 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.

- 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.

- CSCtz35999

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

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is available at the following link:

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

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

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

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

- 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.

- CSCtz47595

  Symptoms: Dial string sends digits at incorrect times.

  Conditions: The symptoms are seen with a Cisco 3925 router running Cisco IOS Release 15.2(3)T using PVDM2-36DM modems with firmware version 3.12.3 connecting over an ISDN PRI to an analog modem.

When using a dial string to dial an extension (or other additional digits), the modem should answer before the dial string is sent. If a comma is used, there should be a pause after connecting before sending the digits. The default value of the digital modem is one second per comma; two commas would be two seconds, three commas = three seconds and so on.

1. With any number of commas in the string, debugs show the digits are sent at random intervals, sometimes before the call was answered and as much as up to 30 seconds after the call connects, i.e.: 919195551212x,22 or 1212x,,,22.
2. With no comma in the dial string, the digits are sent immediately after being generated without waiting for a connection, i.e.: 919195551212x22.

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

Workaround: There is no workaround.

- CSCtz58719

  Symptoms: Watchdog timeout is seen under interrupt or process.

  Conditions: This symptom is observed with a QoS configuration applied. The issue happens because of resource contention between a process path packet and an interrupt path packet.

  Workaround: Disable QoS.

- CSCtz58941

  Symptoms: The router crashes when users execute the **show ip route XXXX** command.

  Conditions: This symptom is observed during the display of the **show ip route XXXX**, when the next-hops of “XXXX” networks are removed.

  Workaround: The **show ip route XXXX** command (without “XXXX”) does not have the problem.

- CSCtz59145

  Symptoms: A crash occurs randomly. The following error messages are often seen before the crash:

  ```
  Mar 31 16:30:16.955 GMT: %SYS-2-MALLOCFAIL: Memory allocation of 20 bytes failed from
  0x644DA7E0, alignment 0 Pool: Processor Free: 274176384 Cause: Interrupt level
  allocation Alternate Pool: None Free: 0 Cause: Interrupt level allocation -Process=
  "<interrupt level>", ipl= 1
  Mar 31 16:30:16.963 GMT: %SYS-3-BADLIST_DESTROY: Removed a non-empty list(707C0248,
  name: FW DP SIP dialog list), having 0 elements
  ```

  This device is not actually running out of memory. There is a memory action going on at the interrupt level which is not allowed.

  Conditions: This symptom occurs when Zone-Based Firewalls inspect SIP traffic. This issue is likely related to the tracebacks and error messages given above. The actual condition is still being investigated.

  Workaround: If plausible, disabling SIP inspection could possibly prevent further crashes.

- CSCtz69084

  Symptoms: The switch crashes when trying to enable IPsec MD5 authentication on the SVI.

  Conditions: This symptom is observed with the following conditions:

  ```
         VLAN 101
  SW1---------------SW2
  ```

  1. Configure the IPsec MD5 authentication in global configuration mode.

  ```
  ipv6 router ospf 1
  area 0 authentication ipsec spi 1000 md5 123456ABCDEF123456ABCDEF123456AB
  ```

  2. Configure the IPsec MD5 authentication as below in the interface mode with MD5 key 7 and device crashes.

Workaround: There is no workaround.

- CSCtz71084

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

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

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

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

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

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

  Workaround: Hard clear.

- CSCua21166

  Symptoms: Unable to form IPSec tunnels due to error: “RM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with securityk9 technology package license.”

  Conditions: Even though the router does not have 225 IPsec SA pairs, error will prevent IPSec from forming. Existing IPSec SAs will not be affected.

  Workaround: Reboot to clear out the leaked counter, or install hsec9 which will disable CERM (Crypto Export Restrictions Manager).

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 2.8/2.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:M/C:N/I:N/A:P/E:U/RL:W/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

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

- CSCua22789

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

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

  Workaround: There is no workaround.

- 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.

- CSCua61330

  Symptoms: Traffic loss is observed during switchover if,

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

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

  Workaround: There is no workaround.

- 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.

- CSCua70065

  Symptoms: CUBE reloads on testing DO-EO secure video call over CUBE when SDP passthru is enabled.

  Conditions: The symptom is observed when running Cisco IOS interim Release 15.3(0.4)T.

  Workaround: There is no workaround.

- CSCua99969

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

  Conditions: This symptom occurs in the VRF context.

  Workaround: There is no workaround.

- CSCub05907

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

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

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

- CSCub10951

  Symptoms: At RR, for an inter-cluster BE case, there are missing updates.

  Conditions: This symptom is observed with the following conditions:

  1. The following configuration exists at all RRs that are fully meshed:
     - bgp additional-paths select best-external
     - nei x advertise best-external
  2. For example, RR5 is the UUT. At UUT, there is,
     - Overall best path via RR1.
     - Best-external (best-internal) path via PE6 (client of RR5): for example, the path is called “ic_path_rr5”.
     - Initially, RR5 advertises “ic_path_rr5” to its nonclient iBGP peers, that is, RR1 and RR3.
  3. At PE6, unconfigure the route so that RR5 no longer has any inter-cluster BE path. RR5 sends the withdrawals to RR1 and RR3 correctly.
  4. At PE6, reconfigure the route so that RR5 will have “ic_path_rr5” as its “best-external (internal) path”. At this point, even though the BGP table at RR5 gets updated correctly, it does not send the updates to RR1 and RR3. They never relearn the route.

  Workaround: Hard/soft clear.

- CSCub18682

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

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

  Workaround: There is no workaround.

- CSCub28913

Symptoms: The Cisco ISR G2 with VPN-ISM drops packets over an IPsec tunnel-protected tunnel interface.

Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T images, when there is a crypto map (static or dynamic) applied to the interface.

Workaround:

- Disable the ISM-VPN (issue “no crypto engine slot xx”, where xx is the slot number where the ISM is located).
- Alternatively, change the configuration to use either static or dynamic VTIs for the tunnels where you need a crypto-map.

- CSCub45809

  Symptoms: Cisco IOS configured for Voice over IP may experience stack corruption due to multiple media loops.

  Conditions: This requires a special configuration of IP features along with disabling the recommended media flow-around command. IOS version 15.2(2)T

  Workaround: Apply media flow-around command.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:U/RL:W/RC:C CVE ID CVE-2012-5044 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

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

- CSCub54872

  Symptoms: A /32 prefix applied to an interface (e.g.: a loopback) is not being treated as connected. This can impact the connectivity of the /32 prefix.

  Conditions: The symptom is observed when the prefix applied to an interface is for a host route (/32 for IPv4 or /128 for IPv6).

  Workaround: Use a shorter prefix.

  Further Problem Description: This issue does not affect software switching platforms.

- CSCub69976

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

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

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

- CSCub70336

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

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

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

- CSCub84239

  Symptoms: ISM-VPN (reventon) crash is observed.

  Conditions: The symptom is observed while reassembling ESP packets before decryption.

  Workaround: Disable ISM-VPN (reventon) and use either onboard crypto engine or software crypto engine.

- CSCub84471

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

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

  Workaround: There is no workaround.

- CSCub86706

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

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

  Workaround: There is no workaround.

- 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.

- CSCuc42518

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

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

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

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4/3.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:OF/RC:C CVE ID CVE-2012-5427 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

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

- CSCuc56259

  Symptoms: A Cisco 3945 that is running 15.2(3)T2 and running as a voice gateway may crash. Just prior to the crash, these messages can be seen:

  ```
  %VOIP_RTP-6-MEDIA_LOOP: The packet is seen traversing the system multiple times
  ```
  and

  ```
  Delivery Ack could not be sent due to lack of buffers.
  ```

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

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

- CSCuc67033

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

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

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

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

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

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

  Conditions: This symptom is observed with the following conditions:

  – The ISM VPN crypto acceleration module is installed, enabled, and used for crypto operations (IPsec, etc.).

  – Cisco IOS supports ISM VPN (Cisco IOS Release 15.2(1)T1 or later releases).

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

- 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.

Resolved Caveats—Cisco IOS Release 15.2(2)T2

Cisco IOS Release 15.2(2)T2 is a rebuild release for Cisco IOS Release 15.2(2)T. The caveats in this section are resolved in Cisco IOS Release 15.2(2)T2 but may be open in previous Cisco IOS releases.

- CSCsg48725

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

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

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

  Workaround: Disable AAA. If this not an option, there is no workaround.

- CSCsy93069

  Symptoms: After a period of telepresence calls, tracebacks and then a router crash is seen.

  Conditions: The symptom is observed only when running Cisco IOS firewall with l7 SIP inspect policies applied. This crash happens at low scale with one CTS 3k call cycling with a hold time of 600 secs.

  It occurs intermittently and over time in an environment where there may be some call failures.

  Workaround: There is no workaround.

- 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.

- CSCtj48387

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

  Conditions: DHCP must be enabled and sessions should be getting DHCP information from a RADIUS server.

  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.

- CSCtq99664

  Symptoms: Traffic does not egress from the interface.

  Conditions: The VRF set on the interface is originally configured for IPv4 and IPv6 address family. If the VRF is reconfigured to remove the IPv4 address family, then all interfaces in that VRF stop sending traffic.

  Workaround: Shut down and re-enable the interface in question.

- CSCtr22434

  Symptoms: Stale IPsec policy is not cleared and the same SPI cannot be used until you reload. Memory leak of crypto acl is also observed.

  Conditions: The symptom is observed with “OSPFv3 ipsec authentication” configured on in the interface.

  Workaround: Use a different SPI or reload the router.

- 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.

- CSCtr86328

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

  Conditions: Cisco IOS device 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

- CSCtr87070

  Symptoms: Enable login failed with error "% Error in authentication".

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

  Workaround: Remove TACACS single-connection.

- CSCts00341

  Symptoms: When executing a CLI that requires domain-name lookup such as **ntp server** *server.domain.com*, the command fails with the following message on the console:

```
ASR1k(config)#ntp server server.domain.com         <<<    DNS is not resolved
with dual RPs on ASR1k
Translating "server.domain.com "...domain server (10.1.1.1) [OK]

%ERROR: Standby doesn't support this command              ^
% Invalid input detected at '^' marker.

ASR1k(config)#do sh run | i ntp
ASR1k(config)#
```

  Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

  Workaround: Instead of using *hostname* in the command, specify the IP address of the host.

- CSCts32708

  Symptoms: Similar to CSCth80642, IOS SSLVPN router fails to accept new sessions. The users will not be able to load the webvpn login page. If you enable debug sdps you may see: Sev 4:sdps_get_pak_from_tcp(),line 1080:tcp_getpacket returned error 2, tcb=0x6A9EFFEC

Conditions: The router remains reachable otherwise (ie you can ping the webvpn IP) SSL process is running and listening on the right port. “Show tcp tcb” and “show tcp brief all numeric” will show connections stuck in CLOSED and CLOSEWAIT state. Clearing the tcp tcb sessions does not restore connectivity Taking webvpn in/out of service does not restore connectivity Disabling webvpn cef and rebooting does not prevent the issue Rebooting does resolve the issue temporarily

Workaround: 1. Reboot. 2. If available for your platform, get the fix for CSCth80642 AND disable webvpn cef (you should reboot or clear the tcb connections after disabling webvpn cef). This may prevent the problem.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2011-3286 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts34693

  Symptoms: A Cisco router may crash with the following error message:

```
000199: %BGP-5-ADJCHANGE: neighbor x.x.x.x  Up
Exception to IOS Thread:
Frame pointer 0x30CF1428, PC = 0x148FDF84
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EEM ED Syslog
-Traceback=
1#07279b80de945124c720ef5414c32a90  :10000000+48FDF84 :10000000+48FE400 :10000
000+4B819C8 :10000000+4B81964 :10000000+F5FAD8 :10000000+F5FD10 :10000000+F5FE
F0 :10000000+F5FF94 :10000000+F60608
```

  Conditions: This symptom is observed with a Cisco ASR 1004 router running Cisco IOS Release 15.0(1)S. This problem appears to be related to an EEM script that executes on a syslog event.

```
event manager applet BGP-MON
 event tag BGP-DOWN syslog pattern "BGP-5-ADJCHANGE.*Down"
 event tag BGP-UP syslog pattern "BGP-5-ADJCHANGE.*Up"
trigger
  correlate event BGP-DOWN or event BGP-UP
 action 02 cli command "enable"
 action 03 cli command "sh log"
 action 04 mail server "$_email_server" to "$_email_to" from
"$_info_routername@mcen.usmc.mil" subject "Problems on $_info_routername,
BGP neighbor Change" body "$_cli_result"
```

  Workaround: There is no workaround.

- CSCts72911

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

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

  Workaround: There is no workaround.

- 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.

- CSCtt23358

  Symptoms: RP reset @ __be_tunnel_protection_remove_idb_for_connection in flexVPN scale setup.

  Conditions: The symptom is observed with a shut/no shut on a flex tunnel and then executing the command **clear crypto session**.

  Workaround: There is no workaround.

- CSCtt26208

  Symptoms: A Cisco 3845 running Cisco IOS Release 15.1(4)M1 may have a processor pool memory leak in CCSIP_SPI_CONTROL.

  Conditions: Not known at this time.

  Workaround: There is no workaround.

- CSCtt26692

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

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

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

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

- 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).

- CSCtt43843

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

  Conditions: This symptom is occurring with a Cisco 7200 platform that is loaded with the Cisco IOS Interim Release 15.2(1.14)T0.1 image.

  Workaround: There is no workaround.

- CSCtt46730

  Symptoms: Platform crashes during IKEv2 negotiation between the spoke and the hub with Cisco TrustSec (CTS) enabled on the Cisco 3945E platform.

  Conditions: This symptom is seen with re-negotiation of IKEv2 SA between the peers.

  Workaround: There is no workaround.

- CSCtt47007

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

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

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

  Workaround: Disable WebVPN CEF and reload the router.

- CSCtt95505

  Symptoms: The router crashes after configuring OSPF routing protocol.

