Release Notes for the Cisco ASA Series, 9.7(x)

First Published: 2017-01-23

Last Modified: 2017-04-17

Release Notes for the Cisco ASA Series, 9.7(x)

This document contains release information for Cisco ASA software Version 9.7(x).

Important Notes

- If you are using SAML authentication with AnyConnect 4.4 or 4.5 and you deploy ASA version 9.7.1.24, 9.8.2.28, or 9.9.2.1 (Release Date: 18-APR-2018), the defaulted SAML behavior is the embedded browser, which is not supported on AnyConnect 4.4 and 4.5. Therefore, you must enable the **saml external-browser** command in tunnel group configuration in order for AnyConnect 4.4 and 4.5 clients to authenticate with SAML using the external (native) browser.

  Note The **saml external-browser** command is for migration purposes for those upgrading to AnyConnect 4.6 or later. Because of security limitations, use this solution only as part of a temporary migration while upgrading AnyConnect software. The command itself will be depreciated in the future.

- Potential Traffic Outage (9.7(1) through 9.7(1.2))—Due to bug CSCvd78303, the ASA may stop passing traffic after 213 days of uptime. The effect on each network will be different, but it could range from an issue of limited connectivity to something more extensive like an outage. You must upgrade to a new version without this bug, when available. In the meantime, you can reboot the ASA to gain another 213 days of uptime. Other workarounds may be available. See Field Notice FN-64291 for affected versions and more information.

- AnyConnect remote access VPN IPv6 DTLS tunnels in a scaled/stress environment may cause the ASA to traceback (for example: you have a large number of tunnels; or tunnels are continually connecting and disconnecting from the ASA headend). **Workaround**: Use IPv6 AnyConnect IKEv2 or IPv4 AnyConnect DTLS VPN remote access session types. (CSCvc77123)

- The RSA toolkit version used in ASA 9.x is different from what was used in ASA 8.4, which causes differences in PKI behavior between these two versions.

  For example, ASAs running 9.x software allow you to import certificates with an Organizational Name Value (OU) field length of 73 characters. ASAs running 8.4 software allow you to import certificates with an OU field name of 60 characters. Because of this difference, certificates that can be imported in ASA 9.x will fail to be imported to ASA 8.4. If you try to import an ASA 9.x certificate to an ASA running version 8.4, you will likely receive the error, "ERROR: Import PKCS12 operation failed.

- When the ASA acts as a TLS server in a TLS proxy configuration, if the client proposes the TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 or

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ciphers and those are chosen, the TLS handshake might fail. You cannot control the cipher selection when the ASA acts as a server in this release, as there is a bug whereby the global **ssl encryption** command no longer takes effect as the default set of ciphers. In 9.8(1), you can use the new **server cipher-suite** command in the TLS proxy configuration to control the cipher. If you encounter this problem, please upgrade to 9.8(1). Alternatively, you can change the configuration of the client so that it does not propose those ciphers.

System Requirements

This section lists the system requirements to run this release.

ASA and ASDM Compatibility

For information about ASA/ASDM software and hardware requirements and compatibility, including module compatibility, see Cisco ASA Compatibility.

VPN Compatibility

For VPN compatibility, see Supported VPN Platforms, Cisco ASA 5500 Series.

New Features

This section lists new features for each release.

Note New, changed, and deprecated syslog messages are listed in the syslog message guide.

New Features in ASA 9.7(1.4)

Released: April 4, 2017

Note Verion 9.7(1) was removed from Cisco.com due to bug CSCvd78303.

Feature	Description
Platform Features	

Feature	Description
New default configuration for the ASA 5506-X series using Integrated Routing and Bridging	A new default configuration will be used for the ASA 5506-X series. The Integrated Bridging and Routing feature provides an alternative to using an external Layer 2 switch. For users replacing the ASA 5505, which includes a hardware switch, this feature lets you replace the ASA 5505 with an ASA 5506-X or other ASA model without using additional hardware. The new default configuration includes: • outside interface on GigabitEthernet 1/1, IP address from DHCP • inside bridge group BVI 1 with GigabitEthernet ½ (inside1) through 1/8 (inside7), IP address 192.168.1.1 • inside --> outside traffic flow • inside ---> inside traffic flow for member interfaces • (ASA 5506W-X) wifi interface on GigabitEthernet 1/9, IP address 192.168.10.1 • (ASA 5506W-X) wifi <--> inside, wifi --> outside traffic flow • DHCP for clients on inside and wifi. The access point itself and all its clients use the ASA as the DHCP server. • Management 1/1 interface is Up, but otherwise unconfigured. The ASA FirePOWER module can then use this interface to access the ASA inside network and use the inside interface as the gateway to the Internet. • ASDM access—inside and wifi hosts allowed. • NAT—Interface PAT for all traffic from inside, wifi, and management to outside. If you are upgrading, you can either erase your configuration and apply the default using the **configure factory-default** command, or you can manually configure a BVI and bridge group members to suit your needs. Note that to easily allow intra-bridge group communication, you need to enable the **same-security-traffic permit inter-interface** command (this command is already present for the ASA 5506W-X default configuration).
Alarm ports support on the ISA 3000	The ISA 3000 supports two alarm input interfaces and one alarm out interface. External sensors such as door sensors can be connected to the alarm inputs. External devices like buzzers can be connected to the alarm out interface. Alarms triggered are conveyed through two LEDs, syslogs, SNMP traps, and through devices connected to the alarm out interface.You can configure descriptions of external alarms. You can also specify the severity and trigger, for external and internal alarms. All alarms can be configured for relay, monitoring and logging. We introduced the following commands: **alarm contact description, alarm contact severity, alarm contact trigger, alarm facility input-alarm, alarm facility power-supply rps, alarm facility temperature, alarm facility temperature high, alarm facility temperature low, clear configure alarm, clear facility-alarm output, show alarm settings, show environment alarm-contact**.

Feature	Description
Microsoft Azure Security Center support on the ASAv10	Microsoft Azure is a public cloud environment that uses a private Microsoft Hyper V Hypervisor. Microsoft Azure Security Center is a Microsoft orchestration and management layer on top of Azure that simplifies the deployment of a highly secure public cloud infrastructure. Integration of the ASAv into Azure Security Center allows the ASAv to be offered as a firewall option to protect Azure environments.

