

Release Notes for the Cisco ASA Series, 9.8(x)

Release Notes for the Cisco ASA Series, 9.8(x)

This document contains release information for Cisco ASA software Version 9.8(x).

Important Notes

- **ASDM signed-image support in 9.8(4.45)/7.18(1.152) and later**—The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM will be blocked and the message “%ERROR: Signature not valid for file disk0:/<filename>” will be displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. ([CSCwb05291](#), [CSCwb05264](#))
- Upgrade ROMMON for ASA 5506-X, 5508-X, and 5516-X to Version 1.1.15—There is a new ROMMON version for these ASA models (May 15, 2019); we highly recommend that you upgrade to the latest version. To upgrade, see the instructions in the [ASA configuration guide](#).



Caution The ROMMON upgrade for 1.1.15 takes twice as long as previous ROMMON versions, approximately 15 minutes. **Do not** power cycle the device during the upgrade. If the upgrade is not complete within 30 minutes or it fails, contact Cisco technical support; **do not** power cycle or reset the device.

- Before upgrading to 9.8(2) or later, FIPS mode requires the failover key to be at least 14 characters—Before you upgrade to 9.8(2) or later in FIPS mode, you must change the **failover key** or **failover ipsec pre-shared-key** to be at least 14 characters long. If your failover key is too short, when you upgrade the first unit, the failover key will be rejected, and both units will become active until you set the failover key to a valid value.
- 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 deprecated in the future.

- Do not upgrade to 9.8(1) for ASAv on Amazon Web Services—Due to [CSCve56153](#), you should not upgrade to 9.8(1). After upgrading, the ASAv becomes unreachable. Upgrade to 9.8(1.5) or later instead.

- ASAv5 memory issues—Starting in Version 9.7(1), the ASAv5 may experience memory exhaustion where certain functions such as enabling AnyConnect or downloading files to the ASAv fail. The following bugs were fixed in 9.8(1.5) to transparently improve memory function and to optionally allow you to assign more memory to the ASAv5 if necessary: [CSCvd90079](#) and [CSCvd90071](#).
- 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."

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 9.8(4)

Released: April 24, 2019

Feature	Description
VPN Features	
Add subdomains to webVPN HSTS	Allows domain owners to submit what domains should be included in the HSTS preload list for web browsers. New/Modified commands: hostname(config-webvpn) includesubdomains <i>Also in 9.12(1).</i>
Administrative Features	

Feature	Description
Allow non-browser-based HTTPS clients to access the ASA	<p>You can allow non-browser-based HTTPS clients to access HTTPS services on the ASA. By default, ASDM, CSM, and REST API are allowed. Many specialty clients (for example, python libraries, curl, and wget) do not support Cross-site request forgery (CSRF) token-based authentication, so you need to specifically allow these clients to use the ASA basic authentication method. For security purposes, you should only allow required clients.</p> <p>New/Modified commands: http server basic-auth-client</p> <p><i>Also in 9.12(1).</i></p>
show tech-support includes additional output	<p>The output of the show tech-support is enhanced to display the output of the following:</p> <ul style="list-style-type: none"> • show ipv6 interface • show aaa-server • show fragment <p>New/Modified commands: show tech-support</p> <p><i>Also in 9.12(1).</i></p>
Support to enable and disable the results for free memory and used memory statistics during SNMP walk operations	<p>To avoid overutilization of CPU resources, you can enable and disable the query of free memory and used memory statistics collected through SNMP walk operations.</p> <p>New/Modified command: snmp-server enable oid</p> <p><i>Also in 9.10(1).</i></p>

New Features in ASA 9.8(3)

Released: July 2, 2018

Feature	Description
Platform Features	
Firepower 2100 Active LED now lights amber when in standby mode	Formerly, the Active LED was unlit in standby mode.
Firewall Features	
Support for removing the logout button from the cut-through proxy login page.	<p>If you configure the cut-through proxy to obtain user identity information (the AAA authentication listener), you can now remove the logout button from the page. This is useful in case where users connect from behind a NAT device and cannot be distinguished by IP address. When one user logs out, it logs out all users of the IP address.</p> <p>New/Modified commands: aaa authentication listener no-logout-button.</p>
Trustsec SXP connection configurable delete hold down timer	<p>The default SXP connection hold down timer is 120 seconds. You can now configure this timer, between 120 to 64000 seconds.</p> <p>New/Modified commands: cts sxp delete-hold-down period, show cts sxp connection brief, show cts sxp connections</p>

Feature	Description
VPN Features	
Support for legacy SAML authentication	<p>If you deploy an ASA with the fix for CSCvg65072, then the default SAML behavior is to use the embedded browser, which is not supported on AnyConnect 4.4 or 4.5. Therefore, to continue to use AnyConnect 4.4 or 4.5, you must enable the legacy external browser SAML authentication method. Because of security limitations, use this option only as part of a temporary plan to migrate to AnyConnect 4.6. This option will be deprecated in the near future.</p> <p>New/Modified commands: saml external-browser</p>
Interface Features	
Unique MAC address generation for single context mode	<p>You can now enable unique MAC address generation for VLAN subinterfaces in single context mode. Normally, subinterfaces share the same MAC address with the main interface. Because IPv6 link-local addresses are generated based on the MAC address, this feature allows for unique IPv6 link-local addresses.</p> <p>New or modified command: mac-address auto</p> <p><i>Also in 9.9(2) and later.</i></p>

New Features in ASA 9.8(2)

Released: August 28, 2017

Feature	Description
Platform Features	
ASA for the Firepower 2100 series	<p>We introduced the ASA for the Firepower 2110, 2120, 2130, and 2140. Similar to the Firepower 4100 and 9300, the Firepower 2100 runs the base FXOS operating system and then the ASA operating system as an application. The Firepower 2100 implementation couples FXOS more closely with the ASA than the Firepower 4100 and 9300 do (pared down FXOS functions, single device image bundle, easy management access for both ASA and FXOS).</p> <p>FXOS owns configuring hardware settings for interfaces, including creating EtherChannels, as well as NTP services, hardware monitoring, and other basic functions. You can use the Firepower Chassis Manager or the FXOS CLI for this configuration. The ASA owns all other functionality, including Smart Licensing (unlike the Firepower 4100 and 9300). The ASA and FXOS each have their own IP address on the Management 1/1 interface, and you can configure management of both the ASA and FXOS instances from any data interface.</p> <p>We introduced the following commands: connect fxos, fxos https, fxos snmp, fxos ssh, ip-client</p>
Department of Defense Unified Capabilities Approved Products List	<p>The ASA was updated to comply with the Unified Capabilities Approved Products List (UC APL) requirements. In this release, when you enter the fips enable command, the ASA will reload. Both failover peers must be in the same FIPS mode before you enable failover.</p> <p>We modified the following command: fips enable</p>

Feature	Description
ASAv for Amazon Web Services M4 instance support	You can now deploy the ASAv as an M4 instance. We did not modify any commands.
ASAv5 1.5 GB RAM capability	Starting in Version 9.7(1), the ASAv5 may experience memory exhaustion where certain functions such as enabling AnyConnect or downloading files to the ASAv fail. You can now assign 1.5 GB (up from 1 GB) of RAM to the ASAv5. We did not modify any commands.
VPN Features	
HTTP Strict Transport Security (HSTS) header support	HSTS protects websites against protocol downgrade attacks and cookie hijacking on clientless SSL VPN. It lets web servers declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol. HSTS is an IETF standards track protocol and is specified in RFC 6797 . We introduced the following commands: hsts enable , hsts max-age <i>age_in_seconds</i>
Interface Features	
VLAN support for the ASAv50	The ASAv50 now supports VLANs on the ixgbe-vf vNIC for SR-IOV interfaces. We did not modify any commands.

New Features in ASA 9.8(1.200)

Released: July 30, 2017



Note This release is only supported on the ASAv for Microsoft Azure. These features are not supported in Version 9.8(2).

Feature	Description
High Availability and Scalability Features	
Active/Backup High Availability for ASAv on Microsoft Azure	A stateless Active/Backup solution that allows for a failure of the active ASAv to trigger an automatic failover of the system to the backup ASAv in the Microsoft Azure public cloud. We introduced the following commands: failover cloud No ASDM support.

