Caveats for Cisco IOS Release 15.2(3)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:

Resolved Caveats—Cisco IOS Release 15.2(3)T3

Cisco IOS Release 15.2(3)T3 is a rebuild release for Cisco IOS Release 15.2(3)T. The caveats in this section are resolved in Cisco IOS Release 15.2(3)T3 but may be open in previous Cisco IOS releases.

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

- CSCsy93069

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

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

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

  Workaround: There is no workaround.

- CSCtj59117

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

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

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

  Workaround: Remove CEF.

- 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

- CSCtq39602

  Symptoms: DMVPN Tunnel is down with IPSEC configured. The **show dmvpn** from 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: Configure “set security-association lifetime kilobytes disable” to disable volume based rekeying will reduce 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 4.3/3.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C CVE ID CVE-2012-3915 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

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

- CSCts37446

  Symptoms: Traceback is observed while testing the antireplay feature.

  Conditions: Traceback is observed while configuring the routers randomly. It is not observed manually.

  Workaround: There is no workaround.

- CSCts44393

  Symptoms: A Cisco ASR 1000 crashes.

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

  Workaround: There is no workaround.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt70133

  Symptoms: The RP resets with FlexVPN configuration.

  Conditions: This symptom is observed when using the **clear crypto session** command on the console.

  Workaround: There is no workaround.

- CSCtu08373

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

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

  Workaround: There is no workaround.

- CSCtu28696

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

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

  Workaround: There is no workaround.

- 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.

- CSCtu40028

  Symptoms: The SCHED process crashes.

  Conditions: The issue occurs after initiating TFTP copy.

  Workaround: There is no workaround.

- CSCtw46061

  Symptoms: The following output shows the leaked SA object continuing to be in the "OBJECT_IN_USE" state. The state is supposed to be changed to OBJECT_FREEING by crypto_engine_delete_ipsec_sa(). This is in turn being called by ident_free_outbound_sa_list().

```
shmcp-fp40#sh crypto eli
Hardware Encryption : ACTIVE
Number of hardware crypto engines = 1

CryptoEngine IOSXE-ESP(14) details: state = Active
Capability    : DES, 3DES, AES, RSA, IPv6, GDOI, FAILCLOSE

IKE-Session   :     0 active, 12287 max, 0 failed
DH            :   211 active, 12287 max, 0 failed
IPSec-Session :   323 active, 32766 max, 0 failed
```

  Conditions: This symptom is observed on a Cisco ASR 1000 series router

  Workaround: There is no workaround.

- CSCtw78451

  Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running show commands.

  Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.

  Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

- CSCtw98456

  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.

  Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

  For example, the IVRF routing table should show:

```
S        10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
```

  but instead it shows:

```
S        10.0.0.0 [1/0] via 192.168.0.1
```

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

  Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in **show crypto ipsec sa**) remain at zero.

  Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other IOS versions and other hardware platforms may be affected.

  Workaround: Configure a static route to the remote network. For example:

```
ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
```

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtx04712

  Symptoms: Removal of crypto map hangs the router.

Conditions: The symptom is observed following removal of “gdoi crypto map” from interface.

Workaround: There is no workaround.

- CSCtx31177

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

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

  Workaround: There is no workaround.

- CSCtx41296

  Symptoms: When you do a **clear crypto session** in 4k flexVPN cases, the memory of crypto IKEv2 shows that it is increasing.

  Conditions: The symptom is observed with session flapping.

  Workaround: There is no workaround.

- 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.

- CSCtx50176

  Symptoms: RP crashes @ be_ikev2_abort_negotiation.

  Conditions: The symptom is observed while bringing up 4K SVTI_BGP with ike_group 16.

  Workaround: There is no workaround.

- 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.

- CSCtx61815

  Symptoms: IPsec sessions are not coming up.

  Conditions: The symptom is observed when 1000 sessions are configured. Only 50 IPsec sessions are coming up.

  Workaround: There is no workaround.

- CSCtx73612

  Symptoms: A Cisco ASR 1000 may reload while reading IPsec MIBs via SNMP and write a crashfile.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.1(1)S1.

  Workaround: Do not poll or trap IPsec information via SNMP.

- 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.

- CSCtx93598

  Symptoms: An “ikev1 dpd” configuration erroneously affects IKEv2 flows.

  Conditions: The symptom is observed if we configured the IKEv1 DPD function with “crypto isakmp keepalive” while IKEv2 is enabled as well. The IKEv2 DPD function will be affected.

  Workaround: There is no workaround.

- CSCty12055

  Symptoms: A Cisco ASR 1000 6RU acting as IPsec-DMVPN hub with 4K sessions up on the router may unexpectedly reload at “IPSec background proc” within a few hours.

  Conditions: The symptom is observed on a Cisco ASR 1000 6RU acting as IPsec- DMVPN hub.

  Workaround: There is no workaround.

- CSCty52047

  Symptoms: IKE SAs are not getting deleted by DPD (crypto isakmp keepalive).

  Conditions: This symptom is observed on a Cisco ASR 1000 router with DPD enabled.

  Workaround: Manually delete the stuck isakmp session:

  clear crypto isakmp conn-id

  You can get the conn-id from the output of the **show crypto isakmp sa** command.

- CSCty61212

  Symptoms: The removal of crypto map hangs the router.

  Conditions: This symptom is observed with the removal of GDOI crypto map from interface.

  Workaround: There is no workaround.

- CSCty79277

  Symptoms: Line protocol stays down after Authz success and traffic is allowed.

  Conditions: The symptom is observed with Cisco IOS Release 15.2(2)T, running on a Cisco 1900 platform, doing **default inter Fa0/1/0** with 802.1x configurations and re-applying will authenticate the connected MAB supplicant. However, the interface’s line protocol remains in DOWN state and traffic will be allowed.

  Workaround: Do a **shut** and **no shut** and authenticate the connected supplicant.

- CSCty82414

  Symptoms: Frequent crashes are seen with IPS enabled Firewall and passing TCP traffic. Trace decode points to the “ips_dp_feature_action_internal” function or nearby areas.

  Conditions: This symptom occurs when IPS is enabled with Firewall in the router.

  Workaround: There is no workaround.

- CSCtz14980

  Symptoms: When you perform the RP switch, the standby RP (original active one) will keep rebooting.

Conditions: The symptom is observed when you have “crypto map GETVPN_MAP gdoi fail-close” configured and image is Cisco IOS XE Release 3.6 or 3.7.

Workaround: There is no workaround.

- 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.

- 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.

- CSCtz47309

  Symptoms: When using smart defaults in flexVPN, the mode transport may be sent from initiator even if “tunnel” is configured.

  Conditions: First seen on a Cisco ASR that is running Cisco IOS Release 15.2(2)S and a Cisco ISR running Cisco IOS Release 15.2(3)T. It is seen with flexVPN.

  Workaround: Use smart defaults on both sides on of the tunnel.

- CSCtz47595

  Symptoms: Dial string sends digits at incorrect times.

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

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

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

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

Workaround: There is no workaround.

- CSCtz72390

  Symptoms: The name mangling functionality is broken. Authorization fails with the "IKEv2:AAA group author request failed" debug message.

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

  Workaround: There is no workaround.

- CSCtz73836

  Symptoms: The router crashes.

  Conditions: This symptom is observed when the router is running NHRP.

  Workaround: There is no workaround.

- CSCtz78194

  Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.

  Conditions: The symptom is observed with the Cisco ASR configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.

  Workaround: Shorten the ISAKMP profile name to less than 31.

- CSCtz86763

  Symptoms: Sessions remain partially created, and memory is consumed and not returned.