Precision Time Protocol (PTP) for the ISA 3000	The ISA 3000 supports PTP, a time synchronization protocol for nodes distributed across a network. It provides greater accuracy than other time synchronization protocols, such as NTP, due to its hardware timestamp feature. The ISA 3000 supports PTP forward mode, as well as the one-step, end-to-end transparent clock. We added the following commands to the default configuration to ensure that PTP traffic is not sent to the ASA FirePOWER module for inspection. If you have an existing deployment, you need to manually add these commands:
	
	`object-group service bypass_sfr_inspect`
	`  service-object udp destination range 319 320`
	`access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any`
	
	We introduced the following commands: **debug ptp, ptp domain, ptp mode e2etransparent, ptp enable, show ptp clock, show ptp internal-info, show ptp port**

Automatic Backup and Restore for the ISA 3000	You can enable auto-backup and/or auto-restore functionality using pre-set parameters in the backup and restore commands. The use cases for these features include initial configuration from external media; device replacement; roll back to an operable state. We introduced the following commands: **backup-package location, backup-package auto, show backup-package status, show backup-package summary**
Firewall Features	
Support for SCTP multi-streaming reordering and reassembly and fragmentation. Support for SCTP multi-homing, where the SCTP endpoints have more than one IP address.	The system now fully supports SCTP multi-streaming reordering, reassembly, and fragmentation, which improves Diameter and M3UA inspection effectiveness for SCTP traffic. The system also supports SCTP multi-homing, where the endpoints have more than one IP address each. For multi-homing, the system opens pinholes for the secondary addresses so that you do not need to write access rules to allow them. SCTP endpoints must be limited to 3 IP addresses each. We modified the output of the following command: **show sctp detail**.
M3UA inspection improvements.	M3UA inspection now supports stateful failover, semi-distributed clustering, and multihoming. You can also configure strict application server process (ASP) state validation and validation for various messages. Strict ASP state validation is required for stateful failover and clustering. We added or modified the following commands: **clear service-policy inspect m3ua session** [**assocID** *id*], **match port sctp**, **message-tag-validation**, **show service-policy inspect m3ua drop**, **show service-policy inspect m3ua endpoint**, **show service-policy inspect m3ua session**, **show service-policy inspect m3ua table**, **strict-asp-state**, **timeout session**.
Support for TLSv1.2 in TLS proxy and Cisco Unified Communications Manager 10.5.2.	You can now use TLSv1.2 with TLS proxy for encrypted SIP or SCCP inspection with the Cisco Unified Communications Manager 10.5.2. The TLS proxy supports the additional TLSv1.2 cipher suites added as part of the **client cipher-suite** command. We modified the following commands: **client cipher-suite**

Feature	Description
Integrated Routing and Bridging	Integrated Routing and Bridging provides the ability to route between a bridge group and a routed interface. A bridge group is a group of interfaces that the ASA bridges instead of routes. The ASA is not a true bridge in that the ASA continues to act as a firewall: access control between interfaces is controlled, and all of the usual firewall checks are in place. Previously, you could only configure bridge groups in transparent firewall mode, where you cannot route between bridge groups. This feature lets you configure bridge groups in routed firewall mode, and to route between bridge groups and between a bridge group and a routed interface. The bridge group participates in routing by using a Bridge Virtual Interface (BVI) to act as a gateway for the bridge group. Integrated Routing and Bridging provides an alternative to using an external Layer 2 switch if you have extra interfaces on the ASA to assign to the bridge group. In routed mode, the BVI can be a named interface and can participate separately from member interfaces in some features, such as access rules and DHCP server. The following features that are supported in transparent mode are not supported in routed mode: multiple context mode, ASA clustering. The following features are also not supported on BVIs: dynamic routing and multicast routing. We modified the following commands: **access-group, access-list ethertype, arp-inspection, dhcpd, mac-address-table static, mac-address-table aging-time, mac-learn, route, show arp-inspection, show bridge-group, show mac-address-table, show mac-learn**
VM Attributes	You can define network objects to filter traffic according to attributes associated with one or more Virtual Machines (VMs) in an VMware ESXi environment managed by VMware vCenter. You can define access control lists (ACLs) to assign policies to traffic from groups of VMs sharing one or more attributes. We added the following command: **show attribute**.
Stale route timeout for interior gateway protocols	You can now configure the timeout for removing stale routes for interior gateway protocols such as OSPF. We added the following command: **timeout igp stale-route**.
Network object limitations for object group search.	You can reduce the memory required to search access rules by enabling object group search with the the **object-group-search access-control** command. When enabled, object group search does not expand network or service objects, but instead searches access rules for matches based on those group definitions. Starting with this release, the following limitation is applied: For each connection, both the source and destination IP addresses are matched against network objects. If the number of objects matched by the source address times the number matched by the destination address exceeds 10,000, the connection is dropped. This check is to prevent performance degradation. Configure your rules to prevent an excessive number of matches.
Routing Features	

Feature	Description
31-bit Subnet Mask	For routed interfaces, you can configure an IP address on a 31-bit subnet for point-to-point connections. The 31-bit subnet includes only 2 addresses; normally, the first and last address in the subnet is reserved for the network and broadcast, so a 2-address subnet is not usable. However, if you have a point-to-point connection and do not need network or broadcast addresses, a 31-bit subnet is a useful way to preserve addresses in IPv4. For example, the failover link between 2 ASAs only requires 2 addresses; any packet that is transmitted by one end of the link is always received by the other, and broadcasting is unnecessary. You can also have a directly-connected management station running SNMP or Syslog. This feature is not supported with BVIs for bridge groups or multicast routing. We modified the following commands: **ip address, http, logging host, snmp-server host, ssh**
High Availability and Scalability Features	
Inter-site clustering improvement for the ASA on the Firepower 4100/9300 chassis	You can now configure the site ID for each Firepower 4100/9300 chassis when you deploy the ASA cluster. Previously, you had to configure the site ID within the ASA application; this new feature eases initial deployment. Note that you can no longer set the site ID within the ASA configuration. Also, for best compatibility with inter-site clustering, we recommend that you upgrade to ASA 9.7(1) and FXOS 2.1.1, which includes several improvements to stability and performance. We modified the following command: **site-id**
Director localization: inter-site clustering improvement for data centers	To improve performance and keep traffic within a site for inter-site clustering for data centers, you can enable director localization. New connections are typically load-balanced and owned by cluster members within a given site. However, the ASA assigns the director role to a member at *any* site. Director localization enables additional director roles: a local director at the same site as the owner, and a global director that can be at any site. Keeping the owner and director at the same site improves performance. Also, if the original owner fails, the local director chooses a new connection owner at the same site. The global director is used if a cluster member receives packets for a connection that is owned on a different site. We introduced or modified the following commands: **director-localization, show asp table cluster chash, show conn, show conn detail**
Interface link state monitoring polling for failover now configurable for faster detection	By default, each ASA in a failover pair checks the link state of its interfaces every 500 msec. You can now configure the polling interval, between 300 msec and 799 msec; for example, if you set the polltime to 300 msec, the ASA can detect an interface failure and trigger failover faster. We introduced the following command: **failover polltime link-state**
Bidirectional Forwarding Detection (BFD) support for Active/Standby failover health monitoring on the Firepower 9300 and 4100	You can enable Bidirectional Forwarding Detection (BFD) for the failover health check between two units of an Active/Standby pair on the Firepower 9300 and 4100. Using BFD for the health check is more reliable than the default health check method and uses less CPU. We introduced the following command: **failover health-check bfd**
VPN Features	