New Features in ASA 9.8(1)

Released: May 15, 2017

Feature	Description
Platform Features	

Feature	Description
ASAv50 platform	The ASAv platform has added a high-end performance ASAv50 platform that provides 10 Gbps Firewall throughput levels. The ASAv50 requires ixgbe-vf vNICs, which are supported on VMware and KVM only.
SR-IOV on the ASAv platform	The ASAv platform supports Single Root I/O Virtualization (SR-IOV) interfaces, which allows multiple VMs to share a single PCIe network adapter inside a host. ASAv SR-IOV support is available on VMware, KVM, and AWS only.
Automatic ASP load balancing now supported for the ASAv	Formerly, you could only manually enable and disable ASP load balancing. We modified the following command: asp load-balance per-packet auto
Firewall Features	
Support for setting the TLS proxy server SSL cipher suite	You can now set the SSL cipher suite when the ASA acts as a TLS proxy server. Formerly, you could only set global settings for the ASA using the ssl cipher command. We introduced the following command: server cipher-suite
Global timeout for ICMP errors	You can now set the idle time before the ASA removes an ICMP connection after receiving an ICMP echo-reply packet. When this timeout is disabled (the default), and you enable ICMP inspection, then the ASA removes the ICMP connection as soon as an echo-reply is received; thus any ICMP errors that are generated for the (now closed) connection are dropped. This timeout delays the removal of ICMP connections so you can receive important ICMP errors. We added the following command: timeout icmp-error
High Availability and Scalability Features	
Improved cluster unit health-check failure detection	You can now configure a lower holdtime for the unit health check: .3 seconds minimum. The previous minimum was .8 seconds. This feature changes the unit health check messaging scheme to <i>heartbeats</i> in the data plane from <i>keepalives</i> in the control plane. Using heartbeats improves the reliability and the responsiveness of clustering by not being susceptible to control plane CPU hogging and scheduling delays. Note that configuring a lower holdtime increases cluster control link messaging activity. We suggest that you analyze your network before you configure a low holdtime; for example, make sure a ping from one unit to another over the cluster control link returns within the <i>holdtime</i> /3, because there will be three heartbeat messages during one holdtime interval. If you downgrade your ASA software after setting the hold time to .3 - .7, this setting will revert to the default of 3 seconds because the new setting is unsupported. We modified the following commands: health-check holdtime, show asp drop cluster counter, show cluster info health details
Configurable debounce time to mark an interface as failed for the Firepower 4100/9300 chassis	You can now configure the debounce time before the ASA considers an interface to be failed, and the unit is removed from the cluster. This feature allows for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the ASA waits the number of milliseconds specified before marking the interface as failed and the unit is removed from the cluster. The default debounce time is 500 ms, with a range of 300 ms to 9 seconds. New or modified command: health-check monitor-interface debounce-time
VPN Features	

Feature	Description
Support for IKEv2, certificate based authentication, and ACL in VTI	<p>Virtual Tunnel Interface (VTI) now supports BGP (static VTI). You can now use IKEv2 in standalone and high availability modes. You can use certificate based authentication by setting up a trustpoint in the IPsec profile. You can also apply access lists on VTI using access-group commands to filter ingress traffic.</p> <p>We introduced the following command in the IPsec profile configuration mode: set trustpoint.</p>
Mobile IKEv2 (MobIKE) is enabled by default	<p>Mobile devices operating as remote access clients require transparent IP address changes while moving. Supporting MobIKE on ASA allows a current IKE security association (SA) to be updated without deleting the current SA. MobIKE is “always on.”</p> <p>We introduced the following command: ikev2 mobike-rrc. Used to enable/disable return routability checking.</p>
SAML 2.0 SSO Updates	<p>The default signing method for a signature in a SAML request changed from SHA1 to SHA2, and you can configure which signing method you prefer: <code>rsa-sha1</code>, <code>rsa-sha256</code>, <code>rsa-sha384</code>, or <code>rsa-sha512</code>.</p> <p>We changed the following command in webvpn mode: saml idp signature can be configured with a <i>value</i>. Disabled is still the default.</p>
Change for tunnelgroup webvpn-attributes	<p>We changed the pre-fill-username and secondary-pre-fill-username value from ssl-client to client.</p> <p>We changed the following commands in webvpn mode: pre-fill-username and secondary-pre-fill-username can be configured with a client value.</p>
AAA Features	
Login history	<p>By default, the login history is saved for 90 days. You can disable this feature or change the duration, up to 365 days. This feature only applies to usernames in the local database when you enable local AAA authentication for one or more of the management methods (SSH, ASDM, Telnet, and so on).</p> <p>We introduced the following commands: aaa authentication login-history, show aaa login-history</p>
Password policy enforcement to prohibit the reuse of passwords, and prohibit use of a password matching a username	<p>You can now prohibit the reuse of previous passwords for up to 7 generations, and you can also prohibit the use of a password that matches a username.</p> <p>We introduced the following commands: password-history, password-policy reuse-interval, password-policy username-check</p>

Feature	Description
Separate authentication for users with SSH public key authentication and users with passwords	<p>In releases prior to 9.6(2), you could enable SSH public key authentication (ssh authentication) without also explicitly enabling AAA SSH authentication with the Local user database (aaa authentication ssh console LOCAL). In 9.6(2), the ASA required you to explicitly enable AAA SSH authentication. In this release, you no longer have to explicitly enable AAA SSH authentication; when you configure the ssh authentication command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for usernames with <i>passwords</i>, and you can use any AAA server type (aaa authentication ssh console radius_1, for example). For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS.</p> <p>We did not modify any commands.</p> <p><i>Also in Version 9.6(3).</i></p>
Monitoring and Troubleshooting Features	
Saving currently-running packet captures when the ASA crashes	<p>Formerly, active packet captures were lost if the ASA crashed. Now, packet captures are saved to disk 0 at the time of the crash with the filename [<i>context_name</i>].<i>capture_name</i>.pcap.</p> <p>We did not modify any commands.</p>

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:

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

This table provides upgrade paths for ASA. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.



Note Be sure to check the upgrade guidelines for each release between your starting version and your ending version. You may need to change your configuration before upgrading in some cases, or else you could experience an outage.



Note For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the [ASA Security Advisories](#).



Note ASA 9.12(x) was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.
 ASA 9.2(x) was the final version for the ASA 5505.
 ASA 9.1(x) was the final version for the ASA 5510, 5520, 5540, 5550, and 5580.

Current Version	Interim Upgrade Version	Target Version
9.7(x)	—	Any of the following: → 9.8(x)
9.6(x)	—	Any of the following: → 9.8(x)
9.5(x)	—	Any of the following: → 9.8(x)
9.4(x)	—	Any of the following: → 9.8(x)
9.3(x)	—	Any of the following: → 9.8(x)
9.2(x)	—	Any of the following: → 9.8(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: → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.8(x) → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)
8.2(x) and earlier	→ 9.0(4)	Any of the following: → 9.8(x) → 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 9.8(x)

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

Caveat ID Number	Description
CSCvj28716	ASA VPN with multiple peers drops incoming packets after failover
CSCvk69317	Configuration Generation in the crypto portion changes without configuration change
CSCvn03552	ASA Traceback with Thread Name: Cluster CFG CLI Rep after removing captures and saving configuration
CSCvn15387	Active unit Tracebacks in 'Thread Name: IKE Daemon'
CSCvn65598	ASDM load fails with the error message: The flash device is in use by another task.
CSCvn82441	[SXP] Issue with establishing SXP connection between ASA on FPR-2110 and switches
CSCvo08881	ASA may log negative values for conn-max exceeded syslog and drop permitted traffic
CSCvo14961	ASA may traceback and reload while waiting for "dns_cache_timer" process to finish.
CSCvo30697	Throughput drop when LINA capture is applied on various platforms
CSCvo33216	FasterXML jackson-databind axis2-jaxws Class Server-Side Request Forge
CSCvo33218	FasterXML jackson-databind openjpa Class Blocking Vulnerability
CSCvo33220	FasterXML jackson-databind jboss-common-core Class Blocking Vulnerabil
CSCvo33222	FasterXML jackson-databind axis2-transport-jms Class Blocking Vulnerab
CSCvo33223	FasterXML jackson-databind slf4j-ext Class Arbitrary Code Execution Vu
CSCvo33224	FasterXML jackson-databind Blaze-ds-Opt and Blaze-ds-Core Classes Arbi
CSCvo33226	FasterXML jackson-databind Polymorphic Deserialization External XML En
CSCvo45738	ASA L2TP clients fail to receive IP address from local pool
CSCvo45755	ASA SCP transfer to box stall mid-transfer
CSCvo74631	IKEv2: VTI tunnel doesn't work as expected when both sides are configured as initiator
CSCvo79255	BGP redistribution to OSPF is getting wrong behavior if monitor-interface is enabled
CSCvo85588	Secondary/active FTD does not block connections while TCP syslog server is not reachable.
CSCvp14697	ASA traceback DATAPATH: Thread Name: SXP CORE
CSCvp18878	ASA: Watchdog traceback in Datapath
CSCvp22166	ASA may traceback and reload because the CPU is not yielded for "dns_cache_timer" thread.

Caveat ID Number	Description
CSCvp23530	OSPF neighbor command not replicated to standby after write standby or reload

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 9.8(4)

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

Caveat ID Number	Description
CSCux69220	WebVPN 'enable intf' with DHCP , CLI missing when ASA boot
CSCuz70352	Unable to SSH over remote access VPN (telnet, asdm working)
CSCvd28906	ASA traceback at first boot in 5506 due to unable to allocate enough LCMB memory
CSCvd76939	ASA policy-map configuration is not replicated to cluster slave
CSCve53415	ASA traceback in DATAPATH thread while running captures
CSCve85565	Traceback when syslog sent over VPN tunnel
CSCve95403	ASA boot loop caused by logs sent after FIPS boot test
CSCvf83160	Traceback on Thread Name: DATAPATH-2-1785
CSCvf85831	asdm displays error uploading image
CSCvg36254	FTD Diagnostic Interface does Proxy ARP for br1 management subnet
CSCvg40735	GTP inspection may spike cpu usage
CSCvg65072	Cisco ASA sw, FTD sw, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability
CSCvg76652	Default DLY value of port-channel sub interface mismatch
CSCvh01213	An ASA may Traceback and reload when processing traffic
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvh16252	ASA may traceback and reload in Thread Name: fover_rep during conn replication
CSCvh26447	Firepower 2100 Series might report failure due to MIO-blade heartbeat failure
CSCvh55035	Firepower Threat Defense device unable to stablish ERSPAN with Nexus 9000
CSCvh55340	ASA Running config through REST-API Full Backup does not contain the specified context configuration
CSCvh83849	DHCP Relay With Dual ISP and Backup IPSEC Tunnels Causes Flapping