  Conditions: This symptom occurs when sessions are churned and reset before they reach active state.

  Workaround: There is no workaround.

- CSCtz90154

  Symptoms: Rapid getVPN re-registration by GM when IPsec failure occurs during initial registration. Multiple ISAKMP SAs created and deleted per second.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.2(1)S or Release 15.2(1)S2 as a GM.

  Workaround: There is no workaround.

- CSCtz98066

  Symptoms: When the master switch (Switch A) is reloaded or loses power and rejoins the stack as a member switch, any traffic stream being sent through Switch A is unable to be received by the destination because the newly joined member is not able to establish an ARP entry for the next hop router/switch. Debugs confirm that Switch A does not send a GARP/ARP for the next hop, though traffic continues to be sent to the switch.

Conditions: The symptom is observed when only Switch A has a physical connection between the source and destination router/L3 switch. The newly elected master (Switch B) does not.

Workaround: Ping destination from Switch A, forcing ARP request/response.

- CSCua12317

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

  Conditions: This symptom is observed with the following conditions:

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

  Workaround:

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

- CSCua12396

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

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

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

- CSCua13848

  Symptoms: The Cisco ASR 1000 crashes.

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

  Workaround: There is no workaround.

- CSCua22789

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

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

  Workaround: There is no workaround.

- CSCua23217

  Symptoms: Ping failure observed.

  Conditions: The symptom is observed with DSL group pairs configured on controllers.

  Workaround: There is no workaround.

- CSCua24689

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

  Conditions: The symptom is observed with the following conditions:

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

  Workaround: Disable VFR if possible.

- CSCua29095

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

  Conditions: This symptom occurs while booting the image.

  Workaround: There is no workaround.

- CSCua39107

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

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

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

- CSCua39390

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

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

  Also getting trace back:

```
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F0478z 0x607F72C0z 0x60722F38z 0x6070A300z
0x6070A9CCz 0x603E1680z 0x6029541Cz 0x60298F6Cz 0x6029AD48z 0x6029D384z
0x6062BC68z 0x60632424z 0x60635764z 0x60635CE0z 0x60877F2Cz
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F04E4z 0x607F7154zz
```

  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.

- 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.

- 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.

- 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.

- CSCua65278

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

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

  Workaround: There is no workaround.

- CSCua75069

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

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

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

  – A subsequent configuration change would cause the net to be advertised or withdrawn.

  – Dampening would cause the net to be withdrawn.

  – SOO policy would cause the net to be withdrawn.

  - Split Horizon or Loop Detection would cause the net to be withdrawn.
  - IPv4 AF-based filtering would cause the net to be withdrawn.
  - ORF-based filtering would cause the net to be withdrawn.
  - The net would be withdrawn because it is no longer in the RIB.

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

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

  Older releases on these trains are not impacted.

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

- CSCua78782

  Symptoms: Authentication of EzVPN fails.

  Conditions: The symptom is observed with BR-->ISP-->HQ.

  Workaround: There is no workaround.

- CSCua93001

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

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

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

- CSCua96106

  Symptoms: MSP is not enabled on Cisco 890 platform images.

  Conditions: This symptom is observed when the **profile flow** global command is not available.

  Workaround: There is no workaround.

- 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.

- CSCub19471

  Symptoms: Crash during boot up with MACE and SNMP configurations.

  Conditions: The symptom is observed when the startup configuration contains MACE type (policy-map type mace) configured with both filter (match access-group) and action (e.g. flow monitor). The SNMP configuration is as follows:

```
flow record type mace mace-record
 collect art all
!
!
flow exporter ndeget
 destination 172.25.215.96
!
!
```

```
flow monitor type mace mace-monitor
 record mace-record
!
!
!
class-map match-all mace-class
 match access-group name mace-acl
!
policy-map type mace mace_global
 class mace-class
  flow monitor mace-monitor
!
interface e0/0
 mace enable


ip access-list extended mace-acl
 permit tcp any any
!
snmp-server community public RO
snmp-server community cisco RW
snmp-server ifindex persist
snmp mib persist cbqos
snmp mib persist circuit
```

Reload the router, then during router boot up there will be a crash.

Workaround: Remove SNMP configuration.

- CSCub30751

  Symptoms: DNS SRV based SIP calls fail even though the router is able to resolve the DNS SRV.

  Conditions: None.

  Workaround: Static IP host entry in the router configuration

- 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.

- CSCub55790

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

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

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

  This advisory is available at the following link:

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

- CSCub69976

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

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

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

- 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 *”.

- CSCub76103

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

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

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

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

- 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.

- 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.

- CSCuc06307

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

  ```
  AC Switching[Vl10]: Invalid packet rcvd in process path, dropping packet
  ```

  Conditions: This symptom has been observed in Cisco IOS Release 15.2(3)T4 and earlier.

  Workaround: There is no workaround.

- CSCuc14674

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

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

  Workaround 1: Disable CEF.

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

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

- CSCuc19046

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

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

  Workaround: There is no workaround.

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

- 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

- CSCuc55634

  Symptoms: IPv6 static route cannot resolve the destination.

  Conditions:

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

  Workaround: There is no workaround.

- 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.

- CSCuc69342

  Symptoms: About 10 minutes after CUBE boot, the router crashes with the following traceback:

  ```
  -Traceback= 5B01805 46158ED 45F4F57 45BB19E 45BA1CF 451D6DC 4525549 45252D9 4519C30
  45196A9 4778FFD
  ```
  After the reload from the crash, it may take some time before it crashes again.

  Conditions: This symptom occurs when CUBE receives the SIP REFER message with the Refer-To header having no user part.

  Workaround: There is no workaround.

- 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.

- CSCuc94508

  Symptoms: The router crashes in NBAR Flowvar ch chunk.

  Conditions: This symptom occurs when the router is configured with NBAR features.

  Workaround: Disable NBAR-related commands.

- 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”.

- 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).

- CSCud33159

  Symptoms: Excessive loss of MPLS VPN traffic and high CPU utilization is observed due to the process switching of MPLS traffic over the ATM interface.

  Conditions: This symptom occurs when MPLS is enabled on the ATM interface with aal5snap encapsulation.

  Workaround: There is no workaround.

- CSCud67792

  Symptoms: An invalid modem is detected.

  Conditions: This symptom is observed during bootup.

  Workaround: Use Cisco IOS Release 15.2T-based images.

- CSCud94557

  Symptoms: Build failed to compile c800 images.

Conditions: The symptom is observed with c800 images.

Workaround: There is no workaround.

- CSCue05844

  Symptoms: The Cisco 3925 router running Cisco IOS Release 15.0(2)SG reloads when connecting to a call manager.

  Conditions: This symptom is observed with the Cisco 3925 router running Cisco IOS Release 15.0(2)SG.

  Workaround: Remove SNMP.

Resolved Caveats—Cisco IOS Release 15.2(3)T2

Cisco IOS Release 15.2(3)T2 is a rebuild release for Cisco IOS Release 15.2(3)T. The caveats in this section are resolved in Cisco IOS Release 15.2(3)T2 but may be open in previous Cisco IOS releases.

- CSCsi02145

  Symptoms: A Cisco router may stop processing traffic on an interface that is configured with VRF Lite.

  Conditions: This symptom is observed when the input queue eventually wedges (76/75) below due to ICMP redirect messages being stuck.

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 5475.d0e0.1da8 (bia 5475.d0e0.1da8)
  Description: to Switch
  Internet address is x.x.x.x/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:02:01, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:32:15
  Input queue: 76/75/117/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

  Workaround: Locate the source of the ICMP redirects and address the underlying reason they are being sent to the router.