Feature	Description
Dynamic RRI for IKEv2 static crypto maps	Dynamic Reverse Route Injection occurs upon the successful establishment of IPsec Security Associations (SA's) when **dynamic** is specified for a **crypto map**. Routes are added based on the negotiated selector information. The routes will be deleted after the IPsec SA's are deleted. Dynamic RRI is supported on IKEv2 based static crypto maps only. We modified the following command: **crypto map set reverse-route**.
Virtual Tunnel Interface (VTI) support for ASA VPN module	The ASA VPN module is enhanced with a new logical interface called Virtual Tunnel Interface (VTI), used to represent a VPN tunnel to a peer. This supports route based VPN with IPsec profiles attached to each end of the tunnel. Using VTI does away with the need to configure static crypto map access lists and map them to interfaces. We introduced the following commands: **crypto ipsec profile, interface tunnel, responder-only, set ikev1 transform-set, set pfs, set security-association lifetime, tunnel destination, tunnel mode ipsec, tunnel protection ipsec profile, tunnel source interface**.
SAML 2.0 based SSO for AnyConnect	SAML 2.0-based service provider IdP is supported in a private network. With the ASA as a gateway between the user and services, authentication on IdP is handled with a restricted anonymous webvpn session, and all traffic between IdP and the user is translated. We added the following command: **saml idp** We modified the following commands: **debug webvpn saml, show saml metadata**
CMPv2	To be positioned as a security gateway device in wireless LTE networks, the ASA now supports certain management functions using the Certificate Management Protocol (CMPv2). We modified the following commands: **enrollment url, keypair, auto-update, crypto-ca-trustpoint, show crypto ca server certificates, show crypto key, show tech-support**
Multiple certificate authentication	You can now validate multiple certificates per session with AnyConnect SSL and IKEv2 client protocols. The Aggregate Authentication protocol has been extended to define the protocol exchange for multiple-certificate authentication and utilize this for both session types. We modified the following command: **authentication {[aaa] [certificate | multiple-certificate] | saml}**
Increase split-tunneling routing limit	The limit for split-tunneling routes for AC-SSL and AC-IKEv2 was increased from 200 to 1200. The IKEv1 limit was left at 200.
Smart Tunnel Support on Chrome	A new method for smart-tunnel support in the Chrome browser on Mac and Windows devices was created. A Chrome Smart Tunnel Extension has replaced Netscape Plugin Application Program Interfaces (NPAPIs) that are no longer supported on Chrome. If you click on the smart tunnel enabled bookmark in Chrome without the extension already being installed, you are redirected to the Chrome Web Store to obtain the extension. New Chrome installations will direct the user to the Chrome Web Store to download the extension. The extension downloads the binaries from ASA that are required to run smart tunnel. Your usual bookmark and application configuration while using smart tunnel is unchanged other than the process of installing the new extension.
Clientless SSL VPN: Session information for all web interfaces	All web interfaces will now display details of the current session, including the user name used to login, and user privileges which are currently assigned. This will help the user be aware of the current user session and will improve user security.

Feature	Description
Clientless SSL VPN: Validation of all cookies for web applications' sessions	All web applications will now grant access only after validating all security-related cookies. In each request, each cookie with an authentication token or a session ID will be verified before granting access to the user session. Multiple session cookies in the same request will result in the connection being dropped. Cookies with failed validations will be treated as invalid and the event will be added to the audit log.
AnyConnect: Maximum Connect Time Alert Interval is now supported in the Group Policy for AnyConnect VPN Client connections.	The alert interval is the interval of time before max connection time is reached that a message will be displayed to the user warning them of termination. Valid time interval is 1-30 minutes. Default is 30 minutes. Previously supported for clientless and site-to-site VPN connections. The following command can now be used for AnyConnect connections: **vpn-session-timeout alert-interval**
AAA Features	
IPv6 address support for LDAP and TACACS+ Servers for AAA	You can now use either IPv4 or IPv6 addresses for LDAP and TACACS+ servers used for AAA. We modified the following command: **aaa-server host, test aaa-server**
Administrative Features	
PBKDF2 hashing for all local **username** and **enable** passwords	Local **username** and **enable** passwords of all lengths are stored in the configuration using a PBKDF2 (Password-Based Key Derivation Function 2) hash. Previously, passwords 32 characters and shorter used the MD5-based hashing method. Already existing passwords continue to use the MD5-based hash unless you enter a new password. See the "Software and Configurations" chapter in the General Operations Configuration Guide for downgrading guidelines. We modified the following commands: **enable password, username**
Licensing Features	
Licensing changes for failover pairs on the Firepower 4100/9300 chassis	Only the active unit requests the license entitlements. Previously, both units requested license entitlements. Supported with FXOS 2.1.1.
Monitoring and Troubleshooting Features	
IPv6 address support for traceroute	The **traceroute** command was modified to accept an IPv6 address. We modified the following command: **traceroute**
Support for the packet tracer for bridge group member interfaces	You can now use the packet tracer for bridge group member interfaces. We added two new options to the **packet-tracer** command; **vlan-id** and **dmac**
IPv6 address support for syslog servers	You can now configure syslog servers with IPv6 addresses to record and send syslogs over TCP and UDP. We modified the following commands: **logging host, show running config, show logging**

Feature	Description
SNMP OIDs and MIBs	The ASA now supports SNMP MIB objects corresponding to the end-to-end transparent clock mode as part of the Precision Time Protocol (PTP) for the ISA 3000. The following SNMP MIB objects are supported: • ciscoPtpMIBSystemInfo • cPtpClockDefaultDSTable • cPtpClockTransDefaultDSTable • cPtpClockPortTransDSTable
Manually stop and start packet captures	You can now manually stop and start the capture. Added/Modified commands: **capture stop**

Upgrade the Software

This section provides the upgrade path information and a link to complete your upgrade.

ASA Upgrade Path

To view your current version and model, use one of the following methods:

- CLI—Use the **show version** command.
- ASDM—Choose **Home** > **Device Dashboard** > **Device Information**.

See the following table for the upgrade path for your version. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

Current Version	Interim Upgrade Version	Target Version
9.6(x)	—	Any of the following: → 9.7(x) → 9.6(x)
9.5(x)	—	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x)

Current Version	Interim Upgrade Version	Target Version
9.4(x)	—	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x)
9.3(x)	—	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x)
9.2(x)	—	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x)
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4)	—	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
9.1(1)	→ 9.1(2)	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.0(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.5(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.4(5+)	—	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.4(1) through 8.4(4)	Any of the following: → 9.0(2), 9.0(3), or 9.0(4) → 8.4(6)	→ 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.3(x)	→ 8.4(6)	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.2(x) and earlier	→ 8.4(6)	Any of the following: → 9.7(x) → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Upgrade Link

To complete your upgrade, see the ASA upgrade guide.