  Conditions: The crash occurs after:

  1. Configuring OSPF with a summary prefix.
  2. Deconfiguring OSPF; and then
  3. Configuring OSPF again. For example:

  ```
  ipv6 router ospf 1
   router-id 1.1.1.1
   summary-prefix 2001:0db8:1:1::/64
   redistribute connected

  no ipv6 router ospf 1

  ipv6 router ospf 1
   router-id 1.1.1.1
   summary-prefix 2001:odb8:1:1::/64
   redistribute connected
  ```

  Workaround: There is no workaround.

- CSCtt96597

  Symptoms: Unable to power-cycle modem using **test cellular** *unit* **modem-power-cycle**.

  Conditions: The symptom is observed when a router cannot communicate with the modem due to a possible modem firmware crash or device disconnect.

  Workaround: Reload router.

- CSCtu07626

  Symptoms: Router processing SIP traffic crashes.

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

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

  Workaround: There is no workaround.

- CSCtu19450

  Symptoms: A system that is running Cisco IOS may reload when a large number of routes are simultaneously deleted at the same time that the inetCidrRouteTable is being walked.

  Conditions: This symptom is only likely to happen when there are large numbers of interfaces and routes within the system, and when large numbers of routes are being rapidly removed, and the system is loaded, at the same time that the inetCidrRouteTable is being walked.

  Routes may be deleted from the system both directly, and also indirectly for example, when a significant number of PPPoE sessions are removed.

  Workaround: Avoid walking the inetCidrRouteTable while significant numbers of routes are being removed from the routing system.

- CSCtu25150

  Symptoms: A Cisco router acting as a voice gateway may unexpectedly reload due to a SegV exception or bus error, or may experience a spurious access.

  Conditions: The exact conditions leading to the crash are not known. The issue is only present in Cisco IOS Release 15.1(4)M and later.

  Workaround: There is no workaround.

- CSCtu29881

  Symptoms: A router may crash while using double authentication for IPsec (ESP + AH) and certain types of traffic.

  The following message is seen in the crashinfo file:

```
validblock_diagnose, code = 1
current memory block, bp = 0xZZZZZZZZ, memorypool type is I/O data check, ptr =
0xZZZZZZZZ
next memory block, bp = 0xZZZZZZZZ, memorypool type is I/O data check, ptr = 0xZZZZZZZ
previous memory block, bp = 0xZZZZZZZZ, memorypool type is I/O data check, ptr =
0xZZZZZZZZ
The router crashes due to I/O memory corruption - block overrun.
```

  Conditions: 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.

- CSCtu32301

  Symptoms: Memory leak may be seen.

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

  Workaround: Do not run the show commands frequently.

- 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: Either do a **clear crypto gdoi** after a reload, or configure a second keyserver entry. This does not have to be an existing keyserver, it can be just a dummy address.

- CSCtu43120

  Symptoms: Service accounting start is not sent for L2TP sessions.

  Conditions: This symptom is observed with L2TP.

  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.

- CSCtw41214

  Symptoms: ACEs are not source IP translated in multidomain authentication (MDA) mode.

  Conditions: The symptom is observed in MDA mode.

  Workaround: There is no workaround.

- CSCtw46229

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

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

  Workaround: Ensure all your PPP connections stay stable.

- 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

- 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.

- CSCtw58664

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

  Conditions: The symptom is observed when using the SSL VPN for SCCP phones feature and when clearing the WebVPN session:

  clear webvpn session context SSLVPNphone

  ```
  [WV-TUNL-EVT]:[0] Returning address 10.0.112.200 to pool
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x2601227C
  -Traceback= 0x26008B3Cz 0x25F9D7E8z 0x25F94A3Cz 0x224B66A8z 0x224BCBA8z
  0x224CBF70z 0x23D22684z 0x23D189C0z 0x237F0144z 0x237F0128z -Traceback=
  0x26008B3Cz 0x25FCEAA8z 0x238561D8z
  ```

  The frequency of the issue is rare.

  Workaround: There is no workaround.

- CSCtw59086

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

  The following message is seen in the Syslog: %SSLVPN-6-LICENSE_NO_FREE_COUNT: All avaiable SSLVPN session licenses are in use

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

  For example:

  sh webvpn session context all

  show webvpn license

```
Max platform license count : 1500
  Available license count    : 100
  Reserved license count     : 100
* In-use count               : 4294967295
```

  Workaround: Reload the Cisco router.

- 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.

- CSCtw73544

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

  Conditions: This symptom is observed with PPP over ATM

  Workaround: There is no workaround.

- CSCtw78064

  Symptoms: The **display-logout** message on a Cisco SCCP Phone is not cleared even after pressing other buttons on the phone.

  Conditions: This symptom is observed on the Cisco SCCP phone (also known as Skinny Phone or ePhone) when the last extension mobility (EM) user in a hunt group logs out using the HLog button. This symptom is observed even if the last EM user logs out of the hunt group and logs back in.

  Workaround: There is no workaround.

- 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

- CSCtw87132

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

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

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

  Workaround: There is no workaround.

- CSCtw95189

  Symptoms: The "%Unknown DHCP problem. No allocation possible" error is observed in the DHCP error log.

  Conditions: This symptom occurs when open access is enabled and the supplicant is authz failed. Then, DHCP IP address assignment does not take place.

  Workaround: There is no workaround.

- 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.

- CSCtx04709

  Symptoms: Some EIGRP routes may not be removed from the routing table after a route is lost. The route is seen as "active" in the EIGRP topology table, and the active timer is "never".

  Conditions: This symptom is seen when a multiple route goes down at the same time, and query arrives from neighbor router. Finally, neighbor detects SIA for affected router and neighbor state is flap. However, active entry is remaining after that, and route is not updated.

  Workaround: The **clear ip eigrp topology** *network mask* command may remove unexpected active entry.

- 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.

- CSCtx22322

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

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

  Workaround: There is no workaround.

- 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.

- CSCtx32527

  Symptoms: The **show crypto session** command reveals the flexVPN GRE tunnel is in a DOWN state instead of DOWN-negotiating.

  Conditions: The symptom is observed with “ip address negotiated” configured on the GRE tunnel interface (with tunnel protection). The tunnel is unable to reach the gateway initially.

  Workaround: Configure an IP address on the tunnel interface instead of “ip address negotiated”.

- 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.

- CSCtx45970

  Symptoms: A crash is seen only in the negative case, when the frequency is not a multiple of history interval.

  Conditions: The symptom is observed when the value is not initialized.

  Workaround: Configure the right configuration with frequency being the multiple of interval.

- CSCtx47213

  Symptoms: The following symptoms are observed:

  1. Session flap when iBGP local-as is being used on RRs.
  2. Replace-as knob is not working in iBGP local-as case.

  Conditions:

  1. The session will flap when iBGP local-as is used on the RR client and RR sends an update.
  2. Replace-as knob even used is ignored and prefixes are appended with local-as.

  Workaround: Do not use iBGP local-as.

- 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.

- CSCtx54882

  Symptoms: A Cisco router may crash due to Bus error crash at voip_rtp_is_media_service_pak.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 15.1(4)M2.

  Workaround: There is no known workaround.

- 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.

- CSCtx64347

  Symptoms: Despite open access being configured on the port, traffic to/from the client is blocked.

  Conditions: This symptom occurs when an authenticating port with open-access and multi-auth hostmode configured, is interrupted.

  Workaround: There is no workaround.

- CSCtx64684

  Symptoms: While configuring the ISIS on two Cisco 2921 routers connected back to back, the ISIS neighbors do not come up.

  Conditions: This symptom is observed only on the SVI interface. This issue is only seen with EHWIC.

  Workaround: If the router has an L3 port, form a neighborship on a physical interface directly or create dot1q subinterfaces if peering is required on multiple VLANs.

- CSCtx65979

  Symptoms: A Cisco 2801 cannot boot up using -adventerprisek9-mz images or higher starting with Cisco IOS interim Release 15.2(2.15)T. Reports insufficient memory to load the image.

  Conditions: The symptom is observed at boot up.

  Workaround: Use -ipbasek9-, -ipvoicek9-, images.

- CSCtx66030

  Symptoms: A Cisco router handling SIP registrations/unregistrations may unexpectedly reload. This symptom is observed on the following devices:

  - SIP-CME
  - SIP-SRST GW
  - CUBE

  Conditions: This symptom is observed when the number of SIP registrations/unregistrations handled is more than 320.

  Workaround: Limit the number of registrations/unregistrations to less than 320.

- CSCtx66046

  Symptoms: The Standby RP crashes with a traceback listing db_free_check.

  Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.

  Workaround: Before removing the address, remove the network statement which covers he address of the loopback interface.

- 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.

- CSCtx67474

  Symptoms: Update message is sent with an empty NLRI when the message consists of 2byte aspath in ASPATH attribute and 4byte value aggregate attribute.

  Conditions: This can happen when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.

  Workaround: Move all the 2byte AS peers to a separate update-group using a non-impacting outbound policy like “advertisement-interval”.

- 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.

- CSCtx87646

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

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

  Workaround: There is no workaround.

- CSCtx90705

  Symptoms: Several MPLS features fail for ping.

  Conditions: The symptom is observed during ISSU downgrade.

  Workaround: There is no workaround.

- CSCtx92802

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

  Conditions: The symptom is observed under the following conditions:

  - Cisco IOS Release 15.0(1)M7 on a Cisco 1841.
  - VRF enabled.
  - CEF enabled.

  - VPN tunnel.

  Workaround: Disable VFR or CEF.

- CSCty01234

  Symptoms: A router running Cisco IOS may reload unexpectedly.

  Conditions: This symptom is observed only with low-end platforms using VDSL interfaces, such as a Cisco 887 router. It also requires that the **qos pre-classify** command be used in conjunction with IPsec and GRE, such as in a DMVPN configuration.

  Workaround: Do not use the **qos pre-classify** command.

- CSCty02403

  Symptoms: An EIGRP topology entry with bogus nexthop is created when more than one attribute is present in the route received from neighbors. It also tries to install one default route with bogus nexthop. So if you have a default route received from some neighbors, then that default route will also flap.

  Conditions: It can only occur when more then one attribute set in any route received from a neighbor.

  Workaround: Do not set more then one attribute in the route.

- 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.

- CSCty21638

  Symptoms: The Cisco 3945 router crashes with the base configuration of SAF/EIGRP.

  Conditions: This symptom occurs when enabling the SAF Forwarder on the Cisco 3945 router.

  Workaround: There is no workaround.

- CSCty30185

  Symptoms: Call transfer to an element crashes if one of the element’s number is invalid.

  Conditions: The issue is observed when call is transferred to parallel hunt group.

  Workaround: There is no workaround.

- 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.

- CSCty37445

  Symptoms: A DMVPN hub router with a spoke which is an EIGRP neighbor. The spoke receives a subnet from hub and then advertises it back to the hub, bypassing split horizon.

  Conditions: The symptom is observed when on the spoke you have a **distribute list route-map** command setting tags.

  Workaround: Once you remove that command EIGRP works normally.

- CSCty42626

  Symptoms: Certificate enrollment fails for some of the Cisco routers due to digital signature failure.

  Conditions: This symptom was initially observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.

  This issue potentially impacts those platforms with HW crypto engine. Affected platforms include (this is not a complete/exhaustive list)

  - c3925E, c3945E
  - c2951, c3925, c3945
  - c7200/VAM2+/VSA, possibly VPNSPA on c7600/cat6K
  - 819H ISR G2 routers with ISM IPSec VPN accelerator

  Workaround: There is no workaround.

- CSCty43587

Symptoms: Crash observed with memory corruption similar to the following:

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

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

Workaround: There is no workaround.

- CSCty48870

  Symptoms: Router crash due to a bus error.

  Conditions: This has been observed in router that is running Cisco IOS Release 15.2(2)T and 15.2(3)T with NBAR enabled on a crypto-enabled interface. NBAR can be enabled through NAT, QoS, or NBAR protocol discovery.

  Workaround: Using **no ip nat service nbar** will help where NBAR is enabled through NAT.

- CSCty53243

  Symptoms: Video call fails in the latest mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has the uc_infra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.

  Conditions: This symptom is observed when CUBE changes the video port to “0” in 200 OK sent to the UAC.

  Workaround: There is no workaround.

- CSCty54434

  Symptoms: ISRG2 with ISM VPN is not bringing up more than one tunnel in a crypto map-based scenario with large certificates (4096 bit).

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

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

- CSCty56850

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

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

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

  show IP NBAR protocol-discovery

  Workaround 2: Perform a snmpget against objects in cnpdAllStatsTable.

- CSCty58992

  Symptoms: One-way audio is observed after transfer to a SIP POTS Phone.

  Conditions: This symptom is observed under the following conditions:

  – Cluster is in v6 mode.

  – A call is made from Phone1 to Phone2, and then Phone2 transfers the call to Phone3(SIP POTS), which is when the issue occurs.

  Workaround: There is no workaround.

- CSCty64721

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

  Conditions: The CTI front end process is using up huge memory causing the CME to crash eventually. When the crash occurs:

```
Processor Pool Total:  140331892 Used:  140150164 Free:     181728
      I/O Pool Total:   27262976 Used:    5508816 Free:   21754160
```

  Workaround: There is no workaround.

- CSCty65189

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

  Conditions: 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.

- CSCty68348

  Symptoms: If the OSPF v2 process is configured with the **nsr** command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

  Conditions: This symptom is observed under the following conditions:

  - The OSPF router is configured for “nsr”.
  - Shutdown/no shutdown of the OSPF process.

  Workaround: Flapping of the neighbor will fix the issue.

- CSCty77190

  Symptoms: DTLS is switched back to TLS after reconnect.

  Conditions: This symptom is observed with the following conditions:

  - Test image c3845-advsecurityk9-mz.152-2.T1.InternalUseOnly
  - Test version - Cisco IOS Release 15.2(01)T

  Workaround: Restart the AnyConnect client.

- CSCty78435

  Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

  Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- CSCty805o53

  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.

- 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.

- CSCty97784

  Symptoms: The router crashes.