- CSCtr45287

  Symptoms: The router crashes in a scale DVTI scenario.

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

  Workaround: Use fewer tunnels or use a different platform.

- CSCts68626

  Symptoms: PPPoE discovery packets causes packet drop.

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

  Workaround: There is no workaround.

- CSCts83046

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

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

  Workaround: There is no workaround.

- CSCtu40028

  Symptoms: The SCHED process crashes.

  Conditions: This symptom occurs after initiating TFTP copy.

  Workaround: There is no workaround.

- CSCtv36812

  Symptoms: Incorrect crashInfo file name is displayed during crash.

  Conditions: This symptom is observed whenever a crash occurs.

  Workaround: There is no workaround.

- CSCtw46229

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

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

  Workaround: Ensure that 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

- CSCtw88689

  Symptoms: A crash is seen while applying the policy map with more than 16 classes with the Cisco 3900e platform.

  Conditions: This symptom occurs when applying the policy map with more than 16 classes.

  Workaround: There is no workaround.

- CSCtw98200

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

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

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

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

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

- CSCtx17480

  Symptoms: The router crashes when trying to free the received LCP CONF Request packet containing the option that is not recognizable or is not acceptable for negotiation and the CONF reject for that option is sent.

  Conditions: This symptom occurs when the option that is not recognizable or is not acceptable for negotiation is of length 0 or invalid length.

  Workaround: There is no workaround.

- CSCtx22322

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

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

  Workaround: There is no workaround.

- CSCtx48753

  Symptoms: Higher memory usage with PPP sessions than seen in Cisco IOS XE Release 3.4/3.5.

  Conditions: This symptom is observed with configurations with PPP sessions. These will see up to 10% higher IOS memory usage than in previous images.

  Workaround: There is no workaround.

- 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.
  - Cisco IOS Release 15.0(1)M5.

  Workaround: Set delay timer without 0.

- CSCtx95840

  Symptoms: A Cisco voice gateway may unexpectedly reload.

  Conditions: This symptom is observed on a Cisco voice gateway running SIP protocol. In this case, the issue occurs when sipSPIUfreeOneCCB() returns, and the leftover event is still being processed after CCB is released from sipSPIUfreeOneCCB(). Based on sipSPIStartRemoveTransTimer(ccb), CCB should have been released later by a background timer.

  Workaround: There is no workaround.

- CSCty01237

  Symptoms: The router logs show:

  ```
  <timestamp> %OER_BR-5-NOTICE: Prefix Learning STARTED
  CMD: 'show run' <timestamp>
  ```

  This is followed by the router crashing.

  Conditions: This issue is seen under the following conditions:

  1. Configure PfR with a learn-list using a prefix-list as a filter and enable learn.
  2. Use a configuration tool, script or NMS that periodically executes **show run** on the MC over HTTP or some other means.

  Workaround 1: If you use the PfR learn-list feature, do not execute **show run** periodically.

  Workaround 2: If you use a monitoring tool that executes **show run** periodically, avoid using a learn-list configuration in PfR.

- CSCty04359

  Symptoms: In a manually created WExp device certificate, when the image is upgraded from Cisco IOS Release 15.1(3)T (Phase 1) to Cisco IOS Release 15.2(3)T (Phase 2), the device goes offline in WCM.

  Conditions: This symptom is observed with a manually created WExp device certificate, when the image is upgraded from Cisco IOS Release 15.1(3)T (Phase 1) to Cisco IOS Release 15.2(3)T (Phase 2).

  Workaround: Configure the trustpoint policy using rsakeypair, and add the **rsakeypair** *trustpoint-name* command to the configuration.

- CSCty32851

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

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

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

- CSCty48870

  Symptoms: The router crashes due to a bus error.

  Conditions: This symptom has been observed in a router that is running Cisco IOS Release 15.2(2)T and Cisco IOS Release 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.

- CSCty51453

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

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

  Workaround 1: Add the following commands to change the TCP segmentation on the router:

  ```
  router(config)# ip tcp mss 1400
  router(config)# ip tcp path-mtu-discovery
  ```

  Workaround 2: Use a different validation method (CRL) when possible.

- 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.

- CSCty55449

  Symptoms: The device crashes after registering an Embedded Event Manager TCL policy.

  Conditions: This symptom occurs if the policy uses the multiple event feature and the trigger portion is registered without curly braces ("{}"). Then, the device will crash. For example, this policy will trigger a crash:

```
::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger
::cisco::eem::correlate event 1 or event 2

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

action_syslog priority crit msg " triggered "
```

  Note how "::cisco::eem::trigger" is not followed by an opening curly brace.

  Workaround: Ensure that the trigger portion (that is, the correlate statement) is enclosed within curly braces. Given the example above, the proper syntax is:

```
::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger {
    ::cisco::eem::correlate event 1 or event 2
}

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

action_syslog priority crit msg " triggered "
```

- CSCty56850

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

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

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

  show IP NBAR protocol-discovery

  Workaround 2: Perform a snmpget against objects in cnpdAllStatsTable.

- CSCty64721

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

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

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

Workaround: There is no workaround.

- CSCty65189

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

  Conditions: This symptom is observed when ZBFW is configured.

  Workaround: There is no workaround.

- CSCty80553

  Symptoms: A multicast router crashes.

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

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

- CSCty86039

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

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

  Workaround: There is no workaround.

- CSCty96052

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

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

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

- CSCty97961

  Symptoms: A device configured with SSLVPN crashes.

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

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

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

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

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

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

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2012-3924 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtz13465

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

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

  Workaround: There is no workaround.

- CSCtz13818

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

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

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

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

- CSCtz26735

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

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

  Workaround: There is no workaround.

- CSCtz37164

  Symptoms: The requests to the RADIUS server are retransmitted even though the session no longer exists, causing unnecessary traffic to RADIUS, and RADIUS getting requests for an invalid session.

  Conditions: This symptom occurs when the RADIUS server is unreachable and the CPE times out the session.

  Workaround: The fix is currently being worked upon. This issue can be seen as per the conditions mentioned above. This issue can be avoided by making sure that the RADIUS server is always reachable.

- CSCtz37863

  Symptoms: IPCP is not in an open state and it does not seem to be calling the This-Layer-Down (TLD) vector.

  Conditions: This symptom is observed if IPv4 saving is enabled and IPCP negotiation failed because of a TermReq received from peer.

  Workaround: There is no workaround.

- CSCtz44989

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

Conditions: This symptom is observed with IPv6 link-local next-hop. When the EIGRP route is redistributed to BGP VRF, it clears the next-hop information (it becomes 0.0.0.0). Then, this route becomes invalid and BGP is not able to export to another VRF.

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. This 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.

- CSCtz70623

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

  Conditions: This symptom occurs when a two-wire cable is unplugged from the G.SHDSL interface.

  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.

- CSCtz72044

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

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

  Workaround: There is no workaround.

- CSCtz73263

  Symptoms: MSP is not getting packets on SVI interface and MSP profile is not getting attached to the flow.

  Conditions: This symptom is observed when the **profile flow** command is configured globally and an MSP profile is applied using **media-proxy services** *profile-name*.

  Workaround: Disable MSP using **no profile flow** and enable it again using **profile flow**.

- CSCtz77171

  Symptoms: Subscriber drops are not reported in mod4 accounting.

  Conditions: This symptom is observed on checking the policy-map interface for account QoS statistics on a port-channel subinterface.

  Workaround: There is no workaround.

- CSCtz80643

  Symptoms: A PPPoE client's host address is installed in the LNS's VRF routing table with the **ip vrf receive** *vrf name* command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

  Conditions: This symptom is observed only when the Virtual-access interface is configured with the **ip vrf receive** *vrf name* command via the Virtual-Template or RADIUS profile.