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account. If you do not have a Cisco support contract, you can only look up bugs by ID; you cannot run searches.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Bugs in Version 9.7(x)

If you have a Cisco support contract, use the following dynamic search for all open bugs severity 3 and higher for Version 9.7(x):

- 9.7 open bug search.

The following table lists open bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCto19832	OpenLDAP needs to be upgraded or patched
CSCva72318	XMLSoft libxml2 XML Content Processing External Entity Expansion Vulne
CSCva72319	XMLSoft libxml2 Format String Vulnerability
CSCvc11628	Pre-fill feature extracts username from wrong cert (cert 1-machine) for double cert vs.(cert 2-user)
CSCvc12313	cURL and libcurl Cookie Handling Content Injection Vulnerability
CSCvc12314	cURL and libcurl Authentication Handling Session Reuse Vulnerability
CSCvc12315	cURL and libcurl Encoding Out-of-Bounds Memory Write Vulnerability
CSCvc12316	cURL and libcurl curl_maprintf Function Memory Double-Free Vulnerabili
CSCvc12317	cURL and libcurl Kerberos Authentication Processing Memory Double-Free
CSCvc12318	cURL and libcurl Character Processing URL Redirection Vulnerability
CSCvc31687	cURL and libcurl curl_getdate Function Out of Bounds Memory Read Vulne
CSCvc31688	cURL and libcurl curl_easy_unescape Function Heap Overflow Vulnerabili
CSCvc31689	cURL and libcurl Shared Cookie Handling Use-After-Free Vulnerability
CSCvc31690	Python smtplib StartTLS Man-in-the-Middle Vulnerability
CSCvc53140	OSPF retransmissions and VPN tunnels lost after Active ASA reload

Caveat ID Number	Description
CSCvc77123	ASA may traceback in network_tcpmod_close_conn with AnyConnect IPv6 DTLS stress scenario

Resolved Bugs in Version 9.7(1.4)

The following table lists select resolved bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCsh75522	Increase Content-length counter from 4 to 8 byte size
CSCtw90511	Packet captures cause CPU spike on Multi-Core platforms due to spin_lock
CSCuh89500	ASA: ifSpeed/ifHighSpeed not populated by SNMP for port-channel
CSCum28756	ASA: Auth failures for SNMPv3 polling after unit rejoins cluster
CSCum70304	FIPS self test power on fails - fipsPostDrbgKat
CSCum74032	ASA traceback on standby when SNMP polling
CSCun16158	Cisco ASA Software IPsec Denial of Service Vulnerability
CSCup37416	Stale VPN Context entries cause ASA to stop encrypting traffic
CSCup96099	"show resource usage detail counter all 1" causes cpu hog
CSCuq80704	ASA classifies TCP packets as PAWS failure incorrectly
CSCus29600	dhcprelay interface doesn't change by changing route
CSCus37458	ASA traceback in Thread name DATAPATH when handling multicast packet
CSCut07712	ASA - TO the box traffic break due to int. missing in asp table routing
CSCuu50708	ASA Traceback on 9.1.5.19
CSCuu54582	ASA-SFR, ASA should attempt to join Cluster after SFR service module up
CSCuv09640	ASA: "Auto-Enable" feature not working with SSH configured with PKF
CSCuv61791	CWS redirection on ASA may corrupt sequence numbers with https traffic
CSCuv86562	Traceback: ASA crash in thread name fover_health_monitoring_thread
CSCuw71147	Traceback in Unicorn Proxy Thread, in http_header_by_name
CSCuw88759	ASA: Protocol and Status showing UP without connecting the interface
CSCuw95262	After some time flash operations fail and configuration can not be saved
CSCux08783	CWS: ASA does not append XSS headers
CSCux08838	ASA: Traceback in Checkheaps

Caveat ID Number	Description
CSCux10499	Smart Tunnel starts and Java closes without any message
CSCux11440	ASA traceback in Unicorn Proxy Thread
CSCux13612	On failover, new standby unit reports out of stack memory
CSCux15273	show memory indicates inaccurate free memory available
CSCux17527	ASA memory leak related to Botnet
CSCux18455	SNMP: Memory Leak Walking CISCO-ENHANCED-MEMPOOL-MIB
CSCux29842	Primary and Secondary ASA in HA is traceback in Thread Name:DataPath
CSCux29929	ASA 9.4.2 traceback in DATAPATH
CSCux35538	Traceback in ctm_ssl_generate_key with DHE ciphers SSL VPN scaled test
CSCux39988	Different output of BVI address in transparent mode on failover pair
CSCux58172	DAP: debug dap trace not fully shown after +1600 lines
CSCux66866	Traffic drop due to constant amount of arp on ASASM
CSCux71197	"show resource usage" gives wrong number of routes after shut/no sh
CSCux82023	Stub Connections Torn Down due to Shun/Threat Detection in ASA Cluster
CSCux82835	Nat pool exhausted observed when enabling asp transactional-commit nat
CSCux83705	DNS Reply Modification for Dual-Stack does not work as expected
CSCux86769	VLAN mapping doesn't work when connection falls back to TLS
CSCux92157	ASA Traceback Assert in Thread Name: ssh_init with component ssh
CSCux94598	ASA using a huge dynamic ACL may cause Anyconnect connectivity failures
CSCux95670	ASA denies to-the-box traffic intended to CX
CSCux96716	ASA tracebacks when replicating Xlate to the standby/slave
CSCux98029	ASA reloads with traceback in thread name DATAPATH or CP Processing
CSCux99214	ASA5516 SSD reports incorrect OID in Entity MIB
CSCux99392	Uploaded/downloaded files via CIFS have Zero Byte size (same WebFolder)
CSCuy00215	Update WR OS to RCPL 27
CSCuy00296	Traceback in Thread: IPsec message handler
CSCuy05949	ASA: MAC address changes on active context when WRITE STANDBY is issued
CSCuy06125	Re-adding context creates context without configs on some slaves