  Conditions: This symptom is observed when NBAR is enabled, that is, “match protocol” actions in the QoS configuration, or “ip nbar protocol-discovery” on an interface or NAT is enabled and “ip nat service nbar” has not been disabled.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCtz25953

  Symptoms: “LFD CORRUPT PKT” error message is dumped and certain length packets are getting dropped.

  Conditions: The symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

  Workaround: There is no workaround.

- 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**.

- CSCtz70623

  Symptoms: A Cisco router may experience a software-forced crash.

  Conditions: Crash may occur when a 2-wire cable is unplugged from the G.SHDSL interface.

  Workaround: There is no workaround.

- CSCtz70938

  Symptoms: When the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are "service-module" CLI in the configuration, the router crashes.

  Conditions: This symptom occurs when the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are "service-module" CLI in the configuration, the router crashes.

  Workaround: Do not use boot configuration files other than startup-configuration when there are "service-module" CLI in the configuration.

- CSCtz72044

  Symptoms: EzVPN client router is failing to renew ISAKMP security association, causing the tunnel to go down.

  Conditions: The issue is timing-dependent, therefore the problem is not systematic.

  Workaround: There is no workaround.

- 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.

- CSCtz99916

  Symptoms: The Cisco 3945 router does not respond to a reinvite from CVP.

  Conditions: This symptom occurs when call legs are not handled in a proper IWF container.

  Workaround: There is no workaround.

- CSCua06598

  Symptoms: Router may crash with breakpoint exception.

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

  Workaround: Disable SNMP IPv6 polling.

- CSCua07791

  Symptoms: A Cisco ISR G2 running Cisco IOS Release 15.2(2)T or later shows a memory leak in the CCSIP_SPI_CONTRO process.

  Conditions: The leak is apparent after 3-4 weeks. The process is CCSIP_SPI_CONTRO.

  Workaround: There is no workaround.

- CSCua31157

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

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

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

  Workaround: There is no workaround.

- 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.

- CSCua44462

  Symptoms: DNS reply is not cached.

  Conditions: DNS based X25 routing. DNS server is reachable via IPsec over Gig link and SHDSL links. There are Cisco devices at different locations. Few of them are communicating to DNS server via IPsec over Gig link and few of them are communicating via IPsec over ATM (EHWIC-4SHDSL-EA and HWIC-4SHDSL). It is seen that the UDP reply contains the x25 address to IP address resolution but it is not being used by the router causing X25 calls to fail.

  Workaround: There is no workaround.

- 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.

Resolved Caveats—Cisco IOS Release 15.2(2)T1

Cisco IOS Release 15.2(2)T1 is a rebuild release for Cisco IOS Release 15.2(2)T. The caveats in this section are resolved in Cisco IOS Release 15.2(2)T1 but may be open in previous Cisco IOS releases.

- 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 command:

  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.

- CSCto59459

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

  Conditions: Any TCP connection will suffer from this defect.

  Workaround: There is no workaround.

- 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.

- CSCto93880

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

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

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

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

- CSCtq12007

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

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

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

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

- CSCtq59923

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

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

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

- 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

- 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

- CSCtr47642

  Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP non-clients and iBGP RR clients and enabling the BGP best-external feature using the **bgp additional-paths select best- external** command, a specific prefix may not have bestpath calculated for a long time.

  Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:

  1. Configure: **bgp additional-paths install** under vpnv4 AF
  2. Configure: **bgp additional-paths select best-external**

  Immediately disable backup path calculation/installation using the **no bgp additional-paths install** command.

  The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.

  Workaround: Configure the **bgp additional-paths install** command and the **bgp additional-paths select best-external** command with a delay of 10 seconds.

- CSCtr86149

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

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

  Workaround: There is no workaround.

- CSCtr88739

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

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

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

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

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

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

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

- CSCtr94471

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

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

  Workaround: There is no workaround.

- 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.

- 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.

- 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
```

- 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

- CSCts44718

  Symptoms: A router may crash.

  Conditions: The crash may occur when a service policy that has a flow monitor as an action is applied to a virtual interface and that virtual interface is deleted. It may also occur when the service policy is applied to a physical interface that is removed by OIR.

  Workaround: Before deleting (or OIRing) the interface, remove the flow monitor from the policy or the policy from the interface.

- CSCts46578

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

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

  Retransmitted packet is allowed through.

  Conditions: CBAC configured.

  Workaround: There is no workaround.

- 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-talker commands.

- CSCts63501

  Symptoms: The non-EOS forwarding path for the explicit null label (reserved label 0) is programmed as drop on the linecard, resulting in PW traffic loss with an MPLS LDP explicit-null configuration.

Conditions: The PW traffic loss occurs on linecards in which MPLS LDP explicit-null is set.

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.

- CSCts67465

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

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

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

- CSCts70790

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

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

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

- CSCts76410

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

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

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

- CSCts78348

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

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

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

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

  Workaround 2: Use auto negotiation.

- 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.

- CSCts97925

  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

  Conditions: This symptom is observed only with IPv6, and not with IPv4.

  Workaround: Disable IPv6 CEF.

- CSCts99818

  Symptoms: Traceback is seen.

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

  Workaround: There is no workaround.

- 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.

- CSCtt03207

  Symptoms: Traffic flows through unauthorized supplicant switch

  Conditions: Authenticator Switch should have established auto-config with authorized supplicant switch. Now bring up, unauthorized supplicant switch by physically connecting to hub placed between ASW & SSW. Though wrong dot1x credential is used, ASW allows network access for unauthorized SSW.

  Workaround: None.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 2.9/2.4:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:M/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

- CSCtt05316

  Symptoms: Under **show content-scan sessions active**, the user group 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.

- CSCtt13401

  Symptoms: The following traceback is seen:

  ```
  %SYS-2-NOBLOCK: suspend with blocking disabled. -Process= "ESWPPM", ipl= 0, pid= 67^M
  ```

  Conditions: This issue occurs when CISP/NEAT auto-config code starts.

  Workaround: There is no workaround.

- 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

- CSCtt17785

  Symptoms: In the output of **show ip eigrp nei** *det*, a Cisco ASR router reports peer version for Cisco ASA devices as 0.0/0.0. Also, the Cisco ASR router does not learn any EIGRP routes redistributed on the Cisco ASA device.

  Conditions: This symptom is observed only when a Cisco ASR router is running on Cisco IOS Release 15.1(3)S and the Cisco ASA device is Cisco ASA Version 8.4(2).

  Workaround: Downgrade the Cisco ASR router to Cisco IOS Release 15.1(2)S.

- 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.

- CSCtt21681

  Symptoms: MAC learning stops once the supplicant is authorized to an auth-fail VLAN.

  Conditions: This symptom occurs in an MDA setup and when an auth-fail VLAN is configured on the port.

  Workaround: There is no workaround.

- CSCtt23038

  Symptoms: IOSD crashes while executing the “show flow monitor name monitor2” command after an RP downgrade on bay 0.

  Conditions: This symptom is observed during a Cisco ASR 1004 ISSU downgrade from MCPDEV to Cisco IOS XE Release 3.5.

  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.

- 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

- CSCtt28764

  Symptoms: Throughput and connection rate are degraded by 50 percent.

Conditions: This symptom is observed when static ip-sgt bindings are configured without ZBFW or IPsec configurations on Cisco ISR G2 routers.

Workaround: There is no workaround.

- CSCtt35936

  Symptoms: EIGRP route updates are not sent to DMVPN spokes. The **show ip eigrp inter** command output shows pending routes in interface Q, which remains constant. The **show ip eigrp int deta** command output shows that the next sequence number of the interface remains the same (does not advance).

  Conditions: This symptom occurs when EIGRP session flapped, resulting in routes being withdrawn and restored.

  Workaround: Add a static route on any spoke that kicks out EIGRP learned routes from the RIB table; this will again kick the interface on the HUB.

- CSCtt36513

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

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

  Workaround: There is no workaround.

- CSCtt43896

  Symptoms: Traffic is not flowing in the failed/running state when the port is in Open Access mode.

  Conditions: This symptom is observed when authorization fails or when in the running state and the port is open.

  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

- 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

- CSCtt98801

  Symptoms: Mobile router reports stale RRP received from HA.

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

  Workaround: There is no workaround.

- CSCtu06894

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

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

  Workaround: There is no workaround.

- 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
  ```

- CSCtu17006

  Symptoms: Mediatrace is not working because RSVP fails to select the output interface.

  Conditions: This symptom is observed only with PFR configuration.

  Workaround: Remove the PFR configuration.

- CSCtu17228

  Symptoms: DHCPv6 relay does not work on an EHWIC.

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

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

  Workaround: There is no workaround.

- CSCtu18712

  Symptoms: The MAB URL redirection feature does not work on Cisco ISR G2 platforms.

  Conditions: This symptom is observed when the URL redirect ACL is downloaded from ACS based on client credentials.

  Workaround: There is no workaround.

- CSCtu18786

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

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

  Workaround: There is no workaround.

- CSCtu28990

  Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.

  Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.

  Workaround: There is no workaround.

- CSCtu29107

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

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

  Workaround: There is no workaround.

- CSCtu36224

  Symptoms: A Cisco router reboots unexpectedly at intermittent intervals.

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

  Workaround: There is no workaround.

- CSCtu36321

  Symptoms: A voice session terminates abruptly when a data device is connected or disconnected behind a phone and the IAB feature is active.

  Conditions: The IAB feature is configured with “authentication event server dead action authorize voice” and:

  - RADIUS connectivity is down.
  - The voice device authenticates after RADIUS connectivity goes down.
  - The voice call is in progress.
  - The data device is connected/disconnected behind the phone.

  The connection/disconnection of the data device may cause the voice session to terminate.

  Workaround: There is no workaround. However, the call may be re-established immediately by the user.

- CSCtu41137

  Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.

  Conditions: The core is observed while doing unconfiguration.

  Workaround: There is no workaround.

- CSCtu43731

  Symptoms: On an RP1, RP switchover causes an RP reset.

  Conditions: This symptom is observed with RP switchover under the following conditions:

  - The router must be an RP1.
  - The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.

  An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.

  Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.

  Workaround 2: Do not enable FNF monitoring.

- 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: None.

  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

- CSCtv52031

  Symptoms: Router crashes while accessing the usergroup database.

  Conditions: The symptom is observed with performance testing.

  Workaround: There is no workaround.

- CSCtw45055

  Symptom: 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:

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

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

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

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

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

Workaround: There is no workaround.

- CSCtw45592

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

  Conditions: When the device is reloaded or when the DNS name is not resolved, the config is not added. After the standby SYNC failure, then issuing the “no ntp server <hostname>”.

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

- 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.

- CSCtw58586

  Symptoms: IKEv2 CLI configuration currently requires to manually link the crypto IKEv2 profile default to the crypto IPSec profile default. This enhancement request will change the behavior and create an automatic anchorage.

  Conditions: This symptom is seen in IKEv2 usage.

  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.

- CSCtw66262

  Symptoms: The “security-group” command is missing after the match filter while configuring a class map. The customer cannot use the CTS ZBFW feature.

  Conditions: This symptom is observed on the Cisco 890 platform.

  Workaround: There is no workaround.

- CSCtw67283

  Symptoms: A router receives either an “Illegal access to a low address” or an “Unexpected exception to CPU” crash depending on the platform. The crash occurs within several minutes of starting traffic.

  Conditions: The router is configured with NBAR2, FNF, and HQoS. While running a mix of HTTP, FTP, SMTP, and DNS traffic, the router crashes within several minutes of starting traffic. The crash has been seen on the Cisco 891, 1941, and 2901 (Cavium based), but has not been seen on the Cisco 2951, 3925, or 3945.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCtx29557

  Symptoms: A standby crashes @ fib_fib_src_interface_sb_init.

  Conditions: All.

  Workaround: There is no workaround.

- CSCtx37680

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

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

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

- 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 software.

  2) Uninstall the update.

  3) Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

  webvpn gateway gateway-name ssl encryption rc4-md5

  4) Use AC 2.5.3046 or 3.0.3054.

  5) Use older versions of Firefox (9.0.1).

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

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

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

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

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

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

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

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

- CSCtx44060

  Symptoms: Flexvpn spoke-to-spoke tunnels do not come up.

  Conditions: None.

  Workaround: Once tunnels fail to come up, clear the NHRP cache on one spoke alone.

- 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.

- CSCtx88093

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

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

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

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

- CSCtx90299

  Symptoms: The DMVPN IPsec sessions might get torn down and unable to re- establish themselves after experiencing link-flap events.

  Conditions: In a scaled DMVPN environment, when physical-port link-state up/down events happen, there will be stormed IPSec events to tear down and/or re-negotiate the sessions; it might run into a bad state that it cannot establish new sessions. Hence, when those active sessions expire (by time period or volume based), it can no longer be re-created. After some period of time, no more active session remains on the router.

  Workaround: Reload the router.

- CSCty03629

  Symptoms: Traffic from a client with a valid IP-SGT mapping is dropped by the firewall.

  Conditions: NAT is co-located with SGFWl.

  Workaround: There is no workaround.

- CSCty04384

  Symptoms: IMA-DSLAPP crashes when doing interoperability testing with third- party DSLAMs.

  Conditions: Change line rates on CO sides with various loop lengths.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(2)T

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

- CSCej11786

  Symptoms: A Cisco 2600 router reloads when a clear counter is performed on the router. This crash is reproducible only after making a number of calls first.

  Conditions: This symptom has been observed on a Cisco 2600 router.

  Workaround: There is no workaround.

- CSCtd63264

  Symptoms: A router may refuse configuration of certain VRF-aware translations (**ip nat outside source static network** *global- network local-network mask* **vrf** *name* **extendable match-in- vrf**) complaining that the translation already overlaps with an existing one, even though the configuration is valid and should be accepted.

  Conditions: The symptom is observed with certain VRF-aware translations.

  Workaround: There is no workaround.