  Workaround: There is no workaround.

- CSCua06598

  Symptoms: The router may crash with breakpoint exception.

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

  Workaround: Disable SNMP IPv6 polling.

- 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: This symptom is observed when the leak is apparent after 3-4 weeks. The process is CCSIP_SPI_CONTRO.

Workaround: There is no workaround.

- CSCua15292

  Symptoms: The router may report unexpected exception with overnight stress traffic.

  Conditions: This symptom is observed with the following conditions:

  - Cisco ISR 3925E is deployed as DMVPN hub router and about 100Mbps traffic is controlled by PfR MC with dynamic PBR.
  - Router logs with

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

  Workaround: There is no workaround.

- 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 1 minute after the tunnel between the spokes came up.

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

  Workaround: There is no workaround.

- CSCua33821

  Symptoms: CPU utilization shoots up to 99% after configuring crypto maps.

  Conditions: This symptom is observed after applying crypto maps.

  Workaround: There is no workaround.

- CSCua40273

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

  Conditions: This symptom occurs on the Cisco ASR 1000 series router running Cisco IOs Release 15.1(02)S.

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

- CSCua43930

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

  Conditions: This symptom occurs on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua45122

  Symptoms: Multicast even log preallocated memory space needs to be conserved on the low-end platform.

  Conditions: This symptom is observed with multicast even log.

  Workaround: There is no workaround.

- CSCua47570

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

  Conditions: This 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.

- CSCua49764

  Symptoms: The WAAS-Express device goes offline on WCM.

  Conditions: This symptom occurs when a certificate is generated using HTTPS when using the Cisco IOS Release 15.1(3)T image. Once upgraded to Cisco IOS Release 15.2(3)T, the WAAS-Express device goes offline on WCM.

  Workaround: Configure an rsakeypair on the TP-self-signed trustpoint with the same name and execute the **enroll** command again or delete the self-signed trustpoint point and reenable the HTTP secure-server.

- CSCua51991

  Symptoms: An invalid SPI message is seen throughout the lifetime of IPsec SA.

  Conditions: This symptom is observed with SVTI-SVTI with a GRE IPv6 configuration. When bringing up 1K sessions, an invalid SPI is seen. There is also inconsistency between the number of child SAs in IKEv2 and the number of IPsec SAs on the same box.

  Workaround: There is no workaround.

- CSCua60785

  Symptoms: Metadata class-map matches only the first of the following filter, if present, in a class map (the other media-type matches are skipped):

  match application attribute [category, sub-category, media-type,

  device-class] *value-string*

  match application application-group *value-string*

  Conditions: This symptom is observed in a case where the class map has the aforementioned filters.

  Workaround: There is no workaround.

- CSCua67998

  Symptoms: The system crashes.

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

  Workaround: There is no workaround.

- CSCua71038

  Symptoms: The router crashes.

  Conditions: This symptom is observed with a Cisco router that is running Cisco IOS Release 15.2(3)T1. The router may crash during the failover test with OCSP and CRL configured.

  Workaround: Configure OCSP or CRL but not both

- CSCua77729

  Symptoms: Embedded AP in the Cisco 1941 ISR becomes unreachable after using the “reload in” command on the Cisco ISR CLI. This issue is seen when using “reload in” on the Cisco ISR CLI and choosing the option to reload embedded AP.

```
CISCO1941W-E/K9 Version 15.1(4)M4
AP801 Software (AP801-K9W7-M), Version 12.4(21a)JA1

Router#reload in 10

Do you want to reload the internal AP ? [yes/no]: yes

Do you want to save the configuration of the AP? [yes/no]: no

System configuration has been modified. Save? [yes/no]: no
Reload scheduled for 13:57:01 UTC Mon May 21 2012 (in 10 minutes) by console
Reload reason: Reload Command
Proceed with reload? [confirm]
Router#
May 21 13:47:03.759:
%SYS-5-SCHEDULED_RELOAD:<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi?a
ction=search&counter=0&paging=5&links=reference&index=all&query=SYS-5-SCHEDULED_RELOAD
>
Reload requested for 13:56:51 UTC Mon May 21 2012 at 13:46:51 UTC Mon May 21
2012 by console. Reload Reason: Reload Command.
```

  After that, AP becomes unreachable, and the user cannot session to AP with “service-module wlan-ap 0 session”.

  Conditions: This symptom is observed when using “reload in” on the Cisco ISR CLI and choosing the option to reload embedded AP. This issue is seen under the following conditions:

```
CISCO1941W-E/K9 Version 15.1(4)M4
AP801 Software (AP801-K9W7-M), Version 12.4(21a)JA1
using the "reload in" command on ISR CLI with Do you want to reload the
internal AP ? [yes/no]: yes
```

  Workaround 1: Use “reload in” on the Cisco ISR CLI and do not choose the option to reload embedded AP.

```
Router#reload in 2
Do you want to reload the internal AP ? [yes/no]: no
```

  Workaround 2: Use the normal **reload** command.

- CSCua84923

  Symptoms: Following a misconfiguration on a two-level hierarchical policy with a user-defied queue-limit on a child policy, the UUT fails to attach the QoS policy on the interface even when corrected queueing features are used.

  Conditions: This symptom is observed with the following conditions:

  1. The issue must have the user-defined queueu-limit defined.
  2. 2) This error recovery defected is confirmed as a side effect with the c3pl cnh compoent project due to ppcp/cce infrastructure enhancement.

  Workaround: There is no workaround.

- CSCua86620

  Symptoms: The vmware-view application is not detected/classified.

  Conditions: This symptom is observed when vmware-view applications are used.

Workaround: There is no workaround.

- CSCua93688

  Symptoms: When pinging from the Cisco 1921 router to connected devices, the response time is unexpectedly slow.

  ```
  round-trip min/avg/max = 8/46/92 ms
  ```

  Conditions: This symptom is observed with the EHWIC-1GE-SFP-CU module on Cisco ISR-G2 platforms.

  Workaround: Shut/no shut the EHWIC-1GE-SFP-CU interface. The ping time resumes to normal.

- CSCua96354

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

  Conditions: This symptom is observed with the following commands:

  - **show oer master traffic-class performance**
  - **show pfr master traffic-class performance**

  Workaround: There is no workaround.

- CSCua97981

  Symptoms: The Cisco IOS redundancy facility is slow to come up after master router reload and gets stuck in the “final progression” state.

  Conditions: This symptom was first seen in Cisco IOS Release 15.2(3)T and was also observed in Cisco IOS Release 15.2(3)T1.

  Workaround: Manually reloading the Standby router will resolve the issue.

- 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.

- 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.

- CSCub46570

  Symptoms: The image cannot be built with an undefined symbol.

  Conditions: This symptom occurs as the commit error triggers the compiling issue.

  Workaround: There is no workaround.

- CSCtq91063

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

  Conditions: This symptom occurs due to the F/S particle pool running out of free particles and the next packet failing to successfully obtain a particle. The F/S pool is used for fragmentation, so this will only occur when there is a large amount of fragmentation occurring. It has only been seen when there is a “ip mtu 1500” configured on a tunnel interface where the physical mtu is 1500 forcing packets to be fragmented on the physical interface rather than on the tunnel interface.

  Workaround 1: Remove “ip mtu 1500” from the tunnel interface.

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

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

- CSCua21166

  Symptoms: Unable to form IPSec tunnels due to the following error:

  “RM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with securityk9 technology package license.”