Caveat ID Number	Description
CSCvh95302	ASDM/Webvpn stops working after reload if IPv6 address configured on the interface
CSCvh98781	ASA/FTD Deployment ERROR 'Management interface is not allowed as Data is in use by this instance'
CSCvi03103	BGP ASN cause policy deployment failures.
CSCvi07974	FTD: Layer 2 packets (ex: BPDUs) are dropped during snort restarts (Inline/Passive Interfaces Only)
CSCvi19125	Multicast ip-proto-50 (ESP) dropped by ASP citing 'np-sp-invalid-spi'
CSCvi19220	ASA fails to encrypt after performing IPv6 to IPv4 NAT translation
CSCvi34164	ASA does not send 104001 and 104002 messages to TCP/UDP syslog
CSCvi37644	PKI:- ASA fails to process CRL's with error "Add CA req to pool failed. Pool full."
CSCvi38151	ASA pair: IPv6 static/connected routes are not sync/replicated between Active/Standby pairs.
CSCvi42008	Stuck uauth entry rejects AnyConnect user connections
CSCvi46759	Allow ASA to process packet with hop limit of 0 (Follow RFC 8200)
CSCvi51515	REST-API:500 Internal Server Error
CSCvi53708	ASA NAT position discrepancy between CLI and REST-API causing REST to delete wrong config
CSCvi54162	"ha-replace" action not working when peer not present
CSCvi55464	ASA5585 device power supply Serial Number not in the snmp response
CSCvi71622	Traceback in DATAPATH on standby FTD
CSCvi77643	Hanging downloads and slow downloads on a FPR4120 due to http inspect
CSCvi79691	LDAP over SSL crypto engine error
CSCvi79999	256 Byte block leak observed due to ARP traffic when using VTI
CSCvi85382	ASA5515 Low DMA memory when ASA-IC-6GE-SFP-A module is installed
CSCvi87214	Neighbour Solicitation messages are observed for IPv6 traffic
CSCvi89194	pki handles: increase and fail to decrement
CSCvi90633	Edit GUI language on ASDM AC downloads but ignores the change FPR-21XX
CSCvi96442	Slave unit drops UDP/500 and IPSec packets for S2S instead of redirecting to Master
CSCvi97729	To-the-box traffic being routing out a data interface when failover is transitioning on a New Active

Caveat ID Number	Description
CSCvj99743	Standby traceback in Thread "Logger" after executing "failover active" with telnet access
CSCvj06993	ASA HA with NSF: NSF is not triggered properly when there is an Interface failure in ASA HA
CSCvj15572	Flow-offload rewrite rules not updated when MAC address of interface changes
CSCvj17314	In version 9.7 and lower ASA does not honor "no signature" under saml configuration
CSCvj28643	reload command does not work properly on ASAv
CSCvj32264	ASA - zonelabs-integrity : Traceback and High CPU due to Process 'Integrity FW task'
CSCvj37448	ASA : Device sends only ID certificate in SSL server certificate packet after reload
CSCvj37924	CWE-20: Improper Input Validation
CSCvj39858	Traceback: Thread Name: IPsec message handler
CSCvj41748	Bonita BPM app's web pages access fail via webvpn
CSCvj42269	ASA 9.8.2 Receiving syslog 321006 reporting System Memory as 101%
CSCvj42450	ASA traceback in Thread Name: DATAPATH-14-17303
CSCvj43591	Firepower 2110 with ASA DHCP does not work properly
CSCvj44262	portal-access-rule changing from "deny" to "permit"
CSCvj46777	Firepower Threat Defense 2100 asa traceback for unknown reason
CSCvj47119	"clear capture /all" might crash Firepower 9300 MI Firepower Threat Defense
CSCvj47256	ASA SIP and Skinny sessions drop, when two subsequent failovers take place
CSCvj48340	ASA memory Leak - snp_svc_insert_dtls_session
CSCvj48542	Trustsec SXP delete hold down timer value needs to be configurable
CSCvj49883	ASA traceback on Firepower Threat Defense 2130-ASA-K9
CSCvj50024	ASA portchannel lacp max-bundle 1 hot-sby port not coming up after link failure
CSCvj54840	create/delete context stress test causes traceback in nameif_install_arp_punt_service
CSCvj56909	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module
CSCvj58342	Multicast dropped after deleting a security context
CSCvj59347	Remove/Increase the maximum 255 characters error limit in result of a cli command!
CSCvj67258	Change 2-tuple and 4-tuple hash table to lockless

Caveat ID Number	Description
CSCvj67740	Static IPv6 route prefix will be removed from the ASA configuration
CSCvj67776	clear crypto ipsec ikev2 commands not replicated to standby
CSCvj72309	FTD does not send Marker for End-of-RIB after a BGP Graceful Restart
CSCvj73581	Traceback in cli_xml_server Thread
CSCvj74210	Traceback at "ssh" when executing 'show service-policy inspect gtp pdp-context detail'
CSCvj75220	Usage of 'virtual http' or 'virtual telnet' incorrectly needs 'same-security permit intra-interface'
CSCvj75793	2100/4100/9300: stopping/pausing capture from Management Center doesn't lower the CPU usage
CSCvj79765	Netflow configuration on Active ASA is replicated in upside down order on Standby unit
CSCvj88461	Withdrawal advertisements for specific prefixes are flooded before flooding aggregate prefix
CSCvj88514	IP Local pools configured with the same name.
CSCvj89470	Cisco Adaptive Security Appliance Direct Memory Access Denial of Service Vulnerability
CSCvj91449	ASA traceback when logging host command is enable for IPv6 after each reboot
CSCvj91619	1550 Block Depletion Causes ASA to reload 6.2.3.3.
CSCvj91815	Invalid Http response (IO error during SSL communication) when trying to copy a file from CSM to ASA
CSCvj91858	Cisco Adaptive Security Appliance Access Control List Bypass Vulnerability
CSCvj92048	Large Config and ACL May Cause Data Interface Health Check Fail on Slave Join
CSCvj92444	ASA keeps Type 7 NSSA after losing neighbor
CSCvj95451	webvpn-17-rewriter: Bookmark logout fails on IE
CSCvj97157	WebPage is not loading due to client rewriter issue on JS files
CSCvj97213	ASA IKEv2 capture type isakmp is saving corrupted packets or is missing packets
CSCvj97514	ASA Smart Licensing messaging fails with 'nonce failed to match'
CSCvj98964	ASA may traceback due to SCTP traffic
CSCvk00985	ASA: 9.6.4, 9.8.2 - Failover logging message appears in user context
CSCvk02250	"show memory binsize" and "show memory top-usage" do not show correct information (Complete fix)

Caveat ID Number	Description
CSCvk04592	Flows get stuck in lina conn table in half-closed state
CSCvk08377	ASA 5525 running 9.8.2.20 memory exhaustion.
CSCvk08535	ASA generates warning messages regarding IKEv1 L2L tunnel-groups
CSCvk11898	GTP soft traceback seen while processing v2 handoff
CSCvk13703	ASA5585 doesn't use priority RX ring when FlowControl is enabled
CSCvk14537	SSH/Telnet Management sessions may get stuck in pc ftpc_suspend
CSCvk14768	ASA traceback with Thread Name: DATAPATH-1-2325
CSCvk18330	Active FTP Data transfers fail with FTP inspection and NAT
CSCvk18378	ASA Traceback and reload when executing show process (rip: inet_ntop6)
CSCvk18578	Enabling compression necessary to load ASA SSLVPN login page customization
CSCvk19435	Unwanted IE present error when parsing GTP APN Restriction
CSCvk20381	Traceback loop seen on fresh ASAv Azure, KVM and VMWare deployments
CSCvk26887	Certificate import from Local CA fails due to invalid Content-Encoding
CSCvk27686	ASA may traceback and reload when accessing qos metrics via ASDM/Telnet/SSH
CSCvk29263	SSH session stuck after committing changes within a Configure Session.
CSCvk30665	ASA "snmp-server enable traps memory-threshold" hogs CPU resulting in "no buffer" drops
CSCvk30739	ASA CP core pinning leads to exhaustion of core-local blocks
CSCvk31035	KVM (FTD): Mapping web server through outside not working consistent with other platforms
CSCvk34648	Firepower 2100 tunnel flap at data rekey with high throughput Lan-to-Lan VPN traffic
CSCvk36087	When logging into the ASA via ASDM, syslog 611101 shows IP as 0.0.0.0 as remote IP
CSCvk36733	mac address is flapping on huasan switch when asa etherchannel is configured with active mode
CSCvk38176	Traceback and reload due to GTP inspection and Failover
CSCvk43865	Traceback: ASA 9.8.2.28 while doing mutex lock
CSCvk45443	ASA cluster: Traffic loop on CCL with NAT and high traffic
CSCvk47583	ASA WebVPN - incorrect rewriting for SAP Netweaver

Caveat ID Number	Description
CSCvk50815	GTP inspection should not process TCP packets
CSCvk51181	FTD IPV6 traffic outage after interface edit and deployment part 1/2
CSCvk54779	Async queue issues with fragmented packets leading to block depletion 9344
CSCvk57516	Low DMA memory leading to VPN failures due to incorrect crypto maps
CSCvk66771	The CPU profiler stops running without having hit the threshold and without collecting any samples.
CSCvk66963	ASA 9.8.3 Smart Licensing Default Config Incorrect
CSCvk67239	FTD or ASA traceback and reload in "Thread Name: Logger Page fault: Address not mapped"
CSCvk67569	ASA unable to handle Chunked Transfer-encoding returned in HTTP response pages in Clientless WebVPN
CSCvk70676	Clientless webvpn fails when ASA sends HTTP as a message-body
CSCvk72192	"Free memory" in "show memory" output is wrong as it includes memory utilisation due to overhead
CSCvk72958	Qos applied on interfaces doesn't work.
CSCvm00066	ASA is stuck on "reading from flash" for several hours
CSCvm01053	ASA 9.8(2)24 traceback on FPR9K-SM-44
CSCvm07458	Using EEM to track VPN connection events may cause traceback and reload
CSCvm08769	Standby unit sending BFD packets with active unit IP, causing BGP neighborship to fail.
CSCvm17985	Initiating write net command with management access for BVI interfaces does not succeed
CSCvm19791	"capture stop" command doesn't work for asp-drop type capture
CSCvm23370	ASA: Memory leak due to PC cssls_get_crypto_ctxt
CSCvm24706	GTP delete bearer request is being dropped
CSCvm25972	ASA Traceback: Thread Name NIC Status Poll.
CSCvm34983	IPSEC RAVPN on Spyker fails due to IKEv2 Xuauth install failure
CSCvm36138	With v1 host configured, a v2c walk from that host succeeds
CSCvm36362	Route tracking failure
CSCvm43975	Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability

Caveat ID Number	Description
CSCvm49283	Make Object Group Search Threshold disabled by default, and configurable. Causes outages.
CSCvm50421	ASA traceback on slave/standby during sync config due to OSPF/EIGRP and IPv6 used together in ACE
CSCvm53531	Cisco Adaptive Security Appliance Software Privilege Escalation Vulnerability
CSCvm54827	Firepower 2100 ASA Smart Licensing Hostname Change Not Reflected in Smart Account
CSCvm55091	HA failed primary unit shows active while "No Switchover" status on FP platforms
CSCvm56019	Cisco Adaptive Security Appliance WebVPN - VPN not connecting through Browser
CSCvm56371	ASA wrongly removes dACL for all Anyconnect clients which has the same dACL attached
CSCvm56719	Traceback high availability standby unit Thread Name: vpnfol_thread_msg
CSCvm65725	ASA kerberos auth fails switch to TCP if server has response too big (ERR_RESPONSE_TOO_BIG)
CSCvm67273	ASA: Memory leak due to PC alloc_fo_ipsec_info_buffer_ver_1+136
CSCvm72378	ASA: CLI: User should not be allowed to create network object "ANY"
CSCvm78449	Unable to modify access control license entry with log default command
CSCvm80779	ASA not inspecting H323 H225
CSCvm80874	ASAv/FP2100 Smart Licensing - Unable to register/renew license
CSCvm82290	ASA core blocks depleted when host unreachable in IRB configuration
CSCvm82930	FTD: SSH to ASA Data interface fails if overlapping NAT statement is configured
CSCvm85257	Spin lock traceback when changing vpn-mode with traffic
CSCvm86443	Only first line of traceroute is captured in event manager output
CSCvm87970	Webvpn Clientless- password management issue
CSCvm91014	NTP synchronization don't work when setting BVI IF as NTP source interface
CSCvm95669	ASA 5506 %Error copying http://x.x.x.x/asasfr-5500x-boot-6.2.3-4.img(No space left on device)
CSCvn03966	FTD - When "object-group-search" is pushed through flexconfig, all ACLs get deleted causing outage.
CSCvn09322	FTD device rebooted after taking Active State for less than 5 minutes
CSCvn09367	Prevent administrators from installing CXSC module on ASA 5500-X

Caveat ID Number	Description
CSCvn09583	show memory has negative values for used memory when low memory condition hit
CSCvn09640	FTD: Need ability to trust ethertype ACLs from the parser. Need to allow BPDU to pass through
CSCvn13556	port-channel IF's Interface number is displayed un-assigned when running at transparent mode
CSCvn15757	ASA may traceback due to SCTP traffic inspection without NULL check
CSCvn17347	Traceback and reload when displaying CPU profiling results
CSCvn19823	ASA : Failed SSL connection not getting deleted and depleting DMA memory
CSCvn22833	ADI process fails to start on ASA on Firepower 4100
CSCvn23254	SNMPv2 pulls empty ifHCInOctets value if Nameif is configured on the interface
CSCvn29446	Keepout configuration on the active ASA can not be synchronized to the standby ASA
CSCvn30108	The 'show memory' CLI output is incorrect on ASAv
CSCvn30393	ASA Traceback in emweb/https during Anyconnect Auth/DAP assessment
CSCvn31347	ACL Unable to configure an ACL after access-group configuration error
CSCvn32620	IKEv2 Failed to obtain an Other VPN license
CSCvn32657	ASA traceback when removing interface configuration used in call-home
CSCvn33943	Standby node traceback in wccp_int_statechange() with HA configuration sync
CSCvn35014	ASA routes change during OS upgrade
CSCvn37829	ASA should allow GCM(SSL) connections to use DMA_ALT1 when primary DMA pool is exhausted
CSCvn38453	ASA: Not able to load Quovadis Root Certificate as trustpoint when FIPS is enabled
CSCvn40592	'No certificate ' command under certificate chain removes wrong certificate
CSCvn44201	ASA discards OSPF hello packets with LLS TLVs sent from a neighbor running on IOS XE 16.5.1 or later
CSCvn44748	Specified virtual mac address could not display when executing "show interface"
CSCvn46425	AnyConnect Cert Auth w/ periodic cert auth fails if failover enabled but other device unreachable
CSCvn47599	RA VPN + SAML authentication causes 2 authorization requests against the RADIUS server
CSCvn47800	ASA stops authenticating new AnyConnect connections due to fiber exhaustion

Caveat ID Number	Description
CSCvn49180	ASA/FTD:MAC address not refreshing after changing member-interface of CCL link
CSCvn55007	DTLS fails after rekey
CSCvn61662	ASA 5500-X may reload without crashinfo written due to CXSC module continuously reloading
CSCvn62787	To support multiple retry on devcmd failure to CRUZ during flow table configuration update.
CSCvn64163	ASA's fail to reboot after power cycle if disk is FSCK'd
CSCvn64418	ISA3000 interoperability issue with Nokia 7705 router
CSCvn67222	DPD doesn't work following a failover, which can (in rare cases) cause an outage if things fail back
CSCvn68527	KP:AnyConnect used IP from pool shows as available
CSCvn69213	ASA traceback and reload due to multiple threads waiting for the same lock - watchdog
CSCvn73962	ASA 5585 9.8.3.14 traceback in Datapath with ipsec
CSCvn76829	ASA as an SSL Client Memory Leak in Handshake Error path
CSCvn78174	traceback on inspect_process
CSCvn78870	ASA Multicontext traceback and reload due to allocate-interface out of range command
CSCvn80394	ASA SNMP CPU Hogs
CSCvn94100	"Process Name: lina" ASA traceback caused by Netflow
CSCvn96898	Memory Leak in DMA_Pool in binsize 1024 with SCP download
CSCvn97591	Packet Tracer fails with "ERROR: TRACER: NP failed tracing packet", with circular asp drop captures
CSCvn97733	Syslog ID 111005 generated incorrectly
CSCvo02097	Upgrading ASA cluster to 9.10.1.7 cause traceback
CSCvo03808	Deploy from FMC fails due to OOM with no indication of why
CSCvo06216	Support more than 255 chars for Split DNS-commit issue in hanover for CSCuz22961
CSCvo11077	Memory leak found in IPsec when we establish and terminate a new IKEv1 tunnel.
CSCvo12057	DHCPRelay does not consume DHCP Offer packet with Unicast flag
CSCvo12504	Failover fsm gets stuck in a multicontext active/active in case of module difference.
CSCvo13497	Unable to remove access-list with 'log default' keyword

Caveat ID Number	Description
CSCvo15497	Tunnel Group: 'no ikev2 local-authentication pre-shared-key' removes local cert authen
CSCvo17775	EIGRP breaks when new sub-interface is added and "mac-address auto" is enabled
CSCvo23222	AnyConnect session rejected due to resource issue in multi context deployments
CSCvo27109	Standby may enter reboot loop upon upgrading to 9.6(4)20 from 9.6(4)6
CSCvo42174	ASA IPsec VPN EAP Fails to Load Valid Certificate in PKI
CSCvo43795	OSPF Process ID doesnot change even after clearing OSPF process
CSCvo45230	ASA5506 - IBR - not able to ping with hostname if the interface is in BVI in IBR mode
CSCvo47562	VPN sessions failing due to PKI handles not freed during rekeys
CSCvo51265	SCP large file transfer to the box result in a traceback
CSCvo55151	crypto ipsec inner-routing-lookup should not be allowed to be configured with VTI present
CSCvo56675	ASA traceback and reload when trying to switch from ACTIVE to STANDBY. Thread Name: fover_FSM_thread
CSCvo58030	Failover mac address configured on interface does not allow to delete subinterface
CSCvo62031	ASA Traceback and reload while running IKE Debug
CSCvo63240	Smart Tunnel bookmarks don't work after upgrade giving certificate error
CSCvo64516	ASA fails command authorization if tcp syslog is down.
CSCvo66534	Traceback and reload citing Datapath as affected thread
CSCvo74350	ASA may traceback and reload. Potentially related to WebVPN traffic
CSCvo93872	Memory leak while inspecting GTP traffic

Resolved Bugs in Version 9.8(3)

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

Caveat ID Number	Description
CSCsj42456	ASA 8.0: CSCOPF.CAB has expired Code Signing cert .
CSCth11758	aggregate-auth debugs should mask passwords
CSCuj98977	ASA Traceback in thread SSH when ran "show service set conn detail"
CSCuu67159	ASA: traceback in DATAPATH-2-1157
CSCuv68725	ASA unable to remove ACE with 'log disable' option