- CSCtj59117

  Symptoms: The following error message is seen and the router freezes and crashes:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle
  ```
  A reload is required to recover.

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

  Workaround: Remove CEF.

- CSCtq29120

  Symptoms: Authenticated MAC address is found in the MAC table even after the port is shut down.

  Conditions: The symptom is observed after the port is shut down.

  Workaround: There is no workaround.

- CSCtq39602

  Symptoms: DMVPN tunnel is down with IPSec configured. The **show dmvpn** command from the spoke shows the state is IKE.

  Conditions: After heavy traffic was pumping from DMVPN hub to spoke for some time: from a few minutes to a couple of hours.

Workaround: Configuring “crypto ipsec security-association lifetime kilobytes disable” to disable volume-based rekeying will reduce the problem.

- CSCtq97723

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

  Conditions: This is seen with a steady bi-directional 64byte ICMP stream:

  - c3900-universalk9-mz.SPA.150-1.M2 image.
  - At 283Mbps = 37.16% wire rate of 1 gig overruns began to increment.

  Workaround: There is no workaround.

- CSCtr07508

  Symptoms: Unexpected reload after enabling WAAS on the interface.

  Conditions: The conditions have not been determined; router had just been reloaded, no traffic was flowing or special configuration done. Was seen several times in regression during a period of time, then ceased to happen in newer versions. Issue may be related with previous configuration on the router. It was not consistent.

  Workaround: There is no workaround.

- CSCtr44373

  Symptoms: This is a platform independent issue. Users cannot receive a call through a BRI port. A fast tone will be heard.

  Conditions: This symptom is observed on a newly released image.

  Workaround: Configure “forward digital all” in the CLI.

  The following example shows a sample configuration:

```
dial-peer voice 111 pots
 destination-pattern 111
 !direct-inward-dial
 port 2/0
 forward-digits all
```

- CSCtr63128

  Symptoms: A Cisco 2951 crashes with “Unexpected exception to CPU: vector 1400, PC = 0x55629DC , LR = 0x5562948” and following traceback:

```
-Traceback= 0x55629DCz 0x5977F74z 0x5584BC4z 0x5584134z 0x5507988z 0x5509DB8z
0x83D0DE8z 0x83D82C4z 0x67F14A8z 0x67F6EB8z 0x67F7150z 0x87ADE04z 0x87AD7DCz
0x87AFB00z 0x87B0830z 0x87B0910z
```

  Conditions: The symptom is observed with a Cisco 2951 router that is configured with IPSec/GRE tunnels with QoS and netflow configured. Not seen on the Cisco 3925 and Cisco 1921 which were tested with identical conditions.

  Crash seen when maximum multicast throughput is reached with the following traffic mix: packet size of 66, 256, 512, and 1024 bytes with a weight of 40, 30, 5 and 21 respectively.

  Issue not seen with the following traffic mix: packet size 66, 570,594, and 1420 bytes with a weight of 57, 7, 18 and 20.

  With the mix causing the crash, the maximum observed multicast throughput seen is 170 Mbps, 27.44 Mbps, and 42 Mbps for c3925, c2951, and c1951 respectively. This seems to indicate a multicast performance issue.

  Workaround: There is no workaround.

- CSCts46578

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

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

  Retransmitted packet is allowed through.

  Conditions: CBAC configured.

  Workaround: There is no workaround.

- CSCts68626

  Symptoms: PPPoE discovery packets causes packet drop.

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

  Workaround: There is no workaround.

- CSCts69534

  Symptoms: A Cisco 3800 router running voice debugs may crash with a bus error.

  Conditions: Voice debugs seem to be triggering the crashes.

  Workaround: There is no workaround.

- CSCts85251

  Symptoms: Router with GETVPN enabled may experience high CPU and memory exhaustion leading to a crash.

  Conditions: First seen on Cisco IOS Release 12.4(24)T5 but not exclusive to it.

  Workaround: There is no workaround.

- CSCtt11210

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

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

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

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

- CSCtt20719

  Symptoms: Incremental leaks at shdsl_efmEndpointCurrEntry_get and shdsl_efmInventoryEntry_get.

  Conditions: The symptom is observed with an SNMP walk on a Cisco 888E router and with a Cisco ISR-G2 with HWIC-2SHDSL-EFM.

  Workaround: There is no workaround.

- CSCtt21228

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

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

  Workaround: There is no workaround.

- CSCtt26721

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

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

  Workaround: There is no workaround.

- CSCtt28764

  Symptoms: Throughput and connection rate are degraded by 50%.

  Conditions: This symptom is seen when static ip-sgt bindings are configured on Cisco ISR G2 routers.

  Workaround: There is no workaround.

- CSCtt96462

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

  - NAT
  - VRF
  - IPSec

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

  Workaround: Disable CEF.

- 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.

- CSCtu11140

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

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

  Workaround: There is no workaround.

- CSCtu16433

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

  ```
  %GDOI-5-GM_REGS_COMPL: Registration to KS <snip> complete for group <snip> using
  address <snip>
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = <snip>
  ```

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

  Workaround: There is no workaround.

- CSCtu18634

  Symptoms: ISR G2 fails to relay specific T30 messages in the POTS->IP direction. This would be a dropped DCS/TCF for an inbound fax, or a dropped DIS/CFR for an outbound fax.

This will cause fax failure reproducible almost every time from/to specific sources where there is minimal dB loss in the PSTN. It is also commonly seen in PSTN hair-pinning scenarios.

Conditions: The symptom is observed with fax calls through a fax gateway configured for T.38 and running Cisco IOS Release 15.1(3)T2 or higher. The issue is seen when the input signal amplitude is too strong. It can be identified by obtaining a PCM capture and a packet capture and comparing the T30 data. The inbound stream of the PCM capture will show the T30 message, but the packet capture will not.

Workaround: Any one of the following workarounds apply:

- Applying BOTH an input gain of -6 dB and an output attenuation of 6 dB to the voice-port. Note that this will cause audio conversations through the circuit to be 6dB quieter in each direction as well.
- Downgrade to Cisco IOS Release 15.1(3)T1 or earlier.
- Convert to fax/modem passthrough.

- 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.

Resolved Caveats—Cisco IOS Release 15.2(2)T

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

- 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.

- CSCso41274

  Symptoms: A router crashes or shows the following traceback:

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

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

Example:

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

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

- CSCso46409

  Symptoms: mbrd_netio_isr and crypto_engine_hsp_hipri traceback log messages are produced.

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

  Workaround: There is no workaround.

- CSCsx64858

  Symptoms: A router may crash after the **show ip cef vrf** *VRF* **platform** command is issued.

  Conditions: This symptom occurs when BGP routes are learned via two equal paths within a VRF. If an update occurs so that only one path remains while the **show ip cef vrf** *VRF* **platform** command is issued, the router may crash.

  Workaround: There is no workaround.

- CSCsz79652

  Symptoms: A memory leak may be seen in Dead memory.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(50)SE and Release 12.2(50)SE1. Cisco IOS Release 12.2(44)SE is not affected. The symptom occurs when using Cisco Network Assistant to poll the device. The **ip http server** command or **ip http secure- server** command must be enabled for the leak to occur.

  Workaround: Disable the http server or stop CNA from polling the device.

- CSCsz97091

  Symptoms: Packet drop occurs when **show version**, **show run**, and **write memory** commands are issued.

  Conditions: Packet drop will be observed as input errors accounted as overruns. The rate of packets being dropped will be proportional to the rate of traffic.

  Workaround: There is no workaround.

- CSCta79941

  Symptoms: A virtual interface is not created when invoked using the **ip unnumbered** *type number* command.

  Conditions: This symptom is observed under a PPP interface when the virtual interface has been previously deleted.

  Workaround: Recreate the virtual interface manually using the **interface** command.

- CSCta93316

  Symptoms: Memory leaks are seen.

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

  Workaround: There is no workaround.

- CSCtb24819

  Symptoms: CLI view created cannot be deleted when user logs in and out. View deletion fails when user first sets into a view and then moves to another view or root view and tries to delete the previously set view.

  Conditions: This issue occurs when a view user telnets into the device and then switches to another view or to root view. This is seen consistently when a view is created and user logs in as a view user.

  Workaround: Log in as the root view user first and then delete the view.

  Further Problem Description: This issue only affects those view users who would log in as a view user and then tries to delete the view by changing itself to another view or the root view.

- CSCtb57180

  Symptoms: A router may crash with a software-forced crash.

  Conditions: Under certain conditions, multiple parallel executions of the **show users** command will cause the device to reload.

  Workaround: It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted devices to connect to the device via telnet, reverse telnet, and SSH.

  For more information on restricting traffic to VTYs, please consult:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml

  The following example permits access to VTYs from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from everywhere else:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit host 172.16.1.2
Router(config)# line vty 0 4
Router(config-line)# access-class 1 in
```

  For devices that act as a terminal server, to apply the access class to reverse telnet ports, the access list must be configured for the aux port and terminal lines as well:

```
Router(config)# line 1 <x>
Router(config-line)# access-class 1 in
```

  Different Cisco platforms support different numbers of terminal lines. Check your device's configuration to determine the correct number of terminal lines for your platform.

  Setting the access list for VTY access can help reduce the occurrences of the issue, but it cannot completely avoid the stale VTY access issue. Besides applying the access list, the following is also suggested:

  1. Avoid nested VTY access. For example, RouterA->RouterB->RouterA->RouterB.
  2. Avoid issuing the **clear vty** command or the **clear line** command when there is any nested VTY access.
  3. Avoid issuing the **clear vty** command or the **clear line** command when there are multiple VTY accesses from the same host.
  4. Avoid issuing the **clear vty** command or the **clear line** command when router CPU utilization is high.
  5. Avoid issuing the **show users** command repetitively in a short period of time.

  Again, the above can help reduce the occurrences of the issue, but it cannot completely avoid the issue.

- CSCtb69063

  Symptoms: Memory corruption occurs when a user name is configured to a maximum length of 64 characters, as shown:

  ```
  config# username <name of 64 characters> priv <0-15> password 0 <password>
  ```

  Conditions: The symptom is observed if the user name is exactly 64 characters.

  Workaround: Configure a user name of less than 63 characters.

  Further Problem Description: When some configurations are added, modified, or deleted the **show configuration id detail** command prints information of last change time, changed by user, and changed from process. If the user name is very large (exactly 64 characters), then the "changed by user" field prints unwanted characters.

- CSCtc78200

  Symptoms: A Cisco router may crash in the parse_configure_idb_extd_args routine.

  Conditions: This symptom is observed when running PPP sessions or when TCL is used for configuring interface range.

  Workaround: As PPP session is being established on the LNS, IOS will momentarily use one of the available VTYs from the router. After initial configuration is done, it is immediately released to the system pool.

  If all VTY connections are in use, then we will see an RP crash if a new PPP session is being established and there are no free VTYs in the system.

  To work around this issue, reserve several VTY connections for PPP session establishment. Since it is possible that a burst of PPP sessions tries to connect thereby using multiple VTY connections at the same time, it is recommended to reserve at least 5 VTY connections. One possible solution is to use an ACL on the last 5 VTY lines:

  ```
  ip access-list extended VTY_ACL
   deny   ip any any
  !
  line vty 5 9
   access-class VTY_ACL in
   exec-timeout 1 0
  ```

  Alternate Workaround: Do not configure "interface range" cli using ios_config from tclsh mode. When in tclsh mode, use normal "interface cli" in a "for loop".

- 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.

- 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.

- CSCtf70365

  Symptoms: When “config ED” is used for EEM with some special configurations (like virtual-template commands), it can trigger error messages.

  Conditions: The symptom is observed only when certain commands are configured.

  Workaround: Use “syslog ED”.

- CSCtg35257

  Symptoms: The message “previous instance of CNS Event Agent still executing” is seen even if a CNS event is not configured.

  Conditions: The symptom is observed if the **cns event <IP> encrypt** command is enabled and disabled.

  Workaround: There is no workaround.

- CSCth06812

  Symptoms: A Cisco ASR 1000 sees a hang followed by a crash.

  Conditions: This symptom is observed on a Cisco ASR 1000 with Cisco IOS Release 2.5.1. (XNE1) and the following configuration:

```
R1(config)#parser view SUPPORT
R1(config-view)# secret cisco
R1(config-view)# commands exec include ping
R1(config-view)# commands exec include configure terminal
R1(config-view)# commands exec include show ip ospf neighbor       <--Where
we see the hang
```

  Workaround: Do not configure “commands exec include show ip ospf neighbor” command in parser view configuration.

- CSCth07787

  Symptoms: A standby device crashes when attempting to configure login banner on the active device.

  Conditions: The symptom is observed only when configuring the banner manually, but not during bulk sync or any copy operations. In addition, this symptom is observed when using the following delimiters: -Cntrl-v + Cntrl-C -Shift-6 + Shift-C

  Workaround: Use any delimiters other than the following: -Cntrl-v + Cntrl-C -Shift-6 + Shift-C.

- CSCth11006

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

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

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

  Cisco has released free software updates that address these vulnerabilities. This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat

- CSCth80642

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

  Conditions: SSLVPN on IOS

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

- CSCth82293

  Symptoms: ISR-G2 router crashes due to bus error at PC 0x0 with spurious errors and the following message:

  ```
  %ALIGN-1-FATAL: Corrupted program counter
  ```

  Conditions: The symptom is observed with wrong usage of CNS initial and partial configurations mixed with **cns config retrieve** execution.

  Workaround: Avoid wrong CNS usage. Consult Cisco for correct CNS usage.

  Further Problem Description: Although the issue is seen with a Cisco 2911, it is not specific to the 2900 series alone. It can occur with any router platform.

- CSCth83508

  Symptoms: When performing an SRE install over WSMA, the router crashes and reboots.

  Conditions: The problem is seen when using WSMA to run the **session install** command.

  Workaround: Perform the install manually from a VTY session.

- 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.

- CSCti24577

  Symptoms: System crashes on active or hangs on standby.

  Conditions: The symptom is observed when a banner command is in the configuration.

  Workaround: Remove all banner commands.

- 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.

- CSCti66155

  Symptoms: A Cisco IPSec router may unexpectedly reload due to bus error or software-forced crash because of memory corruption or STACKLOW error.

Conditions: This is seen when the WAN link goes down and causes recursion between multiple tunnels using tunnel protection. (That is, there are tunnel 0 and tunnel 1. After the WAN link goes down, the routing table shows a link to the tunnel 0 destination through tunnel 1 and the tunnel 1 destination is through tunnel 0.)