  Conditions: This symptom occurs when even though the router does not have 225 IPsec SA pairs, the 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

- CSCua60100

  Symptoms: The router crashes at ip_acl_peruser_ctxt_free while clearing the calls.

  Conditions: The symptom is observed when an ACL filter is applied on the input direction and then the session is established. When you try to clear the session, the router crashes.

  Workaround: There is no workaround.

- CSCua70065

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

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

  Workaround: There is no workaround.

- CSCtz69084

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

  Conditions: This symptom is observed with the following conditions:

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

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

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

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

  Workaround: There is no workaround.

- CSCua18166

  Symptoms: When sub appid is triggered by end points, the network does not recognize it and displays it as "Unknown identifier".

  Conditions: This symptom occurs when the limitation results in not supporting traffic classification based on sub appid.

  Workaround: There is no workaround.

- CSCub47910

  Symptoms: Unexpected reboot is seen due to Bus Error when using software version Cisco IOS Release 15.2(4)M1.

  Conditions: This symptom is observed when SSL VPN is configured on the Cisco ISR in Cisco IOS Release 12.5(4)M1, where the CEF process running in the context of SSL is being interrupted or asked for relinquishing of CPU.

  Workaround: There is no workaround.

- CSCub91815

  Symptoms: Certificate validation fails with a valid certificate.

  Conditions: This symptom is observed during DMVPN setup with an empty CRL cache. This issue is usually seen on the responder side, but the initiator can also show this behavior.

  Workaround: There is no known workaround.

- CSCuc07799

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

  Conditions: This symptom occurs when the ISM-VPN Module is inserted in the router.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(3)T1

Cisco IOS Release 15.2(3)T1 is a rebuild release for Cisco IOS Release 15.2(3)T. The caveats in this section are resolved in Cisco IOS Release 15.2(3)T1 but may be open in previous Cisco IOS releases.

- CSCtq24557

  Symptoms: The router crashes after deleting multiple VRFs. This happens very rarely.

  Conditions: This symptom is observed in a large-scale scenario.

  Workaround: There is no workaround.

- CSCtq39602

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

  Conditions: This symptom is observed after heavy traffic is pumped from the DMVPN hub to the spoke for some time, that is, 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.

- CSCtq95384

  Symptoms: Even after the removal of NSR configurations, BGP still holds memory.

  Conditions: This symptom is observed after the removal of NSR configurations.

  Workaround: There is no workaround.

- CSCtr36083

  Symptoms: IKE SAs are not cleared. Ping fails over the IPsec tunnel.

  Conditions: This symptom occurs when SAs are cleared by using the **clear crypto session local** *address* command.

  Workaround: There is no workaround.

- CSCtr87070

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

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

  Workaround: Remove TACACS single-connection.

- CSCts32708

  Symptoms: Similar to CSCth80642, the Cisco IOS SSLVPN router fails to accept new sessions. Users will not be able to load the WebVPN login page. If you enable debug SDPs, you may see the “Sev 4:sdps_get_pak_from_tcp(),line 1080:tcp_getpacket returned error 2, tcb=0x6A9EFFEC” error message.

  Conditions: This symptom is observed when the router remains reachable. Otherwise, (that is, you can ping the WebVPN IP) the SSL process is running and listening on the right port. The **show tcp tcb** and **show tcp brief all numeric** commands show connections stuck in the 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.

Workaround 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

- 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 nonrestarting peer (RR, in this case).

  Conditions: This 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 nonrestarting router does not send back the corresponding VPN prefixes towards the restarted router.

  Workaround: There is no workaround.

- CSCts85459

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

  Conditions: This 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 you reload the router, the cellular interface does not connect if a crypto map is applied and you will see that IPsec fails to initialize because you do not have an IP address.

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

- CSCtt17762

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

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

  Workaround: There is no workaround.

- CSCtt26692

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

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

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

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

- CSCtt34790

  Symptoms: Unexpected drops occur due to a large shaping burst.

  Conditions: This symptom occurs on high-speed interfaces with large shape values.

  Workaround: There is no workaround.

- CSCtt94440

  Symptoms: The Cisco ASR 1000 series router RP may reload.

  Conditions: This symptom is observed when an etoken is in use and the **show crypto eli all** command is issued.

  Workaround: Avoid using the **show crypto eli all** command. However, you can use the **show crypto eli** command.

- 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.

- CSCtu14409

  Symptoms: The “Insufficient bandwidth 2015 kbps for bandwidth guarantee” error message is displayed when configuring a policy map with “priority level xxx” and then updating it with “police cir xxx”.

  Conditions: This symptom occurs when the priority is configured without a specific rate. This issue is only seen with a Cisco ASR 1000 series router.

  Workaround: Configure police before priority.

- CSCtu22167

  Symptoms: SP crashes.

  Conditions: This symptom is observed under the following conditions:

  - When unicast prefixes have local labels.
  - When the tunnel is the next-hop for those prefixes.
  - When the topology is modified (that is, when you remove or shut down the physical interface) so that the tunnel’s destination address is reachable via the tunnel.

  Workaround: Ensure that the tunnel endpoint peer does not advertise the prefixes to reach the tunnel endpoint.

- CSCtu35116

  Symptoms: VPDN session keeps on trying to come up with MPLS MTU higher than 1500.

  Conditions: This symptom is observed when you upgrade a Cisco 7200VXR from the c7200-a3jk91s-mz.122-31.SB18 to the c7200-adventerprisek9-mz.122-33.SRE4 image.

  Workaround: There is no workaround.

- CSCtu43120

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

Conditions: This symptom is observed with L2TP.

Workaround: There is no workaround.

- CSCtw61192

  Symptoms: When the **redistribute static** command has the *route-map* and the *set tag* arguments, and you enter the **no redistribute static** command, the router sends out only one query and the remaining routes get stuck in active state indefinitely.

  Conditions: This symptom is observed only when you set a tag to a redistributed route.

  Workaround: There is no known workaround.

- CSCtw61872

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

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

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

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

- CSCtw62213

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

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

  Workaround: Increasing the input queue length on the interface and SPD queue length is a valid workaround

- CSCtw62310

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

  Conditions: This 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.

- CSCtw68089

  Symptoms: The routing event detector is not present on Integrated Services Routers such as the Cisco 2800 series.

  Conditions: This symptom occurs for all releases on generation one Cisco ISR routers running Cisco IOS Release 15.2(2)T.

  Workaround: There is no workaround.

- CSCtw73530

  Symptoms: Unable to delete metadata sessions.

Conditions: This symptom is observed when more than 100 metadata sessions are created.

Workaround: Disable metadata and then enable it. Note that this will remove all the flows.

- CSCtw82120

  Symptoms: Cisco IOS might restart when the DMVPN QoS policy-map name is modified at the hub tunnel.

  Conditions: This symptom occurs when the DMVPN/QoS service-policy name is modified on the hub tunnel, and there are several spokes configured with the same NHRP group name. There could be a slim timing window during which Cisco IOS might get restarted due to a race-condition.

  Workaround: Waiting for some time before issuing the next command to change the QoS policy-map name would greatly minimize the chance to hit this race-condition.

- CSCtw86712

  Symptoms: RP crashes.

  Conditions: This symptom is observed when you apply certain tunnel configurations.

  Workaround: There is no workaround.

- CSCtw94598

  Symptoms: Web authentication does not work after an upgrade. NAS-Port-Type = Async.

  Conditions: This symptom is observed when you upgrade to Cisco IOS Release 12.2 (58)SE2 or later or to the Cisco IOS 15.0(1)SE train.

  Workaround: Change NAS-Port-Type on AAA Server to match the new value.

- CSCtw95189

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

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

  Workaround: There is no workaround.