Caveat ID Number	Description
CSCuy57310	Cisco Adaptive Security Appliance Traffic Flow Confidentiality Denial of Service Vulnerability
CSCuy60200	ASA traceback in Unicorn Proxy Thread
CSCva92997	9.7.1 traceback in snp_fp_qos
CSCvb53233	ASA 9.1(7)9 Traceback with %ASA-1-199010 and %ASA-1-716528 syslog messages
CSCvb97470	asa Rest-api - component monitoring - empty value/blank value
CSCvd20408	Threat Defense: Interface capture on ASA CLI causes all traffic to be dropped on data-plane
CSCvd33004	_lina_assert in createFoverInterface when configuring failover
CSCvd44525	ASA "show tech" some commands twice, show running-config/ak47 detailed/startup-config errors
CSCvd53381	ASA Traceback when saving/viewing the configuration due to time-range ACLs
CSCvd67907	ASA SSL client does not respond to renegotiation request
CSCvd86411	ASA 9.6.2.11 - Intermittent authentication with CTP uauth in cluster
CSCve02467	ENH: Lower timeout for igp stale-route should be reduced to a value lower than 10 seconds
CSCve18902	Cisco Adaptive Security Appliance TLS Denial of Service Vulnerability
CSCve20395	ASA Portal Java plug-ins fail with the latest Java updates
CSCve34335	Cisco Adaptive Security Appliance TLS Denial of Service Vulnerability
CSCve61540	Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities
CSCve72964	Traceback in DATAPATH-1-2084 ASA 9.(8)1
CSCve73025	All 1700 "4 byte blocks" were depleted after a weekend VPN load test.
CSCve77049	ASA Memory depletion due to scansafe inspection
CSCve78652	ASA Traceback on Kenton in Thread Name: CTM message handler
CSCve84791	Capturing asp-drop causes unexpected ASA failure
CSCve93327	Snort IAB on FTD requires PDTS to provide perfstat
CSCve94349	SNMP::User is not added to a user-list or host ,after reconfigure it.
CSCve94917	Stale VPN Context issue seen in 9.1 code despite fix for CSCvb29688
CSCve97874	ASA: Low free DMA Memory on Versions 9.6 and later (Applies to ASA 5515 ONLY)

Caveat ID Number	Description
CSCvf04004	AnyConnect multi-cert auth fails with IPsec and tunnel group URL
CSCvf10327	ENH: Unique IPv6 link-local addresses assigned when sub-interface is being created
CSCvf16310	IPv6 Addresses intermittently assigned to AnyConnect clients
CSCvf17214	ASA Exports ECDSA as corrupted PKCS12
CSCvf18160	ASA traceback on failover sync with WebVPN and shared storage-url config
CSCvf22930	FTD on 2100/4100/9300 Traceback in DATAPATH due to flow offload
CSCvf25666	An ASA with low free memory fails to join existing cluster and could traceback and reload
CSCvf26463	ASA 9.8.1 BVI in routed mode is not doing route lookup for traffic generated from ASA
CSCvf28292	DAP config restored but inactive after backup restore
CSCvf28749	ASA not sending register stop when mroute is configured
CSCvf30738	ASA crashes on DATAPATH due to SIP traffic hitting dynamic NAT rule
CSCvf37947	ASA creates a BVi0 interface on a custom routed context
CSCvf39539	Netflow Returns Large Values for Bytes Sent/Received and IP address switch
CSCvf39679	Unable to add new networks to existing EIGRP configuration
CSCvf40179	ERROR: Unable to create crypto map: limit reached, when adding entry
CSCvf40650	Certificates not synced to Standby/All certificates cleared on Standby post deployment failure
CSCvf43019	Webvpn rewriter failing for internal URL
CSCvf43150	ASA// 9.6 // FTP inspection does not allocate new NAT entrie for DATA traffic on Active FTP with PAT
CSCvf43650	OSPF route not getting installed on peer devices when an ASA failover happens with NSF enabled
CSCvf46168	"no capture <name> stop" doesn't change capture status from Stopped
CSCvf49899	ENH: GOID allocation and sync cleanup
CSCvf51066	ASA on FXOS is sending SNMP Ifspeed OID (1.3.6.1.2.1.2.2.1.5) response value = 0
CSCvf54981	ASA - 80 Byte memory block depletion
CSCvf56506	ASA 9.6(2), 9.6(3) traceback in DataPath

Caveat ID Number	Description
CSCvf56774	KP: CPU hogs on standby ASA in fover_parse when performing "write mem all" on active ASA
CSCvf56917	ASA doesn't send LACP PDU during port flap in port-channel
CSCvf57908	Transparent Firewall: Ethertype ACLs installed with incorrect DSAP value
CSCvf59524	Optimization: Allow multiple DATAPATH threads to read compiling tmatch structure in parallel
CSCvf61419	Traceback in thread DATAPATH due to NAT
CSCvf62365	ASA: entConfigChange is unexpectedly sent when secondary ASA is reloaded
CSCvf63108	ASA drops the IGMP Report packet which has Source IP address 0.0.0.0
CSCvf63718	Cisco Adaptive Security Appliance Flow Creation Denial of Service Vulnerability
CSCvf64643	ERROR on Firepower Threat Defense device: Captive-portal port not available. Try again
CSCvf68666	FP2100 IFT customer cannot use ASDM to download image to pc
CSCvf72068	FXOS - ASA/FTD standby unit in transparent mode may still traffic for offloaded flows
CSCvf72930	Firepower Threat Defense may traceback in Thread Name appAgent_monitor_nd_thread during registration
CSCvf74218	ASAv image in AWS GovCloud not working in Hourly Billing Mode
CSCvf76013	ASA crash with snp_egress_capture_sgt()
CSCvf76281	IKEv2 RA cert auth. Unable to allocate new session. Max sessions reached
CSCvf77377	Hostscan: Errors in cscan.log downloading Microsoft and Panda .dll files
CSCvf79262	OpenSSL CVE-2017-3735 "incorrect text display of the certificate"
CSCvf80539	management-only comes back after reboot
CSCvf81222	Memory leak in 112 byte bin when packet hits PBR and connection is built
CSCvf81672	ASA Routes flushed after failover when etherchannel fails
CSCvf81932	'Incomplete command' error with some inspects due to K7 license
CSCvf82832	ASA : ICMPv6 syslog messages after upgrade to 962.
CSCvf83537	Traceback with traffic in 3 node Intra Chassis Cluster
CSCvf83709	Slave kicked out due to CCL link failure and rejoins, but loses v3 user in multiple context mode

Caveat ID Number	Description
CSCvf85065	ASA: Traceback by Thread Name idfw_proc
CSCvf87899	ASA - rare scheduler corruption causes console lock
CSCvf89504	ASA cluster intermittently drop IP fragments when NAT is involved
CSCvf90278	ASA/Firepower Threat Defense traceback when enabling or clearing the packet capture buffer
CSCvf91098	Cisco Firepower 2100 Series Security Appliances IP Fragmentation Denial of Service Vulnerability
CSCvf92262	ASA Webvpn HTTP Strict-Transport-Security Header missing despite fix of CSCvc82150
CSCvf94973	ASA on FP 2100 traceback when uploading AnyConnect image via ASDM or show file system
CSCvf96773	Standby ASA has high CPU usage due to extremely large PAT pool range
CSCvg00265	ASA fails to rejoin the failover HA Or a cluster with insufficient memory error, OGS enabled
CSCvg00565	ASA crashes in glib/g_slice when do "debug menu" self testing
CSCvg01016	ASA does not create pinholes for DCERPC inspection, debug dcerpc shows "MEOW not found".
CSCvg01132	ASA : After upgrading from 9.2(4) to 9.2(4)18 serial connection hangs
CSCvg01827	Permanent License Reservation license not installed on ASA v
CSCvg05250	"clear local-host <IP>" deletes all stub flows present in the entire ASA cluster for all hosts/conns
CSCvg05368	Upon joining cluster slave unit generates ASA-3-202010: NAT/PAT pool exhausted for all PAT'd conns
CSCvg05442	ASA traceback due to deadlock between DATAPATH and webvpn processes
CSCvg06695	Firepower 2100 Threat Defense pair reporting failed status due to "Detect service module failure"
CSCvg07197	ASA : High memory utilization when inspection enabled
CSCvg08891	iPhone IKEv2 PKI leaks over Wi-Fi using local certificate authentication on ASA 5555 9.6.3
CSCvg09778	ASA-SSP HA reload in CP Processing due to DNS inspect
CSCvg12376	Chunk memory not released back to the system after stopping traffic
CSCvg17478	Traceback with Show OSPF Database Commands

Caveat ID Number	Description
CSCvg20796	ASA local DNS resolution fails when DNS server is reachable over a site to site sec VPN tunnel
CSCvg21077	One node rejoined and traffic restarted will cause the unit 100% CPU due to snpi_untranslate
CSCvg23028	REST-API residues on Firepower Threat Defense (2100, 4100, 9300 Series)
CSCvg23945	ASA panic/crash spin_lock_fair_mode_enqueue: Lock (mps_shash_bucket_t) is held for a long time
CSCvg25175	ASA getting stuck in hung state because of STATIC NAT configuration for SNMP ports
CSCvg25538	FORWARD PORT: 1550/2048/9344 byte memory block depletion due to identity UDP traffic
CSCvg25694	Crash on Standby Firepower 4140 module after Policy deployment.
CSCvg25983	ASA Inter-Site Clustering - Extra ARP not generated when ASA receives unicast ARP request
CSCvg26548	High CPU observed with SFR monitoring mode
CSCvg28370	Traceback on ASA with Firepower Services during NAT rule changes and packet capture enabled
CSCvg29442	When IPsec is enabled, high availability goes in Active-Failed state
CSCvg29692	ASA, when acting as an HTTP client (file copy, etc) sometimes fail to close the connection
CSCvg30391	ASA SNMP OID for ifInDiscards always 0
CSCvg32179	Javascript elements rewriter issue
CSCvg32530	ASA broadcasting packets sent to subnet address as destination IP
CSCvg33669	"OCTEON:DROQ[8] idx: 494 len:0" message appearing on console access of the device
CSCvg33985	Cisco Adaptive Security Appliance WebVPN Cross-Site Scripting Vulnerability
CSCvg35618	Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability
CSCvg38437	ASA AC client PKI username from cert longer than 64 characters - radius username is cut short to 64
CSCvg39447	SNMP deployment failure causes policy rollback
CSCvg39694	FP4120 / ASA 9.6(3)230 "established tcp" not working anymore after SW upgrade
CSCvg43389	ASA traceback due to 1550 block exhaustion.