Workaround 1: Change the tunnel source to be the physical WAN interface so that when the WAN link does go down, the tunnels are brought down immediately.

Workaround 2: Change the routing protocol so that the router in question does not have recursive routing when the link goes down.

Workaround 3: If possible, create a floating null route for the tunnel destinations that is less preferred than the route normal route to the tunnel destination, but more preferred than the route that gets installed after the WAN link goes down.

- CSCti67832

  Symptoms: Cisco 3900e platform router reloads while try to enable GETVPN Group Member (GM) all-features debugs.

  Conditions: The symptom is observed on a Cisco 3900e router that is running Cisco IOS interim Release 15.1(2.7)T and while trying to enable the debug **debug crypto gdoi gm all-features**.

  Workaround: There is no workaround.

- CSCti68721

  Symptoms: The output of **show performance monitor history interval** <*all* | *given #*> will appear to have an extra column part way through the output.

  Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

  Workaround: If the symptom occurs, repeat the command.

- CSCti92798

  Symptoms: A Cisco router crashes while configuring http commands with ATM.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(2)T.

  Workaround: There is no workaround.

- CSCtj05903

  Symptoms: Some virtual access interfaces are not created for VT, on reload.

  Conditions: This symptom occurs on scaled sessions.

  Workaround: There is no workaround.

- CSCtj06390

  Symptom: Ping fails after configuring crypto.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(2.18)T.

  Workaround: There is no workaround.

- CSCtj10592

  Symptoms: DVTI GRE IPv4 mode fails to create virtual-access for IKEv2 connections.

  Conditions: The symptom is observed with a simple SVTI to DVTI connection.

  Workaround: There is no workaround.

- CSCtj21237

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

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

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

- CSCtj38234

  Symptoms: IPSec IKEv2 does not respond to INVALID_SPI informational message. It should respond with another INFORMATIONAL IKE message.

  An INVALID_SPI may be sent in an IKE INFORMATIONAL exchange when a node receives an ESP or AH packet with an invalid SPI. The notification data contains the SPI of the invalid packet. The INVALID_SPI message is received within a valid IKE_SA context.

  Conditions: The symptom is observed when an IKEv2 peer sends an INFORMATIONAL IKE message notifying about an INVALID_SPI (IPSec).

  Workaround: There is no workaround.

- 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.

- CSCtj69212

  Symptoms: High level of memory usage due to “MAB Framework” process.

  Conditions: This issue is seen on Cisco Catalyst 3750 switches running Cisco IOS Release 12.2(55)SE when MAB fails on the port and subsequent attempts are made to authorize the device after the restart timer expires.

  Workaround: Unconfigure the following from the switch:

  ```
  aaa accounting send stop-record authentication failure
  ```

- CSCtj76297

  Symptoms: Router hangs with interoperability of VM and crypto configurations.

  Conditions: The symptoms are seen only during interoperability between video-monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

  Workaround: Disable AIM and use onboard CE.

- 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.

- CSCtj79368

  Symptoms: All keyservers crash after removing RSA keys before changing to new ones based on security concerns.

  Conditions: The symptom is observed when removing RSA keys.

  Workaround: Stay on the same RSA keys.

- CSCtj95685

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

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

  Workaround: There is no workaround.

- 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.

- CSCtk15360

  Symptoms: xauth userid mode http-intercept does not prompt for a password and the Ezvpn session does not come up.

  Conditions: This symptom occurs when the EzVPN client, x-auth is configured as http-intercept.

  Workaround: There is no workaround.

- CSCtk18404

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

  Conditions: The symptom is observed with the following conditions:

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

  Workaround: There is no workaround.

- CSCtk59012

  Symptoms: After PRE switchover, the new standby PRE goes in “progress to standby cold-bulk” state and is then periodically reset by the new active PRE.

  Conditions: This issue is observed when a Cisco uBR10K is configured with 300k routes and a PRE switchover occurs.

  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.

- CSCtk98248

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

  Conditions: The symptom is observed with the only FA8 port.

  Workaround: Set the FA8 to auto negotiation.

- CSCtl01141

  Symptoms: cswmMvrfStatsTable does not get populated.

  Conditions: This symptom occurs when the multicast vrf instance is configured on any switch running mtrose image and mibwalk is configured on cswmMvrfStatsTable.

  Workaround: There is no workaround.

- CSCtl20993

  Symptoms: Router crashes during IPsec rekey.

  Conditions: The conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtl23748

  Symptoms: EoMPLS over GRE (DMVPN) with IPSec protection is not working after a reboot.

  Conditions: The symptom is observed when there is a tunnel (Ethernet over MPLS over GRE over IPSec) between PE1 and PE2 and following a reload and when tunnel protection is configured.

  Workaround: There is no workaround.

- CSCtl48297

  Symptoms: Configure BGP dynamic neighbor in IPv4 VRF address-family. Deconfiguring BGP by using the **no router bgp** command will crash the system.

  Conditions: This symptom occurs because BGP dynamic neighbor feature currently is not supported but is allowed to be entered in CLI.

  Workaround: Do not configure BGP dynamic neighbor in VRF address-family.

- CSCtl49844

  Symptoms: Carrier delay configured under interface fails.

  Conditions: The symptom is observed when the cable is detached.

  Workaround: There is no workaround.

- CSCtl50815

  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

  ```
  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
  Non-OER, OOP Reason <reason>
  ```

  Conditions: The symptom is observed under the following conditions:

  - Use ECMP.
  - Use **mode monitor passive**.

  Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl52854

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

  Conditions: 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.

- CSCtl54975

  Symptoms: A small number of Cisco 1812 routers have been observed to unexpectedly restart due to software-forced crashes, repeatedly.

  Conditions: Unknown.

  Workaround: While the root cause is being investigated, units that are experiencing this problem should be replaced. Please replace the Cisco 1812 and send the unit for Failure Analysis, after contacting the Cisco TAC and referencing this bug ID.

- CSCtl55502

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

  Conditions: The symptom is observed when a parser command uses a pipe option in an HTTP URL (e.g.: http://<ipadd>/level/15/exec/show/runn/|/i/http/CR).

  Workaround: There is no workaround.

- 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.

- CSCtl76050

  Symptom: Traceback is observed.

  Conditions: This symptom is seen while defaulting the call-home profile .

  Workaround: There is no workaround.

- CSCtl76209

  Symptoms: Standby reloads when dampening is configured.

  Conditions: This symptom occurs when dampening is configuring parameters that are within the allowed range but the leading maximum penalty is bigger than the allowed maximum (20000). The RP and standby get out of sync. The command is accepted on active RP first, and standby also accepts it. However, then on active and standby, dampening gets turned off because later it is realized that maximum penalty is higher than 20000. When dampening gets configured again at this point, standby may turn dampening off while the active has it enabled, which will lead to configuration mismatch between active and standby, and standby will reload.

  This can be seen with all address families.

Workaround: There is no workaround.

- CSCtl82255

  Symptom: The following is seen on the UUT when the peering IPv6 router does a session reset.

```
ios72ta2-1#show bgp ipv6 unicast summary
BGP router identifier 10.0.0.0, local AS number 1
BGP table version is 34, main routing table version 34
>>> ....

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
2011::1001      4            1      22      27       32    0    0
00:19:44        0
>>>>>>> Table version is different from the main table version ....
```

  Conditions: This symptom occurs when the peering IPv6 router does a session reset then the “show bgp ipv6 unicast summary” does not get to a state where the main table version matches the peers table version. There is no prefix left behind unadvertised.

  Workaround: Hard clear the router that shows mismatch in table version.

- CSCtl87463

  Symptoms: Queue length becomes negative.

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

  Workaround: There is no workaround.

- 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
```

  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)
```

  Workaround: There is no workaround.

- CSCtl95666

  Symptoms: Data path fails after SSO.

  Conditions: This symptom is seen when connection segments are down in standby for auto-provisioned VCs.

  Workaround: There is no workaround.

- 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.

- 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 OS 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.

- CSCtn04716

  Symptoms: Upon switchover, standby reloads continuously because of configuration sync failures for OSPF area commands under non-base topologies.

  Conditions: This symptom occurs under the following steps:

  1. An area X needs to be first configured under base topology.
  2. One or more area commands under non-base topology should be configured for area X.
  3. All area commands for area X under base topology are removed such that the command(s) under non-base topologies are the only ones that remain. Note that this cannot be achieved for **area X stub**, **area X nssa**, and **area X virtual-link** commands as removal of these commands under base topology will result in removal of corresponding commands under non-base topologies as well.
  4. Execute switchover.

  Workaround: Remove the commands under non-base topologies before switchover.

- 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.

- CSCtn22728

  Symptoms: See the following:

```
Router(config)#monitor session 1 type erspan-source
Router(config-mon-erspan-src)#destination ?
  <cr>

Router(config-mon-erspan-src)#destination int g11/48
Router(config-if)#
Config Sync: Line-by-Line sync verifying failure on
command:
  destination int g11/48
due to parser return error
```

  Conditions: This symptom is seen when using unsupported interface CLI option with destination keyword in ERSPAN source session configuration, which may result in Config-Sync failure between Active and Standby-RP, therefore reloading Standby-RP.

  Workaround: Do not issue not applicable commands.

- 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.

- CSCtn24305

  Symptoms: The software version in call home messages has a trailing comma for the released images. This causes a backend processing failure when the software version is needed.

  Conditions: All call home messages from released images have this issue.

  Workaround: Backend can check to remove this trailing comma, if present.

- CSCtn26750

  Symptoms: The standby RP reloads due to a config-sync error.

  Conditions: The symptom is observed when “authentication” or “encryption” is configured for an OSPFv3 virtual link. Then it is changed to use a different SPI, but IPSec fails to remove the policy for the old SPI. When it is changed back to the old SPI, the command fails with the error:

  ```
  %OSPFv3-3-IPSEC_POLICY_ALREADY_EXIST: SPI is already in use with ospf process
  ```

  On the active RP the “virtual-link ipsec” configuration is removed, but on the standby RP it remains. Reconfigure “virtual-link ipsec” using the second SPI. This command succeeds on the active RP so it is synched to the standby, however the command already exists on the standby so it generates the config- sync error and reloads.

  Workaround: Instead of simply changing the SPI from X to Y, remove X using a **no** command and then configure Y.

- CSCtn32323

  Symptoms: 802.1p information is not set on local generated traffic when bridge-dot1q is used on the DSL lines.

  Conditions: Configure the device to transport 802.1p information over a DSL link connection, considering different CoS values for LAN and local generated traffic on the router.

  ```
  interface ATM0.y point-to-point
   bridge-group <x>
   pvc 1/199
    bridge-dot1q encap <vlan>
    service-policy out <egress-policy>
  ```

  Workaround: There is no workaround.

- CSCtn39339

  Symptoms: Data path fails with Hot-Standby Psuedo Wire (HSPW) configurations after a switchover.

  Conditions: The symptom is observed when a switchover occurs with the backup pseudowire up and the primary pseudowire down.

  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.

- 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.

- CSCtn40571

  Symptoms: Issuing the **crypto pki server** *name* **rollover cancel** command can result in multiple rollover certificates installed on Sub-CA router.

  Conditions: This symptom is seen when the rollover certificate is already installed.

  Workaround:

  - Copy startup-configuration from router.
  - Remove the older rollover certificate from configuration under the **crypto pki cert chain** *ca* command.
  - Copy the new configuration back to startup-configuration and reload the router.

- CSCtn42588

  Symptoms: After seeing OSPF neighbors flap quickly one of the neighbors does not properly install routes that should be learned via OSPF. The routes may appear in the OSPF LSDB.

  Conditions: The symptom is observed when “timers throttle spf” or “timers throttle lsa” is configured.

  Workaround: Use default SPF or LSA timers or ensure your LSA timers are smaller than the SPF timers.

- CSCtn43589

  Symptoms: A crash is observed at process_run_degraded_or_crash.

  Conditions: The symptom is observed when SNMP bulkstat has been configured for periodic MIB collection.

  Workaround: There is no workaround.

- CSCtn56097

  Symptoms: Auto mpls-lsp-monitor for pathecho fails.

  Conditions: Auto mpls-lsp-monitor feature does not work due to internal scheduling error.

  Workaround: There is no workaround.

- CSCtn58005

  Symptoms: The prefix-list does not filter local routes configured in the L1-L2 domain.

  Conditions: The symptom is observed on a router running IPv6 ISIS L1-L2 domain and when L1 routes are redistributed into L2 routes.

  Workaround: There is no workaround.

- CSCtn58128

  Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

Conditions: The issue may be triggered by route-flaps in scaled scenario where the route reflector may have 4000 route reflector clients and processing one million+ routes.

Workaround: Ensure “no logging console” is configured.

- CSCtn59075

  Symptoms: A router may crash.

  Conditions: This has been experienced on a Cisco router that is running Cisco IOS Release 15.1(3)T, 15.1(3)T1, and 15.1(4)M. Flexible Netflow needs to be running.

  Workaround: There is no workaround.

- 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 multlink and traffic flows across the multilink.

  Workaround: There is no workaround.

- CSCtn65116

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

  Conditions: The symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Release 12.2(33)SRB and later. Earlier versions are not affected.

  Workaround: Advertise and withdraw or withdraw and re-advertise a more specific prefix. That will force the re-evaluation of the prefix not being imported, for import again.

- CSCtn67577

  Symptoms: SIP-400 crashes while modifying the cell-packing values.

  Conditions: This symptom occurs when cell-packing values are modified at PE2 side.

  Workaround: There is no workaround.

- CSCtn68117

  Symptoms: Session command does not work on Cisco C3K series routers that have become the master after a mastership change.

  Conditions: This symptom is seen when fail-over to slave occurs.

  Workaround: There is no workaround.

- CSCtn70367

  Symptoms: IPSEC key engine crashes at sessions setup.

  Conditions: This symtpom 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.

- CSCtn72925

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

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

Workaround: Use the following command:

clear pfr master *.