- CSCtw98456

  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.

  Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

  For example, the IVRF routing table should show:

  ```
  S        10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
  ```

  but instead it shows:

  ```
  S        10.0.0.0 [1/0] via 192.168.0.1
  ```

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

  Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in **show crypto ipsec sa**) remain at zero.

Conditions: This symptom has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other Cisco IOS versions and other hardware platforms may be affected.

Workaround: Configure a static route to the remote network. For example:

```
ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
```

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtx04709

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

  Conditions: This symptom is observed 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.

- CSCtx27813

  Symptoms: The evaluation license cannot be used on a Cisco router.

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

  Workaround: There is no workaround.

- CSCtx29543

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

  Workaround: There are two possible workarounds:

  1. Ensure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then ensure 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.

- CSCtx31175

  Symptoms: Framed-IP-Address is added twice in the PPP service-stop accounting record.

  Conditions: This symptom is observed with the following conditions:

  1. A user session exists on the Cisco ASR 1001 router.
  2. Stop one user’s session by using the **clear subscriber session username xxx** command on the Cisco ASR 1001 router.

3. The Cisco ASR 1001 router sends double “Framed-IP-Address” in service-stop accounting for one user’s session.

Workaround: Do not use the **clear subscriber session** command to clear the session. Instead, use the **clear pppoe** command.

- CSCtx32329

  Symptoms: When using the **show ipv6 rpf** command, the router crashes or displays garbage for RPF idb/nbr.

  Conditions: This symptom can occur 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.

- CSCtx35064

  Symptoms: Traffic remains on a blackholed path until the holddown timer expires for PfR monitored traffic class. Unreachables are seen on the path, but no reroute occurs until holddown expires.

  Conditions: This symptom is seen under the following conditions:

  – MC reroutes traffic-class out from a particular path (BR/external interface) due to the OOP condition on the primary path.
  – Shortly after enforcement occurs, an impairment on the new primary path occurs, causing a blackhole.
  – PfR MC does not declare OOP on the new primary path and attempts to find a new path until the holddown timer expires. This causes traffic loss.

  Workaround: Reduce the holddown timer to 90 seconds (minimum value) to minimize impact.

- CSCtx38806

  Symptoms: SSL VPN users lose connectivity as soon as a 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 a headend for SSL VPN connections.

  Workaround: Any of the following workarounds will work:

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

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

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

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

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

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

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

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

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

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

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

- 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.

- CSCtx49098

  Symptoms: A crash occurs at udb_pre_feature_unbind_cleanup.

  Conditions: This symptom is observed when a complex 3 level HQoS policy is configured on the interface and it is manipulated with changes.

  Workaround: Do not manipulate the QoS policy while it is being used or avoid using the same child policy multiple times in the parent policy.

- CSCtx54882

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

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

  Workaround: There is no known workaround.

- CSCtx55357

  Symptoms: Auto RP messages are permitted through "ip multicast boundary".

  Conditions: This symptom is observed when the ACL associated with the multicast boundary matches 224.0.1.39 and 224.0.1.40. It is seen on the Cisco ASR 1000 platform.

  Workaround: Use "no ip pim autorp" to disable Auto RP completely from this device.

- CSCtx57073

  Symptoms: A Cisco router may crash with the following error: "Segmentation fault(11), Process = Metadata HA"

Conditions: This symptom is observed while upgrading the router from Cisco IOS XE Release 3.6 to mcp dev.

Workaround: The required changes have been made with this DDTS to prevent the crash.

- CSCtx64347

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

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

  Workaround: There is no workaround.

- CSCtx64684

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

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

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

- CSCtx66030

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

  - SIP-CME
  - SIP-SRST GW
  - CUBE

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

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

- CSCtx67474

  Symptoms: An update message is sent with an empty NLRI when the message consists of a 2byte AS-path in ASPATH attribute and a 4byte value aggregate attribute.

  Conditions: This symptom occurs 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 nonimpacting outbound policy like “advertisement-interval”.

- CSCtx68100

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

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

  Workaround: There is no workaround.

- CSCtx74342

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

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

Workaround: Configuring the SPF throttle timer can change the interval.

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

Routershow 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

- CSCtx82775

  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.

  Conditions: This symptom is observed when MTP is invoked for calls.

  Workaround: Reload the router or perform a no sccp/sccp.

- CSCtx86674

  Symptoms: ATM VPI/VCI does not come up after upgrading to Cisco IOS Release 15.1(4)M4.

  Conditions: This symptom is observed when upgrading to Cisco IOS Release 15.1(4)M4, which was an engineering build given for addressing CSCtx09973.

  Workaround: ATM port shut/no shut resolves the issue. However, it refers to about 5000+ nodes here or “config dsl-group 0 pairs 0” instead of dsl-group auto under controller SHDSL.

- 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.

- CSCtx99544

  Symptoms: Exception occurs when using the **no aaa accounting system default vrf** *VRF3* **start-stop group** *RADIUS-SG-VRF3* command:

  ```
  router(config)# no ip vrf VRF3
  router(config)# no aaa accounting system default vrf VRF3 start-stop group
  RADIUS-SG-VRF3

  %Software-forced reload
  ```

  Conditions: This symptom is observed with the following conditions:

  – Hardware: Cisco ASR 1001 router.

  – Software: asr1001-universalk9.03.04.02.S.151-3.S2.

Workaround: There is no workaround.

- CSCty01234

  Symptoms: A router running Cisco IOS may reload unexpectedly.

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

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

- CSCty02403

  Symptoms: An EIGRP topology entry with bogus next-hop 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 next-hop. So if you have a default route received from some neighbors, then that default route will also flap.

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

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

- CSCty03629

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

  Conditions: This symptom occurs when NAT is colocated with SGFWl.

  Workaround: There is no workaround.

- CSCty03745

  Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.

  Conditions: This symptom occurs when the IPv4 default route exists, that is:

  ```
  ip route 0.0.0.0 0.0.0.0 <next-hop>
  ```

  Or a certain static/IGP route exists. For example:

  ```
  ip route 0.0.253.0 255.255.255.0 <next-hop>
  ```

  Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family. For example, router bgp 65000 address-family l2vpn vpls neighbor 10.10.10.10 next-hop-self
  Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

- 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.

- CSCty15615

  Symptoms: The policy in direction A may disappear after removing the policy from direction B. The policies no longer show up under the interface in **sh policy-map int** or **show running**.

  Conditions: This symptom is observed with policies on both input and output directions, and when you remove the policy from one of the directions. This issue is seen on Cisco 7200/7600 platforms.

  Workaround: There is no workaround.

- CSCty22840

  Symptoms: A router can crash due to a Watchdog timeout on the NTP process as it fails to unpeer from an NTP peer that had already been removed. In addition, the following error might be seen in the system log:

  ```
  NTP Core (ERROR): peer struct for X.X.X.X not in association table
  ```

  Conditions: This symptom is observed when active changes occur in NTP, that is, new peers or servers are added at boot time as part of the existing configuration or during normal operation as part of a new configuration.

  Workaround: Configure NTP to use the ACL with the **ntp access-group peer** command to explicitly define which hosts can function as an NTP peer.

- CSCty24606

  Symptoms: Under certain circumstances, the Cisco ASR 1000 series router’s ASR CUBE can exhibit stale call legs on the new active after switchover even though media inactivity is configured properly.

  Conditions: This symptom is observed during High Availability and box to box redundancy, and after a failover condition. Some call legs stay in an active state even though no media is flowing on the new active. The call legs can not be removed manually unless by a manual software restart of the whole chassis. The call legs do not impact normal call processing.