Caveat ID Number	Description
CSCvg44785	Offloaded flows fail to update their idle timer resulting in connections being incorrectly timed out
CSCvg45952	ASA traceback: thread name scansafe
CSCvg51984	High CPU in IKE Daemon causing slow convergence of VPN tunnels in a scaled environment
CSCvg52545	9300 pair NGFWs in inlineIPS mode do not trigger SNAP packet updates with proper VLAN tags
CSCvg52995	Unable to save configuration in system context after enabling password encryption in ASA
CSCvg53981	"dir /recursive cache:/stc" and "dir cache:stc/2/" list AnyConnect.xsd differently on ASA9.8.2
CSCvg54185	ASA 5506 running on 9.8.2.8 version, memory block of size 80 is getting depleted
CSCvg55617	ASA 9.8.1+ IKEv2 vpn load-balancing sends DELETE following IKE_AUTH
CSCvg56122	SSL handshake fails with large certificate chain size
CSCvg56493	ASA L2TP/IPSEC SMB upload of big files fails - tcp-buffer-timeout drops
CSCvg57954	Modifying service object-groups (add and remove objects) removes ACE
CSCvg58385	ASA reports incorrectly double input packets traffic on PPPoe/VPDN interface
CSCvg58941	Elevated CPU Using Flow-Offload & High Rate of Flow Table Collisions
CSCvg61799	Sysopt permit-vpn behavior change to prevent unintended clear-text traffic
CSCvg61829	SSH/Telnet Traffic, 3-WHS, ACK packets with data is getting dropped - reason (intercept-unexpected)
CSCvg62916	ASA: Software traceback in Thread Name: Dynamic Filter updater
CSCvg65072	Cisco ASA sw, FTD sw, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability
CSCvg66606	GTP echo response is dropped in ASA cluster
CSCvg67135	ASA backs out of connection when it receives Server Key exchange with named curve as x25519
CSCvg68914	segfault while processing TCP traffic (StreamQueue).
CSCvg72276	Direct Authentication is not working in ASA cluster.
CSCvg73231	ASA/FTD: OSPFv3 stops redistributing routes due to missing LSA after failover
CSCvg81583	Split brain after recovery from interface failure when fover and then data ifc goes down in order.

Caveat ID Number	Description
CSCvg82650	RDP session does not establish after changing SSL certificate on ASA.
CSCvg82932	Memory Leaking on ASA with vpnfol_memory_allocate and vpnfol_data_dyn_string_allocator
CSCvg83623	FTD: IPv6 traffic is not being load-balanced as per 5-tuple algorithm
CSCvg85765	Kenton: ASA5506 traceback on policy deploy
CSCvg85982	ERSPAN not working on Firepower Threat Defense running 6.2.2
CSCvg89102	ASA:multi-session command being configured after write erase
CSCvg89215	ASA crashed with Thread name DATAPATH-1-27929 in 3 node Firepower 9300 Distributed Cluster
CSCvg90061	CSM failed to parse the tcp-state-bypass logs
CSCvg90365	icmp/telnet traffic fail by ipv6 address on transparent ASA
CSCvg90403	Blocks of size 80 leak observed when IRB is used in conjunction with multicast traffic
CSCvg90820	SSPs with ASA in multiple context moves in active-active situation while failover is occurring
CSCvg91038	NAT'd traffic with flow offload is not working in transparent mode.
CSCvg97541	Firepower Threat Defense prefilter policy only fast-paths single direction of bidirectional flow
CSCvg98106	ASA ping to IPv6 address selects egress interface source IP instead of specified source IP
CSCvh03889	Failover Master Passphrase Crash via ASDM
CSCvh05081	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module
CSCvh05193	ARP traffic should not be hardcoded to be sent to Snort for inspection
CSCvh13415	ASA:OpenSSL Vulnerabilities CVE-2017-3737 and CVE-2017-3738
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvh15344	snmp: After upgradet to 9.6(3)1, the snmpwalk results are different
CSCvh20742	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvh23085	Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities
CSCvh23089	ACLs with source objects that are ranges incorrectly track hit counts

Caveat ID Number	Description
CSCvh23776	Both ASA traceback in high availability pair on 4140 chassis
CSCvh27703	ASA - Traceback in thread name SSH while applying BGP show commands
CSCvh28309	ASDM stops working with hostscan enabled. ASDM works with hostscan disabled.
CSCvh28763	ASA takes significant time to send ICMPv6 echo when pinging.
CSCvh30261	ASA watchdog traceback during context modification/configuration sync
CSCvh32323	Memory leak in idfw component on ASA
CSCvh32673	Freed memory not released back to the system quick enough on ASA 5506-x platforms
CSCvh44149	ASAv5: Low free DMA memory on 9.8(2) and later
CSCvh46202	Slow 2048 byte block leak due to fragmented traffic over VPN
CSCvh47057	ASA - ICMP flow drops with "no-adjacency" on interface configured in zone when inspection enabled
CSCvh48662	'no snmp-server host <interface> <ip-address>' does not work
CSCvh50032	Unable to completely disable scansafe application health checking
CSCvh53276	IPv6 protocol 112 packets passing through L2FW are dropping with Invalid IP length message
CSCvh53616	ASA on Firepower Threat Defense devices traceback due to SSL
CSCvh54940	ASA traceback with thread name "idfw_proc "
CSCvh55035	Firepower Threat Defense device unable to stablish ERSPAN with Nexus 9000
CSCvh56214	ASA and putty: Incoming packet was garbled on decryption
CSCvh56378	ASA backup command fails to backup identity certificate
CSCvh62164	Firepower 9300 standby stuck in Bulk-Sync state with high CPS traffics on active
CSCvh63896	ASA traceback in threadname CP Processing
CSCvh67981	ASA 9.8.2 Cluster Slave unit traceback when joining cluster and SNMPv3 sync
CSCvh69967	5506 traceback when ASA module and RestAPI both enabled
CSCvh71738	FQDN object are getting resolved after removing access-group configuration
CSCvh72007	Username and privilege display are incorrect when x-auth-token is used for REST API
CSCvh73582	traceback related to SIP inspection processing
CSCvh75025	ASA traceback when failing over to standby unit
CSCvh75060	Rest-API gives empty response for certain queries

Caveat ID Number	Description
CSCvh77942	new Certificate configuration of primary unit does not sync to standby unit in a Active/Active setup
CSCvh79732	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81737	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81870	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh83026	ASA tracebacks intermittently with Thread Name: CTM message handler
CSCvh83145	ASA interface IP and subnet mask changes to 0.0.0.0 0.0.0.0 causing outage of services on interface
CSCvh85514	ASA Traceback in Thread Name: Unicorn Proxy Thread
CSCvh89431	Skinny inspection in Routed ASA with BVIs not letting SCCP phones to register or denying SCCP calls
CSCvh90944	IP address in DHCP GIADDR field is reversed after sending DHCP DECLINE to DHCP server
CSCvh90947	ASA traceback with Thread Name: fover_parse
CSCvh91053	ASA sending DHCP decline not assigning address to AC clients via DHCP
CSCvh91399	upgrade of ASA5500 series firewalls results in boot loop (not able to get past ROMMON)
CSCvh92381	ASA Traceback and goes to boot loop on 9.6.3.1
CSCvh95325	Standby ASA traceback during replication from mate 9.2(4)27
CSCvh95456	Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities
CSCvh97782	KP traceback illegal memory access inside a vendor Modular Exponentiation implementation
CSCvh99159	RADIUS authentication/authorization fails for ASDM
CSCvh99896	[ASA]-Master agent is missing user on standby device in multi-context mode
CSCvi01312	webvpn: multiple rendering issues on Confluence and Jira applications
CSCvi01376	Upon reboot, non-default SSL commands are removed from the Firepower 4100
CSCvi06120	vpn-idle-timeout is not triggered after switching to rebooted failover pair
CSCvi07636	ASA: Traceback in Thread Name UserFromCert
CSCvi08450	CWS redirection on ASA doesn't treat SSL Client Hello retransmission properly in specific condition