- CSCtn88247

  Symptoms: The command **no ip address** is not NVgened on the interface if the switchport configuration is removed from the interface after a reload.

  Conditions: The symptom is observed if you reload the router having one or more interfaces configured with swtichport and you then remove the configuration after the reload.

  Workaround: There is no workaround.

- CSCtn97267

  Symptoms: There is a router crash in the URLF code using Websense.

  Conditions: The symptom is observed on a Cisco ISR G2 during normal operation. It is caused by long URLs overwriting the end of a fixed length buffer.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCto10485

  Symptoms: With a GRE over IPSec configuration using tunnel protection, traffic originated from the router may be dropped on the receiving router due to replay check failures. This is evident by the %CRYPUO-4-PKT-REPLAY drops as shown in the syslog.

  Conditions: This issue typically occurs during high traffic load conditions.

  Workaround: There is no workaround.

- CSCto11238

  Symptoms: OSPF cannot be enabled on a tunnel interface by using either the network statement under OSPF or by enabling OSPF directly under the interface.

  ```
  Router#show ip osp neighbor  tunXXX
  %OSPF: OSPF not enabled on TunnelXXX
  ```

  Conditions: This symptom is observed in both Cisco IOS Release 15.1S and Cisco IOS Release 15.1T IOS software trains. The problem is triggered by configuring either WCCP, L3VPN, or mGRE. A tunnel configured with any of these will have dynamic routing disabled on it. If this is then deleted, the idb is reused by a new tunnel created via the CLI. This newly created tunnel will still have dynamic routing disabled on it and therefore ospf cannot run on it.

  Workaround: Once the problem has occurred, the only way to recover is to reload the router. If WCCP, L3VPN, or mGRE are never configured, the issue will not be seen.

- CSCto13338

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

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

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

  Workaround 2: Use consultative transfer instead of blind transfer.

- CSCto15361

  Symptoms: MF: Active Supervisor crashes after removing the "router eigrp" configuration.

  Conditions: This symptom occurs when the Active Supervisor crashes while disabling the Ipv6 router eigrp because the EIGRP Hello process gets killed. This issue occurs because the EIGRP Hello process calculates the size of the packet. After investigation, it was found that this is purely a timing-based issue. During cleanup, which is done by the EIGRP PDM process, the peer list is cleaned up first, and then an attempt is made to kill the Hello process. In case the peer list is cleaned up, and then the Hello process tries to calculate the size of a particular peer, then it finds the peer as NULL and crashes.

  Workaround: Modify the igrp2_procinfo_free function to kill the EIGRP Hello process prior to cleaning up the peer list.

- CSCto16196

  Symptoms: Performing a **no wccp version2** on the WAAS device connected to the WAN link and then reconfiguring **wccp version 2** results in tracebacks on a Cisco ASR 1000 router configured with WCCP. Traffic loss is also observed.

  Conditions: This symptom is observed when WCCP is configured on a Cisco ASR 1000 router and the WCCP tunnels are up before **wccp version 2** is removed and reapplied on the WAAS devices.

  Workaround: There is no workaround.

- CSCto31255

  Symptoms: Router crashes at fair-enqueue.

  Conditions: The symptom may be seen on Cisco 5400 and 7200 platforms.

  Workaround: There is no workaround.

- CSCto34844

  Symptoms: The Cisco 891 may perform lower than the older generation Cisco 1812 platform.

  Conditions: This symptom occurs when Ethernet traffic using the VLAN tag is encapsulated inside the L2TPv3 tunnel.

  Workaround: There is no workaround.

- CSCto39885

  Symptoms: A router crashes.

  Conditions: gcid and callmon is turned on.

  Workaround: There is no workaround.

- CSCto41215

  Symptoms: DHCP server tries to assign a conflicted address to a client when “remembered binding” is configured.

Conditions: The symptom is observed when the *remember* keyword is configured in the server pool and the address that the server is going to assign is already assigned to another client.

Workaround: Ensure each client in the network is configured or gets a unique IP address.

- 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.

- CSCto48060

  Symptoms: A Cisco 3900 series router may crash with the following error:

  Unexpected exception to CPU: vector 1400

  Conditions: The symptom is observed when the router is configured as a voice gateway using H323 and H245 and connected to CUCM. If CUCM is sending a MultiMediaSystemControl messages with no entry, the router may crash.

  Workaround: There is no workaround.

- CSCto55606

  Symptoms: When same remote unicast neighbor is configured and received on different interfaces, the two neighbors keep flapping.

  Conditions: This symptom is seen when the same EIGRP neighbor is coming up on different interfaces.

  Workaround: This may not be a recommended configuration since having the same neighbor on different interfaces is not allowed in classic mode. This option is provided only for certain migration scenarios.

- CSCto60216

  Symptoms: Cisco IOS crashes in ospfv3_write.

  Conditions: This symptom occurs when the **issu runversion** command is entered multiple times within a short period of time.

  Workaround: Wait for the newly active router processor to completely initialize.

- CSCto61485

  Symptoms: High CPU utilization is seen after session disconnect.

  Conditions: This symptom is observed with scaling test cases with 10K to 24K sessions.

  Workaround: There is no workaround.

- CSCto61736

  Symptoms:

  1. NBAR remains enabled in CEF path.
  2. Packet counters not incrementing in “show adjacency lisp0 detail”.
  3. ADQ/PD not working on ATM-subinterface and frame-relay subinterfaces.
  4. **ip nbar port-map** CLI is broken.

  Conditions:

  1. The symptoms 1 and 2 are observed when NBAR is enabled and disabled on the interface.

2. Symptoms 3 and 4 are seen when the configuration/show CLIs are executed.

Workaround: There is no workaround.

- CSCto63268

  Symptoms: A Cisco 3900e router may crash while configuring a PRI-group on a VWIC2 in a native HWIC slot.

  Conditions: The router must be a Cisco 3900e and the number of timeslots in the new PRI-group must be greater than the number of available DSPs. Additionally, a EVM-HD-8FXS/DID must be installed and the onboard DSPs must be configured for DSP sharing.

  Workaround: Remove the EVM or disable DSP sharing.

- CSCto76700

  Symptoms: Multihop BFD session goes down with TE-FRR cutover.

  Conditions: The symptom may be observed with single hop, VCCV BFD and multihop BFD sessions. But after the TE-FRR cutover, the VCCV BF session comes back up whereas multihop BFD session goes down.

  Workaround: The workaround is to perform a “no shut” the port-channel interface.

- CSCto76888

  Symptoms: G.729 payload issue on a Cisco 2800. A PSTN user calls up on a specific number which is directed to the IVR response via the Cisco 2800 gateway router, but the PSTN user cannot hear anything due to the codec payload mismatch.

  Conditions: The symptom is observed with a first preference of the Codec G.729ab which is sent to a Cisco 2851 for an IVR announcement.

  Workaround: Change the preference of the Codecs to have G.729a as the preferred Codec from MGX.

- 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.

- CSCto81701

  Symptoms: The PfR MC and BR sessions flap.

  Conditions: The symptom is observed with a scale of more than 800 learned TCs.

  Workaround: Use the following configuration:

  ```
  pfr master keepalive 1000
  ```

- CSCto81916

  Symptoms: Voice gateway crashes due to insufficient free memory.

  Conditions: The symptom is observed when the copy feature is used in a voice class SIP profile similar to the example below:

  ```
  voice class sip-profiles 500
   request INVITE peer-header sip Remote-Party-ID copy ":(.*)@" u01
   request INVITE sip-header From modify "From: \"anonymous\" <(.*):(.*)
  @" "From: \"\u01\" <\1:\u01@"
  ```

!
In this case, a memory leak occurs and depletes all the free memory causing the router to crash.

Workaround: There is no workaround.

- CSCto85479

  Symptoms: Spanning Tree Protocol (STP) failure on EHWIC-4ESG.

  Conditions: The symptom is observed on a Cisco 3945 chassis that is running the c3900-universalk9-mz.SPA.151-4.M.bin image. Interfaces gi0/3/0-1 are on EHWIC-4ESG card.

  Workaround: There is no workaround.

- CSCto85731

  Symptoms: Crash seen at the nhrp_cache_info_disseminate_internal function while verifying the traffic through FlexVPN spoke-to-spoke channel.

  Conditions: The symptom is observed under the following conditions:

  1. Configure hub and spokes (flexvpn-nhrp-auto connect) as given in the enclosure.
  2. Initiate the ICMP traffic through spoke-to-spoke channel between spoke devices.
  3. Do a **clear crypto session** at Spoke1.
  4. Repeat steps 2 and 3 a couple of times.

  Workaround: There is no workaround.

  Further Problem Description: In the given conditions, one of the spoke device crashed while sending ICMP traffic (10 packets) through FlexVPN spoke-to- spoke channel. The crash decode points to “nhrp_cache_info_disseminate_internal” function

- 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.

- 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.

- CSCto92529

  Symptoms: Unable to configure "ipv6 ospf authentication ipsec spi 7000 md5 <>".

  Conditions: The symptom is seen on Cisco routers loaded with Cisco IOS interim Release 15.2(2.11)T.

  Workaround: There is no workaround.

- CSCto96750

  Symptoms: The **shutdown** command does not show up in the active running-config.

  Conditions: The following steps recreate the issue:

  1. Administratively shutdown a interface.
  2. Make this interface as the backup for another interface.
  3. Running-config of backup interface in the active does not sych up with standby running-config in SSO mode.

  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.

- CSCtq05004

  Symptoms: A dialer loses its IP address sporadically. The **show interface atm x** will record output drops during the issue. ATM0 is up, line protocol is up:

  ```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
  31956 << Incrementing during the issue
  ```

  The **show interface queueing atm0.1** (hidden command) will show as follows:

  ```
  Interface ATM0 VC 8/35
  Queueing strategy: fifo
  Output queue 40/40, 31956 drops per VC << Incrementing during the issue
  ```

  During the issue, if "debug ppp negotiation" is on, we will see the following:

  ```
  PPP: Missed 5 keepalives, taking LCP down
  PPP DISC: Missed too many keepalives
  ```

  There will be no ATM (physical interface) flap in this case (during the issue).

  A shut/no shut on the ATM interface does not help.

  Conditions: No conditions so far. The behavior is sporadic.

  Workaround: Reload.

- CSCtq06105

  Symptoms: In an MPLS FRR setup, after shut and unshut of the primary interface, traffic continues to flow along the backup interface, which is wrong. Traffic should flow along the primary path once the primary path is restored.

  Conditions: This symptom occurs with a MPLS FRR setup. The primary interface should be shut and unshut to see the issue.

Workaround: Shut and unshut the backup interface. This will make traffic flow along the primary path again, and also get the backup path in ready state

- 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.

- 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.

- CSCtq21785

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(2)S may crash upon performing a CRL check on an invalid certificate.

  Conditions: The conditions are unknown.

  Workaround: Turning off CRL check should stop the crash. It should be configured as: "revocation-check none"

  This will stop the CRL check of the peer certificate but should not be a long term solution.

- 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.

- CSCtq24614

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

  Conditions: The symptom is observed with an ATM SPA.

  Workaround: There is no workaround.

- CSCtq24733

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

  Conditions: The symptom is observed with MRCP is enabled.

  Workaround: There is no workaround.

- CSCtq26863

  Symptoms: After issuing a **shutdown** command on a port or unplugging the port, **show authentication session interface fax/x** will in some occasions show that the session informartion persists.

This can cause issues if the port was previously authenticated to the auth critical or guest VLAN, as the switch will retain this session information when the port is restarted and will ignore EAPoL requests sent by the dot1x supplicant.

Conditions: Issue has been observed under the following circumstances:

- Cisco IOS Release 12.2(33)SXI6 (same environment did not see the issue under an earlier code).
- Multidomain authentication configured.
- Issue intermittently reproducible when many ports are brought online at the same time.

The issue is due to a race condition under heavy load with multiple MAC addresses being presented to dot1x and Auth Manager framework at the same time. This problem is not present with default (single) hostmode.

The issue can only occur if multiple authentication methods are configured on the port, so just dot1x configured on a port will not trigger the problem, it has to be, for example, dot1x and MAB.

The issue cannot occur if dot1x is not configured on a port(e.g.: for just MAB).

Workaround: Issue **dot1x re-authenticate interface** *interface* on the affected ports.

- 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.

- CSCtq33932

  Symptoms: Unable to configure a command under the ATM subinterface.

  Conditions: The symptom is observed when you delete an ATM subinterface and re-create the same. Unable to configure commands under this ATM subinterface.

  Workaround: Create an ATM subinterface with a ID different to that of the one deleted earlier.

- 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

- 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.

- CSCtq37579

  Symptoms: Enabling and disabling “snmp-server traps” crash the UUT.

  Conditions: The symptom is observed when you disable the snmp-server and do a **write memory**.

  Workaround: There is no workaround.

- CSCtq39406

  Symptoms: When you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM, the module shuts down after 2 minutes. Then, all IP connectivity and console connectivity to the router is lost.

  Conditions: This symptom occurs when you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM.

  Workaround: Remove the HWIC-3G-HSPA. When you remove the 3G module from the system, energywise works as expected. You can shut down power modules using the above configuration. As soon as the 3G card is installed in slot 2 or 3 and the energywise level is set to zero, the service module shuts down and the entire router crashes. It has no IP connectivity and the console is inactive. The only workaround is a hard reset (along with removal of the card).

- 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

- CSCtq47856

  Symptoms: The following issues are observed:

  1. Crypto map is configured with a local ACL at registration time.
  2. Local ACL is removed from global configuration (without removing it from the crypto map configuration).
  3. Remove crypto map from the interface.

Issue 1: At this point **show crypto gdoi** continues to display the TEK SA, even though the GM has no interfaces configured with a crypto map.

4. Re-apply the crypto map to the interface and let registration complete.

Issue 2: If **crypto gdoi ks rekey** is issued on the keyserver, then **show crypto gdo** continues to display only the old TEK. New TEKs installed by subsequent rekeys are not displayed.