  Workaround: There is no workaround.

- CSCty24707

  Symptoms: Standby RP continually reboots and never recovers.

  Conditions: This symptom is observed during an RP standby switchover with QoS applied to ISG sessions.

  Workaround: Shut down the virtual template interface and do a switchover.

- CSCty25810

  Symptoms: Tracebacks are observed on the PAN module in auth_feature_critical_get_authorized_domain_any()/dot1x_matm_mac_addr_learned () functions.

  Conditions: This symptom occurs due to an invalid HWIDB pointer. HWIDB is NULL for the mac-addresses learned over the CPU_PORT in case of L2VPN.

  Workaround: There is no workaround.

- CSCty30886

  Symptoms: A standby RP reloads.

  Conditions: This symptom is observed when bringing up PPPoE sessions with configured invalid local IP address pool under the virtual-template profile and “aaa authorization network default group radius” on the box with no radius present. No IP address is assigned to the PPPoE Client.

  Workaround: There is no workaround.

- CSCty37020

  Symptoms: Learned inside BGP prefixes are not getting added into the MC database.

  Conditions: This symptom is observed with learned inside BGP prefixes.

  Workaround: There is no workaround.

- CSCty37445

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

  Conditions: This 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 the Cisco 3945 router and the Cisco 3945E router due to digital signature failure.

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

  Workaround: There is no workaround.

- CSCty43587

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

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

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

  Workaround: There is no workaround.

- CSCty46273

  Symptoms: A router configured with the Locator ID Separation Protocol (LISP) may crash when the connected routes in the RIB flap.

  Conditions: This symptom is observed when LISP tracks the reachability of routing locators (RLOCs) in the RIB. For the crash to occur, a locator being watched by LISP must be covered by a route that is itself covered by a connected route. If both these routes are removed from the RIB in close succession, there is a small possibility that the race-condition resulting in this crash may be hit.

Workaround: There is no workaround.

- CSCty49656

  Symptoms: A crash is observed when executing the **no ip routing** command.

  Conditions: This symptom is observed under the following conditions:

  1. Use a Cisco IOS image that has fix for CSCtg94470.
  2. Configure OSPF.
  3. Enable multicast.
  4. Create several (>6000) routes in the network to be learned by OSPF.
  5. Wait for OSPF to learn all the (>6000) routes from the network.

  Finally, executing the **no ip routing** command may crash the box.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCty61212

  Symptoms: The removal of crypto map hangs the router.

  Conditions: This symptom is observed with the removal of GDOI crypto map from interface.

  Workaround: There is no workaround.

- CSCty65334

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

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

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

- CSCty68348

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

  Conditions: This symptom is observed under the following conditions:

  – The OSPF router is configured for “nsr”.

  – Shutdown/no shutdown of the OSPF process.

  Workaround: Flapping of the neighbor will fix the issue.

- CSCty68402

  Symptoms: NTT model 4 configurations are not taking effect.

  Conditions: This symptom occurs under the following conditions:

```
policy-map sub-interface-account
 class prec1
  police cir 4000000 conform-action transmit exceed-action drop
  account
 class prec2
  police cir 3500000 conform-action transmit exceed-action drop
  account
 class prec3
  account
  class class-default fragment prec4
  bandwidth remaining ratio 1
  account

policy-map main-interface
 class prec1
  priority level 1
  queue-limit 86 packets
 class prec2
  priority level 2
  queue-limit 78 packets
 class prec3
  bandwidth remaining ratio 1
  random-detect
  queue-limit 70 packets
  class prec4 service-fragment prec4
  shape average 200000
  bandwidth remaining ratio 1
  queue-limit 62 packets
class class-default
  queue-limit 80 packets
```

  Workaround: There is no workaround.

- CSCty73817

  Symptoms: In large-scale PPPoE sessions with QoS, the Standby RP might reboot continuously (until the workaround is applied) after switchover. This issue is seen when the QoS Policy Accounting feature is used. When the issue occurs, the Active RP remains operational and the Standby RP reboots with the following message:

```
  %PLATFORM-6-EVENT_LOG: 43 3145575308: *Mar 16 13:47:23.482: %QOS-6-RELOAD:
Index addition failed, reloading self
```

  Conditions: This symptom occurs when all the following conditions are met:

  1. There is a large amount of sessions.
  2. The QoS Policy Accounting feature is used.
  3. Switchover is done.

  Workaround: Bring down sessions before switchover. For example, shut down the physical interfaces that the sessions go through, or issue the Cisco IOS command **clear pppoe all**.

- CSCty76106

  Symptoms: A crash is seen after two days of soaking with traffic.

  Conditions: This symptom occurs with a node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, constant frequent polling of SNMP, RCMD, full scale of routes, and bidirectional traffic.

  Workaround: There is no workaround.

- CSCty77190

  Symptoms: DTLS is switched back to TLS after reconnect.

  Conditions: This symptom is observed with the following conditions:

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

  Workaround: Restart the AnyConnect client.

- CSCty78435

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

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

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

- CSCty84989

  Symptoms: IKEv2 pushed routes are not installed in the IPv6 inner VRF routing table.

  Conditions: This symptom occurs when using IKEv2 on pure IPV6 tunnels with tunnel protection IPsec and a VRF on the tunnel.

  Workaround: There is no workaround.

- CSCty85634

  Symptoms: A router configured with the Locator ID Separation Protocol (LISP) without an EID-table for the default VRF fails to maintain its LISP map-cache during an RP switchover. After the switchover, the existing remote EID entries in CEF eventually expire and new data packet signals result in repopulation of the LISP map-cache, thus resuming normal operation.

  Conditions: This symptom occurs in a LISP configuration that contains EID-tables for VRFs other than the default and does not contain an EID-table for the default VRF.

  Workaround: Configure an EID-table for the default VRF before the switchover with some LISP configuration such as “ipv4 itr”.

- CSCty86111

  Symptoms: The Cisco ISR G2 router crashes after “no ccm-manager fallback-mgcp” is configured.

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

  Workaround: There is no workaround.

- 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.

- 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.

- CSCtz08037

  Symptoms: The router fails to pass any traffic after receiving the “%OCE-3-OCE_FWD_STATE_HANDLE: Limit of oce forward state handle allocation reached; maximum allowable number is 50000” error message.

  Conditions: This symptom is observed MPLS L2VPN is configured with EoMPLSoGRE with IPSec encryption on top of the VTI tunnel with IPSec encryption (double encryption).

  Workaround: Reload the router.

- CSCtz15211

  Symptoms: The ISM card does not encrypt packets through a double encrypted tunnel.

Conditions: This symptom is observed with ISR g2 with the ISM module and crypto configured for GRE over IPsec packets to be encrypted through a VTI (double encryption).

Workaround: Use onboard encryption.

- CSCtz24280

  Symptoms: MSP flows are not identified.

  Conditions: This symptom is observed when “proxy-call-id” is present in the “Route” header of SIP packets.

  Workaround: Remove proxy servers from the topology.

- CSCtz25364

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

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

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

- CSCtz27137

  Symptoms: An upgrade to the S640 signature package may cause a Cisco IOS router to crash.

  Conditions: This symptom is observed in a Cisco 1841, 1941, and 2911 router running one of the following Cisco IOS versions:

  - Cisco IOS Release 12.4(24)T4
  - Cisco IOS Release 15.0(1)M4
  - Cisco IOS Release 15.0(1)M8
  - Cisco IOS Release 15.2(3)T

  Workaround: Update the signature package to anything less than S639. If already updated with any package larger than or equal to S639, follow the below steps to disable IPS:

  - Access the router via the console.
  - Enter break sequence to access ROMmon mode.
  - Change the config-register value to 0x2412.
  - Boot the router to bypass the startup-configuration.
  - Configure the basic IP parameters.
  - TFTP a modified configuration to the router’s running-configuration with Cisco IOS IPS disabled.
  - Reset the config-register to 0x2102.
  - Enter the **write memory** command and reload.