Caveat ID Number	Description
CSCuy07753	Smart tunnel does not work since Firefox 32bit version 43
CSCuy08051	9.5(1) ECDSA CSR sets KU KeyEnciph vice KeyAgreement
CSCuy10665	HA: Number of interfaces mismatch after SFR module reload on both units
CSCuy11281	ASA: Assert traceback in version 9.4.2
CSCuy12786	Mem leak on active ASA after executing write st then logoff repeatedly
CSCuy15636	ASA may traceback with: DATAPATH-9-3101/DATAPATH-7-3145/DATAPATH-3-1685
CSCuy15798	Add support for IPv6 assigned address field in Radius Accounting packet
CSCuy19933	ASA rewriter incorrectly handle HTML code of type <base>xxx</base>
CSCuy21206	Traceback when drop is enabled with diameter inspection and tls-proxy
CSCuy21287	STBY ASA does't pass traffic via ASA-IC-6GE-SFP-B ifc after reload
CSCuy22155	ASA generates unexpected syslog messages with mcast routing disabled
CSCuy22561	VPN Load-Balancing does not send load-balancing cert for IPv6 Address
CSCuy25163	Cisco ASA ACL ICMP Echo Request Code Filtering Vulnerability
CSCuy27428	ASA traceback in thread name snmp after upgrade to 9.1(7)
CSCuy32321	Traceback in ldap_client_thread with ldap attr mapping and pw-mgmt
CSCuy32728	VPN LB stops working when cluster encryption is configured
CSCuy32964	ASA Crash on cluster member or on standby member of failover pair after replication of conns
CSCuy34265	ASA Access-list missing and losing elements after configuration change
CSCuy36897	Can't navigate to OWA 2013 due to ssl errors
CSCuy39186	IKEv2 S2S tunnel does not come up because previous sa not deleted
CSCuy40207	Traceback: assertion "0" failed: file "ctm_daemon.c"
CSCuy41986	OCSP validation fails when multiple certs in chain are verified
CSCuy42087	ASA: Not able to remove ACE with "log default" keyword
CSCuy42223	BGP:Deployment failed with reason supported on management-only interface
CSCuy43438	L2TP over IPSec can not be connected after disconnection from client.
CSCuy43540	SNMP Syslog Traps are not RFC3164 Compliant for the TAG (Mnemonic) Field
CSCuy43839	ASA reloads in thread name: DATAPATH while encrypting L2L packet

Caveat ID Number	Description
CSCuy43857	ASA WebVPN: Java Exception with Kronos application
CSCuy44472	BVI : Interface IPv6 address deleted from standby context on HA - A/A
CSCuy45475	ASA : Configuration not replicated on mate if standby IP is missing
CSCuy47545	http config missing in multicontext after reload of stdby 916.9 or later
CSCuy47706	Traceback at gtpv1_process_pdp_create_req
CSCuy49291	Number of routes in the active and standby units are not same
CSCuy50406	Crash in proxyi_rx_q_timeout_timer
CSCuy51918	Buffer overflow in RAMFS dirent structure causing traceback
CSCuy53516	ASA corrupts data in TLS-Proxy with TLS version 1.2
CSCuy54567	Evaluation of pix-asa for OpenSSL March 2016
CSCuy55468	Unicorn Proxy Thread causing CP contention
CSCuy57644	ASAv sub-interface failing to send traffic with customised mac-address
CSCuy58084	Unable to configure a user for ssh public auth only (tied w/ CSCuw90580)
CSCuy60320	IPv6 Routes not installed on QP
CSCuy60793	Duplicate link-local address observed after failover
CSCuy62198	If FQDN is more than 64 chars then we redirect to ip instead of FQDN
CSCuy63642	ASA 9.1(6) traceback processing outbound DTLS Packet
CSCuy66942	Cisco ASA Software DHCP Relay Denial of Service vulnerability
CSCuy67333	SIP call transfer fail due to differences b/w fixing CallId and Refer-To
CSCuy73652	Traceback in thread name idfw when modifying object-group having FQDN
CSCuy74218	Assert Traceback in Thread Name: DATAPATH on clustered packet reassembly
CSCuy74362	WebVPN FTP client failing with "Error contacting host" message
CSCuy78802	orignial master not defending all GARP packets after cluster split brain
CSCuy79453	Threat-detection: expired shun hosts remain in some ifcs in tfw mode
CSCuy80058	FO replication failed: cmd=no disable, when disabling webvpn-cache
CSCuy80070	OSPF routes not populating over L2L tunnel
CSCuy80830	ASA failed to allow tcp traffic from inside to outside
CSCuy82905	ASA crashes when global access-list config is cleared

Caveat ID Number	Description
CSCuy84044	Rewriter error with webworker JS
CSCuy85243	ASA traceback when receive Radius attribute with improper variable type
CSCuy86333	BFD: ASA might traceback in snp_bfd_pp_process+101
CSCuy87597	ASA - Traceback in CP Processing Thread During Private Key Decryption
CSCuy88971	ASA does not suppress EIGRP candidate default route information
CSCuy89288	AnyConnect DTLS on-demand DPDs are not sent intermittently
CSCuy89425	AAA: RSA/SDI unable to set new PIN
CSCuy90936	ASA may stop responding to OSPF Hello packets
CSCuy91405	ASA should not load-balance same flow traffic over port-channel CCL
CSCuy93102	show running-config doesn't display any threat-detection commands
CSCuy94591	ASA inconsistent logs about Connection limit exceeded
CSCuy95543	Improve efficiency of malloc_avail_freemem()
CSCuy98769	Slow ASA OSPF interface transition from DOWN to WAITING after failover
CSCuy99280	ENH: ASAv should have a different pre-loaded cert
CSCuz00077	ASA 9.1.6.4 traceback with Thread Name: telnet/ci
CSCuz00778	IKEv2 tunnel gets re-established intermittently after a IPSec rekey
CSCuz04385	IPSec rekey collision handling failure cases IKE tunnel drop
CSCuz04534	Memory leak in 112 byte bin when packet hits PBR and WCCP rules
CSCuz06125	Active and Standby ASA use same MAC addr with only active MAC configured
CSCuz06153	Incorrect msg shown when configuring MAC addr same as already configured
CSCuz06499	WebVPN: Webpage not fully rewritten when ASA has the same FQDN as srv
CSCuz09255	ASA does not respond to NS in Active/Active HA
CSCuz09394	infinite loop in JS rewriter state machine when return followed by var
CSCuz10371	ASA Traceback and reload by strncpy_sx.c
CSCuz11685	Cisco ASA Software Internet Key Exchange Version 1 XAUTH Denial of Service Vulnerability
CSCuz14600	Kenton 9.5.1'boot system/boot config' commands not retained after reload
CSCuz14808	5585-10 traceback in Thread Name: idfw_proc