Caveat ID Number	Description
CSCvi16029	Cisco Adaptive Security Appliance WebVPN Denial of Service Vulnerability
CSCvi16264	ASA traceback and reload due to watchdog timeout when DATAPATH accesses compiling ACL structure
CSCvi19263	ASA 9.7.1.15 Traceback while releasing a vpn context spin lock
CSCvi22507	IKEv1 RRI : With Answer-only Reverse Route gets deleted during Phase 1 rekey
CSCvi23766	IKEv2 stuck Tunnel Manager Entries
CSCvi33962	WebVPN rewriter: drop down menu doesn't work in BMC Remedy
CSCvi35805	ASA Cut-Through Proxy allowing user to access website, but displaying "authentication failed"
CSCvi37889	Packet Tracer fails with "ERROR: TRACER: NP failed tracing packet", even after removing captures
CSCvi42965	ASA does not report accurate free memory under "show memory" output
CSCvi45567	Not able to do snmpwalk when snmpv1&2c host group configured.
CSCvi45807	ASA: dns expire-entry-timer configuration disappears after reboot
CSCvi46573	ASA: IKEv2 S2S VPN with a dynamic crypto map - ASP table not programmed correctly
CSCvi55070	IKEv1 RRI : With Originate-only Reverse Route gets deleted during Phase 1 rekey
CSCvi58045	interface shutdown command not replicating in HA.
CSCvi58089	Memory leak on webvpn
CSCvi64007	Zeroize RSA key after Failover causes REST API to fail to changeto System context
CSCvi66291	ASA far exceeds 100% rate in TCP Intercept output
CSCvi66905	PIM Auto-RP packets are dropped after cluster master switchover
CSCvi68495	Standby ASA not sending NTP packets to NTP server
CSCvi70606	ASA 9.6(4): WebVPN page not loading correctly
CSCvi76577	ASA:netsnmp:Snmpwalk is failed on some group of IPs of a host-group.
CSCvi77352	Illegal update occurs when device removes itself from the cluster
CSCvi80849	Cisco Firepower 2100 Series POODLE TLS security scanner alerts
CSCvi81436	ASA Lots of 'PPPoE daemon not configured' messages are outputted in console
CSCvi82779	ASA generate traceback in DATAPATH thread

Caveat ID Number	Description
CSCvi86799	ASA traceback during output of "show service-policy" with a high number of interfaces and qos
CSCvi87921	ASA self-signed RSA certificate is not allowed for TLS in FIPS mode
CSCvi89194	pki handles: increase and fail to decrement
CSCvi95544	ASA not matching IPv6 traffic correctly in ACL with "any" keyword configured
CSCvi97776	show environment output incompletely from show tech
CSCvj22929	Reapplying Certificate Chain Configuration Renders LOCAL CA TP Status "Not Authenticated"
CSCvj25817	ASA responds to MOBIKE but clears SA due to DPD.
CSCvj26450	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
CSCvj39858	Traceback: Thread Name: IPsec message handler
CSCvj43591	Firepower 2110 with ASA DHCP does not work properly
CSCvj46777	FPR 2100 asa traceback for unknown reason
CSCvj48542	Trustsec SXP delete hold down timer value needs to be configurable
CSCvj56008	Scansafe feature doesn't work at all for HTTPS traffic

Resolved Bugs in Version 9.8(2)

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

Caveat ID Number	Description
CSCse02836	ASDM: doesn't show the source port, even when an ACE has one
CSCto19051	Resolve any vulnerabilities in ASA/FTD lina Heimdal Kerberos code
CSCto19832	OpenLDAP needs to be upgraded or patched in ASA/FTD lina process
CSCuj69650	ASA block new conns with "logging permit-hostdown" & TCP syslog is down
CSCuu90811	TLS CTP does not work in TLSv1.2 when GCM ciphers are used
CSCuv63875	ASA traceback in Thread Name:ci/console while running show ospf commands
CSCuw37752	FTP data conn scaling fails with dynamic PAT
CSCuz22961	Support for more than 255 characters for Split DNS value
CSCuz52474	Evaluation of pix-asa for OpenSSL May 2016
CSCuz72137	ASA dropping packets with "novalid adjacency" though valid ARP entry avail

Caveat ID Number	Description
CSCuz77293	OSPF multicast filter rules missing in cluster slave
CSCva69652	NGFW CLI 'show tech-support' missing SNORT data
CSCva92997	9.7.1 traceback in snp_fp_qos
CSCvb40875	Default inspect statements are missing on ASA 5500-x and 2100 device running Threat Defense
CSCvb75685	EZVPN NEM client can't reconnect after "no vpnclient enable" is entered
CSCvb91810	ASA - Incorrect interface-based route-lookup if more specific route exist out different interface
CSCvb93926	ENH: Remove DES and 3DES from ASDM AnyConnect IKEv2 Wizard
CSCvc07112	Implement detection and auto-fix capability for scheduler corruption problems
CSCvc27704	Logs lost when TCP is used as transport protocol for Syslogs
CSCvc56526	CEP records edit page take minutes to load
CSCvc72860	Implement debugs to troubleshoot issue where flash becomes read only after ASA is up a long time.
CSCvc76146	981 VTI - Slow BGP neighbor formation after state change
CSCvc82150	PSB Requirement SEC-HTP-HSTS.x4i : HTTP Strict-Transport-Security Header
CSCvc82270	ASA 1550 block gradual depletion
CSCvc83462	gzip compression not working via Webvpn
CSCvc85369	ASA does not respond to IPv6 MLD Query.
CSCvc96614	ASA: IKEv2 ipsec-proposal command removed if more than 9 proposals configured in single command
CSCvd00293	VTI - Some sessions do not get cleared from vpn-sessiondb
CSCvd01101	Syslog logging messages performance is low with tcp protocol
CSCvd01130	ASA TCP SIP inspection translation not working when IP phone is behind VPN tunnel
CSCvd03718	Error configuring the interface in multi-context mode
CSCvd05267	Copy to running-config with a loop reloads the box with no indication as to why
CSCvd17581	ASA IKEv1: Set non-zero SPI in INVALID_ID_INFO Notify
CSCvd20013	Traceback in "Thread Name: IPsec message handler" on EZVPN client
CSCvd25094	Traceback when modifying interfaces. Assert in interface_action.c

Caveat ID Number	Description
CSCvd26699	ASA erroneously triggers syslog ID 201011
CSCvd28780	Crash when clearing interface configuration and NAT
CSCvd35811	Traceback in thread name DATAPATH
CSCvd36992	Ether-channel: 5585-60 LACP state shows SYSTEM ID of old neighbor on interface which is in disabled
CSCvd37850	9.6.2 DHCPR: Maximum relay bindings (500) exceeded
CSCvd43471	Packets encrypted through virtual tunnel interface have source MAC of 0000.0000.0000
CSCvd46434	ASA crashes after entering the command "debug menu ike-common 11"
CSCvd49262	Traceback when trying to save/view access-list with giant object groups (display_hole_og)
CSCvd49550	ASA with 9.5.1 and above does not show SXP socket when managment0/0 is used as src-ip
CSCvd50107	ASA traceback in Thread name: idfw_proc on running "show access-list", while displaying remark
CSCvd53381	ASA Traceback when saving/viewing the configuration due to time-range ACLs
CSCvd55115	ASA in cluster results in incorrect user group mappings between the Master and Slave
CSCvd58094	ASA traceback in ARP thread, PBR configured
CSCvd58321	Web folder filebrowser applet code signing certificate expired
CSCvd66303	Error deploying ASAv on ESXi vCenter 6.5
CSCvd69551	ASA fails to contact the secondary LDAP server with reactivation mode timed configured
CSCvd71473	ASA: slow memory leak when using many DNS queries
CSCvd75631	Threat Defense DHCP Client tries to request a DHCP address instead of declining
CSCvd76791	Sub-Interfaces Not Supported on SRIOV/IXGBE-VF
CSCvd76821	tcp-options md5 allow is pushed to slave units as tcp-options md5 clear
CSCvd76939	ASA policy-map configuration is not replicated to cluster slave
CSCvd77893	ASA may generate an assert traceback while modifying access-group
CSCvd78444	Traceback due to webvpn process configuration
CSCvd79797	ASA local dns resolution fails when dns server is reachable through a site to site ipsec tunnel

Caveat ID Number	Description
CSCvd79863	FTD OSPF with ECMP, packets are sent to peer in down state for existing connections
CSCvd80721	In security context, cannot generate the SNMP events trap.
CSCvd82064	Cisco Adaptive Security Appliance Authenticated Cross-Site Scripting Vulnerability
CSCvd82265	Increase memory allocated to rest-agent on ASAv5
CSCvd87211	ASA traceback when trying to remove configured capture
CSCvd87647	ASA traceback in Thread Name: fover_parse performing upgrade from 9.1.5 to 9.4.3
CSCvd89003	ASA traceback observed in Datapath due to SIP inspection
CSCvd89925	Unable to switch standby unit of the failover pair to active
CSCvd90071	Allow ASAv5 to operate using > 1GB memory
CSCvd90079	ASAv5: Reduce DMA packet memory to 64MB
CSCvd90096	WebVPN forces IE to use IE8 mode
CSCvd92196	ASA981 Beta: asp load-balance output inconsistent with show run vs. show run all
CSCvd92423	ASA Traceback in Unicorn Proxy Thread
CSCvd92489	L2TP/IPsec fails when transform-set with mode transport is 11th in dynamic-map
CSCvd96108	Traceback in thread name DATAPATH due to lan to lan VPN
CSCvd97249	FTD: block depletion with continuous SSL traffic and decrypt resign enabled.
CSCvd97568	FTD traceback observed during failover synchronization.
CSCvd97780	ASA/FTD giving incorrect results for "trace" output in packet capture
CSCvd99476	The interactive icons on internal bookmark site not showing properly (+CSCO+0undefined)
CSCvd99859	ASA may drop DNS reply containing only additional RR of type TXT
CSCvd99945	ASA traceback when customer was authenticating to AnyConnect
CSCve00395	ISA 3000: show tech needs to include show inventory
CSCve02469	ASA Issue with bgp route summarization(auto-summary)and route advertisement
CSCve02854	SFR Backplane is pulling the public address for policy match instead of ASA inside address
CSCve03387	Proxy ARP information for SSH NLP NAT is not updating on the FTD upon failover
CSCve03974	ASA with FirePOWER services module generates traceback and reload