- CSCtz59429

  Symptoms: Packets do not match a flow with the attribute “application category voice-video”.

  Conditions: This symptom occurs when a flow with the attribute “application category voice-video” is matched for the same attribute.

  Workaround: There is no workaround.

- 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.

- CSCtz72390

  Symptoms: The name mangling functionality is broken. Authorization fails with the “IKEv2:AAA group author request failed” debug message.

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

  Workaround: There is no workaround.

- CSCtz85134

  Symptoms: A manually generated self-signed trustpoint gets erased and a new trustpoint is autogenerated when SSL-Express Accelerator is enabled and the router’s configuration is saved and it is reloaded.

  Conditions: This symptom is observed when the trustpoint is generated manually and SSL-Express Accelerator must be enabled. This issue is seen only when the configuration is saved and the router is reloaded.

  Workaround: Disable SSL-Express Accelerator.

- 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.

- CSCua22313

  Symptoms: SSLv3.0- and TLSv1.0-based data transfer using certain older client applications (like IE6) fails.

  Conditions: This symptom is observed when the HTTPS page is fetched by a client application that does not have a fix for the BEAST vulnerability (http://blogs.cisco.com/security/beat-the-beast-with-tls/) and the connection is optimized by SSL-Express Accelerator in WAAS-Express.

  Workaround: Upgrade the client application to the latest version or at least a version that has a fix for BEAST in case of Internet Explorer version 8 or higher.

- CSCua08883

  Symptoms: Tracebacks are seen in the Persaqos script.

  Conditions: This symptom is observed with the Persaqos script.

  Workaround: There is no workaround.

- CSCtz93002

  Symptoms: 117 images fail with the following error message:

  ```
  make-3.79.1-p7[3]: ***
  ```

```
[crypto/sub_subsys_crypto_ipsec_common.o/crypto_classify.o] Error 1
make-3.79.1-p7[2]: [CBSCONTEXT-obj-4k] Error 2 (ignored)
```

Conditions: This symptom is observed with an automatic merge.

Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(3)T

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

- CSCtx31294

  Symptoms: Anyconnect is unable to connect to the Cisco IOS headend (ISR-G2) when cert-based authentication is in use.

  Conditions: This symptom is observed with the following conditions:

  1. Cert-based authentication is configured using “authentication local rsa-sig” on the Cisco IOS headend.
  2. Remote authentication on the Cisco IOS headend can be EAP or rsa-sig. The Anyconnect client is unable to connect, and hence the tunnel is not established.

  Workaround: There is no workaround.

- 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.

- CSCty57085

  Symptoms: When accessing the Sharepoint present at HQ and downloading a file of 8.5 MB, the transaction time is more when compared to no WAAS.

  Conditions: This symptom is observed when there is a large amount of traffic.

  Workaround: There is no workaround.

- CSCty80566

  Symptoms: Cisco IOS crashes.

  Conditions: This symptom is observed with Cisco IOS during normal usage.

  Workaround: There is no workaround.

- CSCty90223

  Symptoms: A crash occurs at nhrp_nhs_recovery_co_destroy during setup and configuration.

  Conditions: This symptom is observed under the following conditions:

  1. Add and remove the ip nhrp configuration over the tunnel interface on the spoke multiple times.
  2. Do shut/no shut on the tunnel interface.

3. Rapidly change IPv6 addresses over the tunnel interface on the spoke side and on the hub side multiple times.
4. Replace the original (correct) IPv6 addresses on both the spoke and the hub.
5. 5) Wait for the registration timer to start.

The crash, while not consistently observed, is seen fairly often with the same steps.

Workaround: There is no known workaround.

Resolved Caveats—Cisco IOS Release 15.2(3)T

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

- CSCtj48387

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

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

  Workaround: There is no workaround.

- 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

- 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

- 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

- 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

- 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.

- CSCtt35379

  Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

  Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

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

- 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

- CSCtw73530

  Symptoms: Unable to delete metadata sessions.

  Conditions: This symptom is observed when more than 100 metadata sessions are created.

  Workaround: Disable metadata and then enable it. Note that this will remove all the flows.

- CSCtw99591

  Symptoms: *cpfrMCIndex* OID loops and does not increase.

  Conditions: This symptom is observed while doing a MIB walk.

  Workaround: Poll individual MIBs or walk around the PfR MIB.

- CSCtx04712

  Symptoms: Removal of crypto map hangs the router.

  Conditions: The symptom is observed following removal of “gdoi crypto map” from interface.

  Workaround: There is no workaround.

- CSCtx06801

  Symptoms: Certain websites may not load 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.

- CSCtx40818

  Symptoms: Traffic drops in a Cisco and displays the following error message:

```
%IP-3-LOOPPAK: Looping packet detected and dropped -
src=122.0.0.11, dst=121.0.0.11, hl=20, tl=40, prot=6, sport=80, dport=57894
```

  Conditions: This symptom is observed if the WAAS, NAT and firewall are enabled.

  Workaround: Disable WAAS.

- 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.

- CSCtx62790

  Symptoms: MSP chunks may increase causing memory depletion within 2 hrs of stress testing.

  Conditions: This symptom is observed due to a corner negative scenario. Here, MSP gets separated from the IXIA client. A “NO RTSP PLAY” error message displays which completes the call or causes session teardown. This symptom is observed even with other protcols having immature call states.

  Workaround: There is no workaround.

- CSCtx64210

  Symptoms: An unprotected debug message prints out on the console.

  Conditions: This symptom is observed during normal operation.

  Workaround: There is no workaround.

- CSCtx67290

  Symptoms: A Cisco Session Border Controller crashes when receiving an oversize rtcp-fb element in the SDP.

  Conditions: The symptom is observed when there is an oversize rctp-fb element in the SDP.

  Workaround: There is no workaround.

- CSCtx87939

  Symptoms: When the **Mediatrace Poll** command is invoked using WSMA interface, the “hops response received notifications” message is displayed. This message corrupts the WSMA output for the command.

  Conditions: This symptom is observed when Mediatrace poll is used in a WSMA interface.

  Workaround: There is no workaround.

- 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 following method 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.

- CSCtx92665

  Symptoms: Executing the **show mediatrace session stat** command causes a crash at *__be_sla_mt_route_data_print*.

  Conditions: This symptom is observed when **show mediatrace session stat** or **show mediatrace session data** is used.

  Workaround: There is no workaround.

- 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.

- CSCty07771

  Symptoms: CSCts55654 may cause extensive performance degradation.

  Conditions: This symptom is observed when normal QoS policy is applied on egress direction.

  Workaround: There is no workaround.

- CSCty13747

  Symptoms: Cisco Network Based Application Recognition (NBAR) applications with “engine-id=13” not shown or exported.

  Conditions: This symptom is observed while executing the **show flow exporter option application table** command.

  Workaround: The issue has been fixed.

- CSCty54728

  Symptoms: The **media-proxy** *{rsvp | metadata}* <*name*> command and its subcommands are not applied when a Cisco router reloads.

  Conditions: This symptom is observed when the **media-proxy** *{rsvp | metadata}* <*name*> command does not generate correct **show running-config** output.

  Workaround: Reload the router, and then configure the **media- proxy** *{rsvp | metadata}* <*name*> command and its subcommands.

- CSCty58300

  Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

  Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

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