Caveat ID Number	Description
CSCuz16398	Incorrect modification of NAT divert table.
CSCuz16498	Error messages on console "ERROR: Problem with interface "
CSCuz16565	9.6.2 EST - assertion "0" failed: file "snp_vxlan.c"
CSCuz21068	CSCOPut_hash can initiate unexepected requests
CSCuz21178	ASA traceback in threadname ssh
CSCuz22618	MH/MS:Observed traceback - mh->mh_mem_pool < MEMPOOL_MAX_TYPE
CSCuz23354	CPU usage is high after timer dequeue failed in GTP
CSCuz23576	Allocated memory showing high (invalid) values
CSCuz27165	BTF is not blocking blacklisted domain with more than 2 labels in it
CSCuz28000	Context config may get rejected if all the units in Cluster reloaded
CSCuz30425	Network command disappears from BGP after reload with name
CSCuz33255	Traceback in IKEv2 Daemon with 20+ second CPU hog.
CSCuz34753	ASA QOS fails to classify packets between priority and best effort queue
CSCuz36545	Drop down menu doesn't work on Simfosia web page
CSCuz36938	Traceback on editing a network object on exceeding the max snmp hosts
CSCuz38115	ASA Tback when large ACL applied to interface with object-group-search
CSCuz38180	ASA: Page Fault traceback in DATAPATH on standby ASA after booting up
CSCuz38703	ASA capture type isakmp saving malformed ISAKMP packets
CSCuz38888	WebVPN rewrite fails for MSCA Cert enrollment page / VBScript
CSCuz40081	ASA memory leak due to vpnfo
CSCuz41033	dynamic crypto map fails if named the same as static crypto map
CSCuz42390	ASA Stateful failover for DRP works intermittently
CSCuz42986	ASA(HA) doesn't send RST packets when sfr module shutdown
CSCuz44687	Traceback data path self deadlock panic while attempt to get spin lock
CSCuz44968	Commands not installed on Standby due to parser switch
CSCuz50929	Many "show blocks" outputs have truncated PC values with ASLR
CSCuz52474	Evaluation of pix-asa for OpenSSL May 2016
CSCuz53273	Captive-portal code should not be invoked when CX card is present

Caveat ID Number	Description
CSCuz54193	ASA: Traceback on ASA in Datapath as we enable SFR traffic redirection
CSCuz54545	ASA Address not mapped traceback - configuring snmp-server host
CSCuz58142	ASA Access-list missing and losing elements Warning Message enhancement
CSCuz60555	ASA-2-321006 May be received invalidly when memory is not high
CSCuz61092	Interface health-check failover causes OSPF not to advertise ASA as ABR
CSCuz63531	Observing Memory corruption, assert for debug ospf
CSCuz64603	GTP traceback at gtp_update_sig_conn_timestamp while processing data
CSCuz64784	ASA traceback in DATAPATH on all cluster units during context removal
CSCuz66269	SCP Client not allow to enter password with "no ssh stricthostkeycheck"
CSCuz66661	ASA Cut-through Proxy inactivity timeout not working
CSCuz67349	ASA Cluster fragments reassembled before transmission with no inspection
CSCuz67590	ASA may Traceback with Thread Name: cluster rx thread
CSCuz67596	ASA may Traceback with Thread Name: Unicorn Admin Handler
CSCuz67690	ASA crashed due to Election severe problem no master is promoted
CSCuz68940	Crypto ca trustpool import does not fall back to data routing table
CSCuz70330	ASA: SSH being denied on the ASA device as the maximum limit is reached
CSCuz72244	Error Indication dropped with Null TID MBReq dropped with no Ctrl F-TEID
CSCuz72352	traceback during tls-proxy handshake
CSCuz77818	PIM BiDir DF Elections stuck in "offer" state on some interfaces
CSCuz79800	ASA cant delete ACL lines and remarks - Specified remark does not exist
CSCuz80281	IPv6 neighbor discovery packet processing behavior
CSCuz87146	nat-t-disable feature is not working for ikev2
CSCuz89989	Ikev1 tunnel drops with reason " Peer Address Changed"
CSCuz90648	2048/1550/9344 Byte block leak cause traffic disruption & module failure
CSCuz92074	ASA with PAT fails to untranslate SIP Via field that doesnt contain port
CSCuz92921	ASA crashes while clearing global access-list
CSCuz93626	Inspect-mmp configuration is missing in latest branches.
CSCuz94158	Hash miscalculation for "Any" address on inside

Caveat ID Number	Description
CSCuz94862	IKEv2: Data rekey collisions can cause inactive IPsec SAs to get stuck
CSCuz94890	ASAv ACKs FIN before all data is received during smart licensing exch
CSCuz95703	management-only cli not available in user context of QP-D
CSCuz95806	DNS Doctoring DNS64 is not working
CSCuz98201	ASAv - High CPU utilization
CSCuz98220	ASA traceback with Thread Name: Dispatch Unit
CSCuz98704	Traceback in CP Processing thread after upgrade
CSCva00190	ASA 9.4.2.6 High CPU due to CTM message handler due to chip resets
CSCva00939	Remove ACL warning messages in show access-list when FQDN is resolved
CSCva01570	Unexpected end of file logon.html in WebVPN
CSCva02655	ASA sends invalid interface id to SFR for clientless VPN traffic
CSCva02817	ASA not rate limiting with DSCP bit set from the Server
CSCva03607	show service-policy output reporting incorrect values
CSCva03982	ASA : Mem leak in cluster mode due to PBR lookup
CSCva05513	ASA: SLA Monitor not working with floating timeout configured to nonzero
CSCva05778	ASAv5 shows very high memory usage
CSCva07268	Unable to auth a 2nd time via clientless after ASA upgrade
CSCva10054	ASA ASSERT traceback in DATAPATH due to sctp inspection
CSCva12520	snmpwalk not working for some NAT OIDs
CSCva15911	On reloading the ASA, ASA mounts SSD as disk 0, instead of the flash.
CSCva16471	IPv6 OSPF routes do not update when a lower metric route is advertised
CSCva22048	ASA: SIP Call Drops with PAT when same media port used in multiple calls
CSCva24799	TLS Proxy feature missing client trust-point command
CSCva24924	ASA SM on 9300 reloads multi-context over SSH when config-url is entered
CSCva26771	ASA : PBR Mem leak as packet dropped
CSCva31378	ASA treaceback at Thread Name: rtcli async executor process
CSCva32092	OSPFv3/IPv6 flapping every 30 min between ASA cluster and 4500
CSCva35439	ASA DATAPATH traceback (Cluster)