5. On the keyserver, issue **crypto gdoi ks rekey replace**.

Issue 3: GM crashes in the IPSec code while processing the new SAs and shortening the old ones.

Conditions: The symptom is observed on a router that is running GET VPN.

Workaround: Remove the ACL from the crypto map configuration before removing it from the global configuration.

- CSCtq49325

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

  Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

  Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.

  Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However if a particular path is threaded to be sent, in this case it is scheduled for a reply message, the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths from sending before deletion. A similar condition will occur if the packtization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq49860

  Symptoms: If an ISM VPN module is installed in the Cisco ISR G2 platform, export limits will be exceeded without an HSECk9 license installed.

  Conditions: The symptom is observed with an ISM VPN module installed and enabled for crypto acceleration.

  Workaround: There is no workaround.

- CSCtq52655

  Symptoms: Unable to route packets through the router, specifically when testing ICMP traffic.

  Conditions: This happens when using the VMI in aggregate mode. It only appears to occur with IPv6.

  Workaround: Turn off IPv6 CEF.

- CSCtq55173

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

  Conditions: The crash is triggered when the **clear ip nat translation ***, **clear ip nat translation forced**, or **clear crypto ipsec client ezvpn** command is entered.

  Workaround: There is no workaround.

- CSCtq56948

  Symptoms: The default route attribute is used by features like uRPF and if it is missed out, it may cause uRPF to allow packets whose source addresses match against the default route.

  Conditions: This symptom occurs because some prefixes in the FIB are sourced by non-RIB features, such as CTS, or are used to represent next hops for recursive paths. Such prefixes inherit the forwarding information from their covers, but the default route attribute is not inherited.

  Workaround: There is no workaround.

- 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.

- 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 specififed.

  Workaround: Specify a URL.

- CSCtq62322

  Symptoms: On an SNR call, when the call is forward and connected to CUE after ringing to the remote target, nothing happens (for example, no CUE prompt occurs, and the user cannot leave voice mail).

  Conditions: This symptom is observed if the answer-too-soon timer is configured, the remote target is a pstn call, and the calling party is using a sccp phone.

  Workaround: There is no workaround.

- CSCtq62759

  Symptoms: CLNS routing table is not updated when LAN interface with CLNS router isis configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when isis ages out the stale routes.

  Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

  Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq63225

  Symptoms: Packet drop seen when running traffic.

  Conditions: The symptom is observed when IPSec along with QoS is configured.

  Workaround: There is no workaround.

- CSCtq63838

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

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

  Conditions: This symptom is observed with the DSMP process.

  Workaround: There is no workaround.

- CSCtq64034

  Symptoms: NAT does not send gratuitous ARP for a translated address when an interface comes up.

  Conditions: The symptom is observed when an alias (translated address) is created with the interface (whose IP address is in the same subnet as the alias entry) is in shut down state.

  Workaround: Perform an admin shut/no shut on the interface with an IP address in the same subnet as the alias entry.

- CSCtq67750

  Symptoms: In relation to caveat CSCtn52350, before-after is on without it having been turned on.

  Conditions: The symptom is observed when the following CLI is configured:

```
archive
 log config
  logging persistency
```

  Workaround: Remove “logging persistency” from the configuration:

```
archive
 log config
  no logging persistency
```

- 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.

- CSCtq71011

  Symptoms: The router crashes, or in some cases a traceback is seen.

  Conditions: This symptom is seen when IPv6 routes with diverse paths are enabled.

  Workaround: There is no workaround.

- 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 SS towers by applying an ACL in the content-scan configuration.

- CSCtq72873

  Symptoms: A crash is caused when a MAB client fails to authenticate and is simultaneously deleted from the switch. This caveat has only been seen on the Cisco Catalyst 6k switch, but it potentially also affects the Cisco Catalyst 3k and 4k families.

  Conditions: The switch port must be configured for MAB. A MAB client must connect and then simultaneously it must be deleted and fail authentication. This is a race condition and so this bug is rarely seen.

  The failure of authentication could be caused by the ACS server rejecting the MAB request or the ACS server being unavailable. The deletion of the MAB client on the switch can be caused by shutting down the MAB enabled interface or issuing the **clear authentication sessions** CLI.

  Workaround: There is no workaround for this issue other than disabling MAB on the interface. However for the crash to happen the MAB client must be deleted from the switch. Avoiding shutting down the MAB-enabled interface and avoiding any CLI that clears the MAB session, will reduce the risk of the switch crashing.

- 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.

- 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.

- CSCtq76005

  Symptoms: Configuring “atm route-brige ip” on an MPLS-enabled ATM interface makes router punt all incoming MPLS packets to CPU.

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

  Workaround: Remove RBE.

- 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.

- CSCtq77274

  Symptoms: FXS phones are not recognized as SCCP endpoints.

  Conditions: This symptom occurs when FXS phones are configured as SCCP endpoints.

  Workaround: There is no workaround.

- CSCtq77363

  Symptoms: License images are not working properly.

  Conditions: This symptom is seen when the license image is loaded. There is a traceback due to access of uninitialized variables.

  Workaround: There are no workarounds.

- CSCtq78217

  Symptoms: A router crashes with the following information:

  ```
  System returned to ROM by address error at PC 0xZZZZZZZZ, address 0xZZZZZZZZ
  ```

  Conditions: The symptom is observed with CUBE + SIP.

  Workaround: There is no workaround.

- CSCtq79382

  Symptoms: In the HA setup and on the Active, if you have a probe configured with VRF and you remove the VRF with **no ip vrf** *vrfname* and reboot, it keeps rebooting again and again (crashes).

  Conditions: The symptom is observed when removing the VRF and rebooting the Active terminal.

  Workaround: Check that the system is in standby and that there is no VRF configured. Even though there is a probe configured with VRF, you can proceed without crashing the Active after a reboot.

- CSCtq80477

  Symptoms: Invalid input detector with “no interface serial multipoint” interface.

  Conditions: CSCto98742 fix was causing the chain breakage in the “no” form of the CLI.

  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.

- 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.

- 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.

- CSCtq84635

  Symptoms: Trunk DNs can act as if busy (such as by triggering CFB) even though they have no calls and show commands for ephone-dns or ports report nothing unusual.

  Conditions: This symptom occurs in Cisco IOS Release 15.0(1)M after heavy use; it is believed not to occur in Cisco IOS Release 12.4(20)T or prior releases.

  Workaround: Delete and re-add trunk DNs.

- 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.

- CSCtq86500

  Symptoms: With the fix for CSCtf32100, clear text packets destined for the router and coming into a crypto-protected interface are not switched when VSA is used as the crypto engine.

  Conditions: This symptom occurs with packets destined for the router and coming in on an interface with the crypto map applied and VSA as the crypto engine.

  Workaround: Disable VSA and use software encryption.

- CSCtq86515

  Symptoms: UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.

  Conditions: This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.

  Workaround: Do not drop traffic on the device sending the UDP Jitter probe.

- CSCtq88777

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

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

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

- CSCtq90054

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

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

  Workaround: There is no workaround.

- CSCtq90577

  Symptoms: A router crashes when removing Netflow.

  Conditions: The symptom is observed when removing Netflow.

  Workaround: There is no workaround.

- CSCtq91176

  Symptoms: When the Virtual-PPP interface is used with L2TP version 2 and the topology uses an L2TP Tunnel Switch (LTS) (multihop node) and L2TP Network Server (LNS), and PPP between the client and LNS does renegotiation, then the PPP session cannot be established.

  Conditions: This symptom occurs when the LTS forwards the call based on the domain or full username from the PPP authentication username, and the LNS does PPP renegotiation.

  Workaround 1: Disable lcp renegotiation on the LNS and clear the L2TP tunnel at the LNS and LTS.

  Workaround 2: Forward the call on the LTS using an L2TP tunnel name instead of the PPP username/domain name.

- CSCtq91305

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

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

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

  Workaround: There is no workaround.

- CSCtq91939

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

  Conditions: The symptom is observed under the following conditions:

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

  Workaround: There is no workaround.

- 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.

- CSCtq92650

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

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

  Workaround: There is no workaround.

- 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.

- CSCtq95566

  Symptoms: CUCM will append ":5060" to the contents of a contact header when building an outgoing URI if no other port is specified. This is incorrect per the RFC3261. For example: If the following header is received in the contact header of a 200 OK:

  ```
  Contact: <sip:5551112222@192.168.1.1;gr=urn:uuid:44022016-d652-53cf-96e2-
  8421b7e3dbf5>
  ```

  CUCM will build the URI of the ACK as:

  ```
  ACK sip:5551112222@192.168.1.1:5060;gr=urn:uuid:44022016-d652-53cf-96e2- 8421b7e3dbf5
  SIP/2.0
  ```

  Conditions: This was is on a Cisco Unified Communications Manager Release 8.6 (1).

  Workaround: There is no workaround.

- 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.

- CSCtq96466

  Symptoms: The interface configuration “ipv6 dhcp client pd <pd-name>” is not shown in the running-config under virtual-template interfaces.

  Conditions: This happens when the above CLI is configured on a virtual- template interface.

  Workaround: There is no workaround.

- CSCtq96544

  Symptoms: Application ID is limited to 100.

  Conditions: The symptom is observed when configuring a new application. The application ID only allows values in the range of 0-100.

  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 Cisco IOS Software 15.1(2)GC.

  Workaround: There is no workaround.

- 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.

- CSCtr01957

  Symptoms: System crashes when doing a **crypto engine slot 0**.

  Conditions: The symptom is observed with a system boot up with **no crypto engine slot 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.

- CSCtr06926

  Symptoms: A CA server in auto grant mode goes into disabled state when it receives a client certificate enrolment request.

  Conditions: The symptom is observed when a client certificate enrolment request is received.

  Workaround: Do not place the CA server in auto grant mode.

- CSCtr07142

  Symptoms: A memory leak is seen at crypto_ss_open.

  Conditions: No special configuration is needed.

  Workaround: There is no workaround.

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

- CSCtr09142

  Symptoms: Poor throughput is observed with content-scan.

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

  Workaround: There is no workaround.

- CSCtr09251

  Symptoms: Continuous alignment errors and performance degradation in throughput of MS RPC traffic through the ZBFW.

  Conditions: The symptom is observed when inspecting MS RPC traffic through the ZBFW on a Cisco 2911 router that is running Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- 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.

- CSCtr13172

  Symptoms: The **config replace** command crashes the router.

  Conditions: The symptom is observed when close to the maximum number of mediatrace and performance monitoring policies along with DMVPN are configured on the router and the target configuration contains none of these elements.

  Workaround: Uninstall the mediatrace and performance monitor policies prior to replacing the configuration.

- CSCtr14763

  Symptoms: A BFD session is always up, although the link protocol is down.

  Conditions: First the BFD session is up between the routers. After the VLAN is changed on the switch between the routers, the BFD peer is not reachable but the BFD sessions are always up.

  Workaround: There is no workaround.

- CSCtr18559

  Symptoms: An unallocated/unassigned number is received from PBX but as a response, a network congestion message is sent back. Gateway rejects call with 4# when actually its supposed to send a 7#.

  Conditions: The issue occurs only when the country Brazil is configured. When country is set to “itu”, then a 5# is sent which is correct for an unallocated/unassigned number. Follow this link to track cause code to CAs mapping based on selection of countries: http://www.pulsewan.com/data101/r2mfc.pd

Workaround: There is no workaround.

- CSCtr18574

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

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

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

  Workaround: There is no workaround.

- 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.

- CSCtr20300

  Symptoms: SA negotiation test is failing for ipsec_core script.

  Conditions: The symptom is observed when the SA should come into idle state after using **show crypto isakmp sa**.

  Workaround: There is no workaround.

- CSCtr20908

  Symptoms: A spurious access will occur on platforms that detect spurious accesses. A crash will occur on platforms that do not detect spurious accesses such as the Cisco ASR 1000, Cisco 3900 and 3900e.

  Conditions: The issue occurs when running the **show run all** command and when WEBVPN configurations are present.

  Workaround: Use the Cisco IOS 15.1(3)T train.

- CSCtr23134

  Symptoms: Crash seen when IKEv2 debugs are enabled.

  Conditions: The symptom is observed when using the debug "debug crypto ikev2 internal."

  Workaround: There is no workaround.

- 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.

- CSCtr25821

  Symptoms: A Cisco 800 series router crashes with **isdn leased-line bri*0* 128** command:

  ```
  Unexpected exception to CPU: vector 1000, PC = 0x0 , LR = 0x8155A310
  ```

  Conditions: The symptom is observed with the **isdn leased-line bri*0* 128** command.

Workaround: The issue does not occur if there is no cable that connects to the BRI interface. Disconnect the cable from the BRI interface while **isdn leased-line bri*0* 128** is configured.

- CSCtr26531

  Symptoms: When you disable the ISM VPN accelerator using **no crypto engine slot 0, the ISM VPN module is not disabled.**

  Also, under a high load the ISM VPN firmware download will fail.

  Conditions: The symptom is observed with an ISM VPN module and during high traffic load.

  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

- CSCtr29338

  Symptoms: A router crashes.

  Conditions: The symptom is observed after an %ISDN-6-DISCONNECT message from “unknown” followed by a couple of “Illegal Access to Low Address” messages.

  Workaround: There is no workaround.

- CSCtr31153

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

  Conditions: The symptom is observed on a Cisco 7200 series router loaded with Cisco IOS interim Release 15.2(0.19)T0.1.

  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.

- 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.

- 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.

- CSCtr38563

  Symptoms: Switch crashes after configuring a secondary IP address. If the address is saved previously and the switch is upgraded, it will enter a crashing loop.

  Conditions: This occurs when configuring a secondary IP address on a VLAN interface.

  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.

- CSCtr42341

  Symptoms: Crash at task_execute_prep.

  Conditions: The symptom is observed with a Cisco 800 series router that is configured with BFD.

  Workaround: There is no workaround.

- CSCtr42913

  Symptoms: Stale crypto maps seen even after unconfiguring tunnel protection.

  Conditions: The symptom is observed when removing the tunnel source configuration.

  Workaround: Unconfigure and configure again or unconfigure tunnel protection first.