Caveat ID Number	Description
CSCva35990	Traceback on CP Process with H323 inspection, rip h323_service_early_msg
CSCva36202	BGP Socket not open in ASA after reload
CSCva36884	Cisco ASA Cross Site Scripting SSLVPN Vulnerability
CSCva38556	Cisco ASA Input Validation File Injection Vulnerability
CSCva39094	ASA traceback in CLI thread while making MPF changes
CSCva40844	Crypto accelerator ring timeout causes packet drops
CSCva43746	ASA 'show inventory' shows 'Driver Error, invalid query ready'
CSCva43992	IKEv2 RA cert auth. Unable to allocate new session. Max sessions reached
CSCva45590	ASA OSPFv3 interface ID changes upon disabling/enabling failover
CSCva46920	Traceback in Thread Name: ssh when issuing show tls-proxy session detail
CSCva47608	SCTP MH:pin hole removed and added freq on standby with dual nat
CSCva49256	memory leak in ssh
CSCva50554	ASA uses "::" for host IP addresses if booted with an improper config
CSCva50838	ASA capture type isakmp not saving reassembled rfc7383 IKEv2 packets
CSCva52514	ASAv-Azure: waagent may reload when asav deployed with load balancer
CSCva53581	Increasing the global ARP request pool
CSCva56114	CISCO-MEMORY-POOL-MIB returns incorrect values for heapcache
CSCva56343	Clustering: TFW asynchronous flow packet drop due to L2 entry timeout
CSCva62667	Shut down interfaces shows up in ASP routing table
CSCva62861	uauth is failed after failover
CSCva66278	SmartLic: Inter-chassis master switchover license race condition
CSCva68364	SNMPv3 active engineID is not reset when ASA is replaced
CSCva68987	ASA drops ICMP request packets when ICMP inspection is disabled
CSCva69346	Unable to relay DHCP discover packet from ASA when NAT is matched
CSCva69584	OSPF generates Type-5 LSA with incorrect mask, which gets stuck in LSDB
CSCva69799	ASA stuck in boot loop due to FIPS Self-Test failure
CSCva70095	ASA negotiates TLS1.2 when server in tls-proxy
CSCva71783	ICMP error packets in response to reply packets are dropped

Caveat ID Number	Description
CSCva76568	ASA : Enabling IKEv1/IKEv2 opens RADIUS ports
CSCva77852	ipsecvpn-ikev2_oth: 5525 9.4.2.11 traceback in Thread Name: IKEv2 Daemon
CSCva81412	ASR9000 BGP Graceful Restart doesnt work as expected
CSCva81749	IPV6 address not assigned when connecting via IPSEC protocol
CSCva84079	ASAv hangs often during reboot
CSCva84625	ASAv show hostname generates smart licensing authorization request
CSCva84635	ASA: CHILD_SA collision brings down IKEv2 SA
CSCva85382	ASA memory leak for CTS SGT mappings
CSCva85933	FTD - 6.1 - redistribute connected is redistributing Internal-Data (NLP)
CSCva86626	HTML5: Guacamole server requires page refresh
CSCva87077	GTP traceback at gtpv1_process_msg for echo response
CSCva87160	OTP authentication is not working for clientless ssl vpn
CSCva88796	AnyConnect Sessions Cannot Connect Due to Stuck L2TP Uauth Sessions
CSCva90419	issuer-name falsely detecting duplicates in certificate map using attr
CSCva90806	ASA Traceback when issue 'show asp table classify domain permit'
CSCva91420	ASA Traceback in CTM Message Handler
CSCva92151	Cisco ASA SNMP Remote Code Execution Vulnerability
CSCva92813	ASA Cluster DHCP Relay doesn't forward the server replies to the client
CSCva92975	ASA 5585-60 dropping out of cluster with traceback
CSCva94702	Enqueue failures on DP-CP queue may stall inspected TCP connection
CSCva97863	971 EST - Console hang on show capture
CSCva98240	SIP: Address from Route: header not translated correctly
CSCvb03994	Traceback in IKE_DBG
CSCvb04685	Unable to delete the SNMP config
CSCvb05667	H.323 inspection causes Traceback in Thread Name: CP Processing
CSCvb05787	traceback in network udpmod_get after anyconnect test load application
CSCvb08776	Internal ATA Compact Flash size is incorrectly shown in "show version"
CSCvb13737	wr mem/ wr standby is not syncing configs on standby

Caveat ID Number	Description
CSCvb14997	ASA DHCP Relay rewrites netmask and gw received as part of DHCP Offer
CSCvb15265	ASA Page fault traceback in Thread Name: DATAPATH
CSCvb19251	ASA drops ACK to DHCPINFORM message citing "DHCPRA: Ignoring ACK due to different server identity."
CSCvb19492	ASA stops processing DHCP Offers in a based RAVPN
CSCvb19843	Buffer Overflow in ASA Leads to Remote Code Execution
CSCvb20256	Sweet32 Vulnerability in ASA's SSH Implementation
CSCvb21922	Remove ACL warning messages in show access-list when FQDN is unresolved
CSCvb22435	ASA Traceback in thread name CP Processing due to DCERPC inspection
CSCvb22848	ASA 9.1.7-9 crash in Thread Name: NIC status poll
CSCvb25139	IPv6 DNS packets getting malformed when DNS inspection is enabled.
CSCvb26119	Webvpn rewriter failing on matterport.com
CSCvb27868	ASA 1550 block depletion with multi-context transparent firewall
CSCvb29411	AAA authentication/authorization fails if only accessible via mgmt vrf
CSCvb29688	Stale VPN Context entries cause ASA to stop encrypting traffic despite fix for CSCup37416
CSCvb30445	ASA may generate DATAPATH Traceback with policy-based routing enabled
CSCvb31055	ASA Multiple Context SNMP PAT Interface Missing
CSCvb31833	Traceback : ASA with Threadname: DATAPATH-0-1790
CSCvb32297	WebVPN:VNC plugin:Java:Connection reset by peer: socket write error
CSCvb32341	ASA traceback with passive-interface default on 9.6(2)
CSCvb33009	Cisco ASA Signature Verification Misleading Digital Signing Text On Boot
CSCvb33013	Cisco ASA Remove Mis-leading Secure Boot commands on non-SB hardware
CSCvb36199	Thread Name: snmp ASA5585-SSP-2 running 9.6.2 traceback
CSCvb37456	Failover after IKE rekey fails to initiate ph1 rekey on act device
CSCvb38522	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
CSCvb39082	SmartLic: Trigger auth renewal from the app for cluster role change
CSCvb39147	Lower NFS throughput rate on Cisco ASA platform
CSCvb40417	nlp_int_tap routes seen in ASA "sh route" command

Caveat ID Number	Description
CSCvb40818	nlp information seen in ipv6 commands
CSCvb40847	ASA not sending Authen Session End log if user logs out manually
CSCvb40898	Cisco ASA Software DNS Denial of Service Vulnerability
CSCvb41097	GTPv2 Dropping instance 1 handoffs
CSCvb43120	ASA Traceback in Checkheaps Thread
CSCvb45039	ASA traceback with Thread Name aaa_shim_thread
CSCvb46321	Cisco ASA Software and Cisco FTD Software TCP Normalizer Denial of Service Vulnerability
CSCvb46531	ASDM : memory usage reading incorrect for ASAv 9.6.2
CSCvb47006	ASA traceback observed on auto-update thread.
CSCvb48640	Evaluation of pix-asa for Openssl September 2016
CSCvb49264	Delete Bearer Req fails to delete second default bearer after v2 Handoff callflow.
CSCvb49273	Traceback triggered by CoA on ASA when sending/receiving to/from ISE
CSCvb49445	IKEv2: It is NOT cleaning the sessions after disconnected from the client.
CSCvb50301	ASA traceback at Thread Name: rtcli
CSCvb50609	RADIUS authorization request does not send Called-Station-ID attribute
CSCvb50750	Lina core during failover with sip traffic
CSCvb52157	viewer_dart.js file not loading correctly
CSCvb52381	OSPF continuously flaps after master change (L2 cluster, multi-ctx)
CSCvb52492	VPN tunnels are lost after failover due to OSPF route issue
CSCvb52988	ASA Traceback Thread Name: emweb/https
CSCvb53094	ASA : Discrepancy in used memory calculation for Multiple context firewall
CSCvb55721	GARP flood done by ASAs in multi-site cluster using the site-ip address
CSCvb57817	EIGRP: Need to add large number error handling when getting scaled bandwidth
CSCvb58087	Object-group-search redundant service group objects are incorrectly removed
CSCvb61056	9.6.2 TCP connection doesn't work through L2TP
CSCvb63503	AAA session handle leak with IKEv2 when denied due to time range
CSCvb63819	ASA-SM traceback with Thread : fover_parse during upgrade OS 9.1.6 to 9.4.3

Caveat ID Number	Description
CSCvb64161	ASA fairly infrequently rewrites the dest MAC address of multicast packet for client
CSCvb66593	webvpn_state cookie information disclosure in url
CSCvb68766	ASA traceback at Thread Name: IKE Daemon.
CSCvb74084	SCP fails in 962
CSCvb74249	ASA dropping traffic with TCP syslog configured in multicontext mode
CSCvb75685	EZVPN NEM client can't reconnect after "no vpnclient enable" is entered
CSCvb78614	4GE-SSM RJ45 interface may drop traffic due to interface "rate limit drops"
CSCvb83446	v1 PDP may get deleted on parse IE failure
CSCvb88126	ASA: Stuck uauth entry rejects AnyConnect connection despite fix for CSCuu48197
CSCvb89988	WebVPN: Internal page login button not working through rewriter
CSCvb92125	ASA drops DNS PTR Reply with reason Label length exceeded during rewrite
CSCvb92417	Cluster ASA drops to-the-box ICMP replies with reason "inspect-icmp-seq-num-not-matched"
CSCvb92823	ASA SIP inspection may delay transmission of 200 OK when embedded with NOTIFY
CSCvc00015	Incorrect behaviour when SNMP polling is done on virtual IP of an ASA cluster.
CSCvc00689	ASA : memory leak due to ikev2
CSCvc00760	RDP Plugin Connection failed with error
CSCvc01685	PLR: ASAv generates invalid reservation code
CSCvc04741	ASA DHCP relay is incompatible with intercept-dhcp feature
CSCvc05005	ASA cluster TCP/SSL ports are not displayed on LISTEN state
CSCvc06150	ASA unable to add multiple attribute entries in a certificate map
CSCvc07330	ASAv may crash when running webvpn
CSCvc14190	ASA fails SSL VPN session establishment with EC under load
CSCvc14448	9.6.2 - Traceback during AnyConnect IKEv2 Performance Test
CSCvc14502	ASA multicontext disallowing new conns with TCP syslog unreachable and logging permit-hostdown set
CSCvc16330	ASA-SM 9.5.2 inspect-sctp licensing breaks existing deployments
CSCvc19318	ASA traceback at Thread Name: sch_syslog
CSCvc23838	Cisco ASA Heap Overflow in Webvpn CIFS

Caveat ID Number	Description
CSCvc24657	MIB object cempMemPoolHCUsed disappeared
CSCvc24788	ASA: OspfV3 routes are not getting installed
CSCvc25195	ASA portal reveals that multiple context is configured when anyconnect is deployed.
CSCvc25281	Error synchronizing the SNMPv3 user after rebooting a cluster unit
CSCvc25409	ASA memory leak in CloneOctetString when using SNMP polling
CSCvc33796	Implement speed improvements for ACL and NAT table compilation
CSCvc36805	Firepower Threat Defense (FTD) IKEv2 NAT-T gets disabled after reboot
CSCvc37557	SSL connection hangs between ASA and backend server in clientless WebVPN
CSCvc38425	ASA with FirePOWER module generates traceback and reloads or causes process not running
CSCvc39121	Anyconnect address assignment fails using external DHCP server when ASA is in Multi-context Mode
CSCvc44240	ASA clustering: mac-address cmd is ignored on spanned port-channel interface in 9.6.2
CSCvc48640	ASA not update access-list dynamically when forward-reference enable is configured
CSCvc52072	Webvpn portal not displayed corrrectly for connections landing on default webvpn group.
CSCvc52272	ASA inspection-MPF ACL changes are not getting ordered correctly in the ASP Table
CSCvc52504	ASA may traceback with Thread Name: Unicorn Admin Handler
CSCvc52879	Reloading Active unit in Active/Standby ASA failover pair is not triggering a failover.
CSCvc55974	ikev2 handles get leaked in a L2L setup
CSCvc58272	ASA incorrectly processing negative numbers in wrappers, resulting in graphical webvpn issue
CSCvc60254	SIP: 200 OK messages with multiple seqments not reassembled correctly
CSCvc60964	ASA L3 Cluster: DHCP relay drops DHCPOFFER in case of asymmetric routing
CSCvc62252	Tracking route is up while the reachability is down
CSCvc62556	Traceback in ASA Cluster Thread Name: qos_metric_daemon
CSCvc65409	Traceback observed on gtpv2_process_msg on cluster
CSCvc68229	BGP's BFD support code opens tcp/udp 3784 and 3785 to bypass access-lists

Caveat ID Number	Description
CSCvc77123	ASA may traceback in network_tcpmod_close_conn with AnyConnect IPv6 DTLS stress scenario
CSCvc79077	ASA watchdog traceback during cluster config sync with rest-api enabled
CSCvc79371	ASA nat pool not getting updated correctly.
CSCvc79454	Unable to configure ssh public auth for script users
CSCvc82146	ASA traceback in threadname Datapath
CSCvc88411	1550-byte block depletion seen due to Radius Accounting packets
CSCvd78303	ARP functions fail after 213 days of uptime, drop with error 'punt-rate-limit-exceeded'

End-User License Agreement

For information on the end-user license agreement, go to http://www.cisco.com/go/warranty.

Related Documentation

For additional information on the ASA, see Navigating the Cisco ASA Series Documentation.