- CSCtr44686

  Symptoms: There is a crash after matching traffic and resetting the connection using following maps:

```
policy-map type inspect smtp SMTP_L7_P1
 class type inspect smtp SMTP_L7_C1
  reset
policy-map type inspect smtp SMTP_L7_P2
 class type inspect smtp SMTP_L7_C2A
  reset
 class type inspect smtp SMTP_L7_C2B
  reset
```

  Conditions: The symptom is observed with the above maps.

  Workaround: Replace “reset” with “log”.

- CSCtr44864

  Symptoms: SYS-2-MALLOCFAIL error message with a device configured with ZBFW and Layer FTP application inspection.

  Conditions: Will observe the following console log messages: %SYS-2-MALLOCFAIL: Memory allocation of 214 bytes failed from 0x22349EA4, alignment 0 Pool: Processor Free: 604021800 Cause: Interrupt level allocation Alternate Pool: None Free: 0 Cause: Interrupt level allocation -Process= ’’<interrupt level>’’, ipl= 1

  Workaround: Disable FTP Application Inspection.

- 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”.

- CSCtr45978

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

  Conditions: Device configured with Cisco IOS WAAS, and crafted FTP packets are passed across the WAN link. Has only been observed on 15.2(1)T IOS Code.

  Once the connection limit is reached and the rest of the connections started going pass-through.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:C

  No CVE ID has been assigned to this issue.

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

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

- 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

- CSCtr50118

  Symptoms: The router crashes.

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

  Workaround: There is no workaround.

- 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.

- CSCtr51926

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

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

  Workaround 1: Enable IPv6 explicitly on the main interface:

  ```
  interface x/y ipv6 enable
  ```

  Workaround 2: Reconfigure the IPv6 address on the subinterface:

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

- CSCtr52186

  Symptoms: Console will not time out from exec session.

  Conditions: The symptom is observed when the router is booted up with "exec- timeout 0 0" for the particular TTY.

  Workaround: Configure significant exec-timeout value and "exit" from exec mode.

- 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 indicies.

  Workaround: Instead of using "get", use "getnext" to list valid indicies for the MIB OID.

- 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.

- 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.

- CSCtr54327

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

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

  Workaround: There is no workaround.

- 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.

- CSCtr55348

  Symptoms: Seemingly unending MIB walk.

  Conditions: The 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.

- CSCtr57804

  Symptoms: ASR 1K router may delete "ipv6 prefix no-advertise" configuration from its subinterfaces when the subinterface is shut down. This may also be seen after a router reload.

  Conditions: This issue is seen when the prefixes defined on the subinterface have been inherited from the "ipv6 general-prefixes" defined in the configuration.

  Workaround: Remove "ipv6 general-prefixes" from the configuration.

- 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.

- 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.

- CSCtr59775

  Symptoms: Proxy map-reply reports locator as unreachable/down.

  Conditions: The symptom is observed when ETR registers to a map-server with proxy map-reply turned on.

  Workaround: Turn-off proxy map-replying.

- CSCtr59840

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

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

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

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

- CSCtr61289

  Symptoms: FlexVPN client remains in NEGOTIATING state, despite being on auto- connect mode, when the FlexVPN server executes a **clear crypto session**.

  Conditions: This occurs in a dVTI setting, where the server has a virtual- template interface and the client has a static tunnel interface that connects to the server. This is not observed in a static setting.

  Workaround: On the client, issue a **clear crypto ikev2 client flexvpn** to clear the FlexVPN session and allow the client to reconnect to the server again.

- 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.

- 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.

- CSCtr66630

  Symptoms: There is prefix corruption when configuring 6VPE. 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.

- CSCtr71465

  Symptoms: A router crashes at ipv4fib_les_switch_fastswitching_compat while booting.

Conditions: The symptom is observed on a Cisco 888E router that is running Cisco IOS interim Release 15.1(2)T1.1 or later.

Workaround: There is no workaround.

- CSCtr75399

  Symptoms: Incremental chunk leaks at NBAR FO chunk and NBAR Flowvar chunk.

  Conditions: The issue is seen in a steady state scenario.

  Workaround: There is no workaround.

- CSCtr83533

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

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

  Workaround 1: Reload the router.

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

- 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.

- CSCtr84800

  Symptoms: An accounting stop is not triggered from DHCP when a client releases the binding.

  Conditions: A DHCP server has a pool with accounting set. When a DHCP client releases the lease, an accounting stop is not sent.

  Workaround: There is now workaround.

- CSCtr86077

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

  Conditions: The symptom is observed under the following conditions:

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

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

- CSCtr86437

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

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

Workaround: Reconfigure “ipv6 nat prefix.”

- 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.

- 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.

- 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.

- CSCtr94052

  Symptoms: Tracebacks seen for Call Forward to CUE scenarios.

  Conditions: The issue is observed from Cisco IOS interim Release 15.2(1.3)T and onwards.

  Workaround: There is no workaround.

- CSCtr94887

  Symptoms: Using MRCP v1, VXML script with ASR operation will always receive noinput event.

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

  Workaround: There is no workaround.

- CSCtr97248

  Symptoms: Router reloads with the following:

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

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

  Workaround: Use the following configuration:

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

- CSCts01653

  Symptoms: Spurious memory access seen on video monitoring router.

  Conditions: The issue is seen after recreating the interface.

  Workaround: There is no workaround.

- CSCts04963

  Symptoms: The following spurious access is seen:

  ```
  No alignment data has been recorded.
  Total Spurious Accesses 789, Recorded 1
  Address Count Traceback 0 789 0x23342B70z 0x239B3450z
  ```

  Decodes:

  ```
  0x23342B70:csdb_dp_timer_handle_flow_idle_timeout(0x233429ac)+0x1c4
  0x239B3450:tw_notify(0x239b3394)+0xbc
  ```

  Conditions: The symptom is observed when MACE and WAAS are configured on the router. While running traffic, spurious memory access is seen. The number of spurious memory accesses indicate that this is continuously happening while timer events are triggered. This is usually seen within 10 minutes of running traffic. After a random amount of time, the router hangs and there is no response. A send break has to be sent at the console to recover to rommon.

  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.

- CSCts11594

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

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

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

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

- CSCts11743

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

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

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

- CSCts12366

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

  Conditions: None

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2011-2578 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

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

- CSCts16285

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

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

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

- CSCts20102

  Symptoms: NVRAM may lose or corrupt after router comes up.

  Conditions: The symptom is observed during stress testing.

  Workaround: Use the **wr erase** and then the **wr memory** commands if NVRAM corruption occurs.

- 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.

- 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.

- CSCts30143

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

  Conditions: The symptom is observed under normal operation.

  Workaround: There is no workaround.

- 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.

  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.

- 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.

- CSCts39240

  Symptoms: The **advertise** command is not available in BGP peer-policy templates.

  Conditions: This symptom is observed on Cisco router running Cisco IOS Release 15.2(01.05)T, Cisco IOS Release 15.2(00.16)S, Cisco IOS Release 15.1 (03)S0.3, or later releases.

  Workaround: The keyword and functionality is still available to be configured in the BGP neighbor command.

- 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.

- CSCts49769

  Symptoms: Switch or router device crashes after critical authentication is unconfigured.

  Conditions: The symptom is observed when critical authentication is configured on an interface using the command:

  authentication event server dead action reinitialize vlan ...

  and then un-configured using either:

  no authentication event server dead action authorize vlan ...

  or

  no authentication event server dead.

  Workaround: Use the correct command to unconfigure critical authentication: **no authentication event server dead action reinitialize vlan ...**.

- 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**.

- CSCts60981

  Symptoms: Watchdog timer tracebacks in common-flow-table code.

  Conditions: The symptom is observed when NBAR is turned on with IPv6 traffic with encrypted payload.

  Workaround: There is no workaround.

- 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.

- CSCts64539

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

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

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

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

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

- CSCts69973

  Symptoms: Spoke with 100 tunnels crashed at nhrp_process_delayed_resolution_event_wrapper.

  Conditions: Source interfaces of the tunnels started to bring up.

  Workaround: There is no workaround.

- CSCts71546

  Symptoms: When a data client is authenticated first and then a voice client is authenticated, the traffic from the data client gets dropped.

  Conditions: The symptom is observed in multi-auth and multidomain host modes when the dynamic VLAN for the voice client is different than the configured voice VLAN and the data client has to be authenticated first.

  Workaround: Dynamic VLAN and configured VLAN for voice device should be same.

- CSCts86975

  Symptoms: Spurious memory access and/or crash at cce_dp_csdb_api_classify.

  Conditions: The symptom is observed when MACE (performance agent) has been configured.

  Workaround: There is no workaround.

- CSCts98336

  Symptoms: IKEv2 router crashes in exec when unconfiguring an active IKEv2 profile.

  Conditions: The symptom is observed when an IKEv2 profile is in use. The crash is occurring only if the profile is configured in a certain way.

  Workaround: Unconfigure first the AAA authorization block.

  ```
  Conf t
  crypto ikev2 profile <profilename>
  no aaa authorization group <type> list <AAA list name> name-mangler <Mangler name>

  no crypto ikev2 profile <profilename>
  ```

- CSCtt03187

  Symptoms: CISP sub-systems are missing and the **cisp enable** CLI is not found.

  Conditions: The CISP enable feature is not found on the Cisco 3945E platform.

  Workaround: There is no workaround.

  Further Problem Description: While making a comparison between the dx_mrvl code and the esw_mrvl code where the hwidb was being initialized it was found in the esw_mrvl case the initialization of the hwidb was taking place irrespective of the check on interesting, igmp or dot1x packet. In the case of dx_mrvl case the initialization of the hwidb was taking place on the condition of else. Thus the initialization in case of dx_mrvl within else condition was not reasonable because hwidb should be initialized irrespective of packet type.

- CSCtt04168

  Symptoms: Tearing down one of the authenticated sessions will clear the mac- address of the other authenticated session.

  Conditions: This symptom is observed in multidomain authentication (MDA) and multi-auth host mode.

  Workaround: The only workaround is to change the host mode to multi-host.

- CSCtt07525

  Symptoms: Spoke router may crash when NHRP is cleared on another spoke.

  Conditions: The symptom is observed with FlexVPN and with spoke-to-spoke tunnels.

  Workaround: There is no workaround.

- CSCtt10507

  Symptoms: When data and voice clients are authenticated and then voice client session is cleared, data session traffic is blocked.

  Conditions: The symptom is observed in multi-auth and multi-domain host modes when the dynamic VLAN for the voice client is different than the configured voice VLAN.

  Workaround: Dynamic VLAN and configured VLAN for voice device should be same.

- CSCtt10633

  Symptoms: Tearing down the voice authenticated session will clear the mac- address of other authenticated data sessions.

  Conditions: This symptom is observed in multidomain authentication (MDA) and multi-auth host mode.

  Workaround: There is no workaround.

- CSCtt11996

  Symptoms: When Open Access is enabled and the port is unauthorized and is in authz fail state, a traffic drop is observed for about 20 secs as soon as the restart timer kicks in.

  Conditions: This symptom is observed when Open Access is enabled.

  Workaround: Enable “spanning-tree portfast”.

- CSCtt14448

  Symptoms: Traceback seen at esw_mrvl_mat_oper_enqueue_msg.

  Conditions: The symptom is observed on a UUT loaded with the Cisco 15.2(1.13) T image.

  Workaround: There is no workaround.

  Further Problem Description: The traceback was seen because of no process to handle MAT operation related functions in esw_mrvl_portdriver_subsys_init initialization.

- CSCtt14867

  Symptoms: Wake on LAN (WoL) is not able to wake up the PC.

  Conditions: This symptom is observed in multidomain authentication (MDA) and single-host host modes.

  Workaround: There is no workaround.

- CSCtt15061

  Symptoms: Router crashes after few hours when two copper cards are installed on the router.

Conditions: The symptom is observed when two copper (SHDSL-EA) cards are installed on a single router.

Workaround: There is no workaround.

- CSCtt20215

  Symptoms: Controller down after reload.

  Conditions: The symptom is observed with a VWIC3 E1/CAS connected to a PBX.

  Workaround: Need to unplug/plug the cable or reset link from PBX side.

- CSCtt33158

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

  Conditions: The symptom is observed if WRED is already present and the queue limit is configured in packets.

  Workaround: Remove WRED and reattach it.

- CSCtt37564

  Symptoms: dACL is not working.

  Conditions: The symptom is observed under all conditions. The IP is not learnt for the first host resulting in ACLs never being applied.

  Workaround: Will work in multi-auth environments.

- 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)T0.1image.

  Workaround: There is no workaround.

- CSCtt44337

  Symptoms: A Cisco 2911 crashes multiple times after an upgrade.

  Conditions: Crashes are encountered on the Cisco 2911 after an upgrade to Cisco IOS Release 15.2(1)T1 to support the SCANSAFE functionality. The crashes are due to reviving TCP packets out of order.

  Workaround: There is no workaround.

- CSCtt45536

  Symptoms: “FlowVar- Chunk malloc failed” messages are seen and this may be accompanied by slow console response.

  Conditions: The symptom is observed when a mix of IPv4 and IPv6 traffic is going through the router configured with QoS, VM, etc.

  Workaround: There is no workaround.

- CSCtu11467

  Symptoms: A “clear auth session mac <data-mac>” is not triggering new authentication for MAB clients.

  Conditions: The symptom is observed when the configured and downloaded data VLAN are different.

  Workaround: Configure the same VLAN in switch and ACS.

- CSCtu12162

  Symptoms: When data and voice client are authenticated and then the voice client session is cleared, (two or more times), the voice mac is not learnt back and the voice authentication session does not start.

  Conditions: The symptom is observed in multi-auth and multi-domain hostmodes

  Workaround: Dynamic VLAN and configured VLAN for voice device should be same.

- 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.

- CSCtu17987

  Symptoms: When a dot1x PC is rebooted, EAPOL packets are not reaching the CPU. Authentication of the PC fails.

  Conditions: Observed in MDA mode.

  Workaround: Once the dot1x is failed, clear the session by issuing **clear auth sess interface**.