Caveat ID Number	Description
CSCve04326	Slave should have use CCL to forward traffic instead of blackholing when egress interface is down
CSCve04443	ASAv Azure: Allow 750 VPN sessions on ASAv30
CSCve05841	ASA reloaded while joining cluster and active as slave
CSCve06436	Routes do not sync properly between different minor versions during hitless upgrade
CSCve07856	CRL verification fails due to incorrect KU after CSCvd41423
CSCve08898	Memory leak with capture with trace and clear capture
CSCve08947	In multi-context ASA drops traffic sourced from certain ports when interface PAT is used
CSCve09249	ASA: Active FTP not working with extended keyword in NAT.
CSCve12654	ASA clustering to support rollback feature with CSM
CSCve13410	Upgrading the ASA results in No Valid adjacency due to track configure on the route
CSCve15873	ASA: Multicast packets getting dropped starting code 9.6.3
CSCve18293	ASA traceback observed in datapath
CSCve18880	Username is not fetched from certificate when certificate map is used in clientless portal
CSCve19179	Cisco Adaptive Security Appliance WebVPN Cross-Site Scripting Vulnerability
CSCve20346	ASA SNI connection fails after upgrade - no shared cipher
CSCve20438	"activate-tunnel-group-scripts" not available in 9.6.3.1
CSCve20980	CSCOGet_origin wrapper doesn't handle 'origin' property if it belongs to Location object
CSCve21824	"hostscan data-limit" service-internal command must be exposed and documented
CSCve23033	ICMP Unreachables (PMTU) dropped indicating "Routing failed to locate next hop"
CSCve23091	Auto-RP packet is dropped due to no-route - No route to host
CSCve23155	BTF not supported on ASA application on FXOS Chassis, but smart licensing show this feature enabled.
CSCve23784	ASA may traceback on displaying access-list config or saving running config
CSCve24088	Smart Licensing ID cert renewal failure should not deregister product instance
CSCve26349	ASDM doesn't display Object Descriptions
CSCve28027	Calls not working with CUCI Lync version 11.6.3 on ASA

Caveat ID Number	Description
CSCve28639	AnyConnect Cert Auth w/ periodic cert auth fails if failover enabled but other device unreachable
CSCve29989	ASA - Traceback in DATAPATH during PAT pool socket allocation
CSCve31809	ASA corrupt dst mac address of return traffic from l2tp client
CSCve31880	network_udpmod_get not releasing shr_lock in rare error case
CSCve34335	SSL Record length verification missing in remove pad length function
CSCve34729	ASA interfaces may stop passing traffic after ASA reload with FIPS mode enabled
CSCve35799	CPU Hog CI_CONSOLE Traceback During Configuration
CSCve37948	ASA does not install routes learned via OSPF over IPSec using UDP/4500
CSCve42460	"NSF IETF/CISCO" commands getting removed on reload
CSCve42583	ASA: IPv6 protocol X rule for passing through FW is dropping packets with Invalid IP length message
CSCve43146	AnyConnect new customization creation fails on ASDM for all ASA versions above 9.5(3)
CSCve44561	ASA sends the ICMP unreachable type 3 code 4 in the wrong direction when SFR redirection enabled
CSCve46883	FTD Diagnostic Interface does Proxy ARP for br1 management subnet
CSCve47393	OSPF Rogue LSA with maximum sequence number vulnerability
CSCve48105	Slave reports Master's interface status as "init" while it is up
CSCve49968	Downloadable ACLs retrieved for Cut Through Proxy in a cluster are not marked dynamic on slaves
CSCve50118	ASA Memory Leak - RSA toolkit
CSCve53582	SSH Connections to ASA fail with SLA monitoring & nonzero floating-conn timeout
CSCve53783	"service resetoutside" impacts to-the-device traffic on all interfaces, behaves different on Standby
CSCve55694	ASDM sets service as "service tcp destination eq -1" when configuring range on service object
CSCve56153	asav in aws: asav unreachable after binary upgrade to 9.8.1
CSCve57150	vpn vlan mapping issue
CSCve57548	ASA- Traceback in 'Thread Name : Datapath' on crypto_SSL functions
CSCve58709	ASA 9.5.1 onwards, Traffic incorrectly routed instead of management interface

Caveat ID Number	Description
CSCve60829	ASA Cluster : Potential UDP loop on cluster link with PAT pool
CSCve61284	ASA Log message 414003 may be generated with bogus IP data when TCP Syslog Server down
CSCve62358	ASA 2048 block depletion when PBR next-hop is interface address
CSCve63762	ASASM: Interface vlans going to admin down after reload.
CSCve64342	'Dynamic Access Policies' page is freezed and unable to access after HS image uninstalled.
CSCve66939	Don't offer 9.8.1 as an upgrade option for ASAs in AWS
CSCve69985	ASDM does not allow more than one static MAC address table entry per interface in transparent mode.
CSCve71661	FTD - Multicast and BPDU traffic dropped due to dst-l2_lookup-fail
CSCve71712	webvpn-17-rewriter: Jira 7.3.0's login page through WebVPN portal does not render completely
CSCve72155	Memory leak at location "snp_fp_encrypt" when syslog server is reachable over the VPN tunnel
CSCve72201	ASA Webvpn Rewriter issue. Unable to browse tabs of WebSite over Clientless VPN
CSCve72227	IPsec SA fail to come up and flap with more than 1000 IPsec SA count in ASA5506/5508/5516
CSCve72433	ASDM error requesting to remove prefix-list used in route-maps for dynamic routing protocol
CSCve73556	ASA traceback on websns_rcv_tcp
CSCve75132	Start of Flow Block event has incorrect number of Initiator Bytes
CSCve76799	ENH: ASA cannot boot up when installed in KVM AHV Nutanix.
CSCve76967	ASDM Where Used option not displaying results
CSCve77440	Traceback in Unicorn Proxy Thread due to Webvpn
CSCve78986	ASA/ 9.6.3 // WebVPN Smart tunnel works but floods windows with event viewer
CSCve85698	ASA WebVPN Rewriter: WebVPN bookmark scholar.google.com not properly written
CSCve87984	Network connectivity is not enabled for more than 19 context
CSCve90305	Contexts are missing on ASA once Chassis reloads after becoming Master on 9.7 and later code
CSCve91223	Standby ASA rejects NAT rule when dest overlaps with interface IP, Active allows this

Caveat ID Number	Description
CSCve92587	Unable to copy anyconnect image via SCP to the ASA flash post upgrade to 9.8(1)
CSCve93019	ASDM Hangs when editing crypto map associated to Dynamic Site-to-Site tunnel
CSCve94828	Cannot create\edit new document with MS Office apps in SP2013
CSCve94886	Traceback on ASA with Firepower Services during NAT rule changes and packet capture enabled
CSCve95969	Unable to scale the flash virtualisation feature up to 250 contexts
CSCve97831	CDA agent stucks in 'Probing' when domain-lookup is enable
CSCve97844	ASA OSPF interface gets stuck in State DOWN (waiting for NSF) after 3rd failover
CSCve99752	Edit Second password on ASDM AC downloads but ignores the change ASA 9.8.1 higher
CSCvf01873	Regex is not matching for HTTP argument field
CSCvf03676	Ports not getting reserved on ASA after adding snmp configuration.
CSCvf07075	ASA - Crypto accelerator traceback in a loop
CSCvf08411	Display of Cipher Algorithms at ASDM is incorrect,when TLS1.2's Cipher Security Level is "medium"
CSCvf11695	Traceback: Duplicate host entries in flow-export action cause crash after policy deployment
CSCvf14391	multicast traffic sourced from anyconnect pool dropped due to reverse path checked.
CSCvf16142	ASA-5-720012:(VPN-Secondary)Failed to update IPSec failover runtime data in ASA cluster environment
CSCvf16429	Ikev2 Remote Access client sessions stuck in Delete state
CSCvf16808	Unable to SSH to Active Unit//TCP connection Limit Exceeded
CSCvf17222	SAML 2.0 (5525) 9.7.1 ASA : ASA compiler not taking the sign-in URL for SAML authentication.
CSCvf17850	ssh/snmp not working in transparent mode after giving 'clear conf int'
CSCvf19938	ASAv: Upgrade issues to the 9.7.1.4 and 9.8.1 when installed on Hyper-V Windows Server 2012-R2
CSCvf21556	ASA: SNMP Host Group not working as required for multi context configuration.
CSCvf24063	ASA5585 traceback in DATAPATH - snp_vpn_process_natt_pkt
CSCvf24387	EC Certificates that are imported to the ASA in PKCS12s cannot be used for SSL
CSCvf31539	ASA Connections stuck in idle state with DCD enabled

Caveat ID Number	Description
CSCvf35263	Port Manager Debug File portmgr.out contains incomplete Timestamps
CSCvf38655	ASA crash in fover_parse after version up
CSCvf39608	Azure-HA: 'clear configure failover' doesn't clear the Peer IP address and sometimes crashes ASAv
CSCvf41547	traceback in watchdog process
CSCvf44142	ASA 9.x: DNS inspection appending "0" on PTR query
CSCvf44950	iOS and OS X IKEv2 Native Clients unable to connect to ASA with EAP-TLS
CSCvf48785	ASA crashes with '[no] nameif' command on cluster interface while running regression
CSCvf54081	TLS version 1.1 connection failed no shared signature algorithms@t1_lib.c:3106

Resolved Bugs in Version 9.8(1.200)

We did not resolve any bugs in this release.

Resolved Bugs in Version 9.8(1)

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

Caveat ID Number	Description
CSCuj69650	ASA block new conns with "logging permit-hostdown" & TCP syslog is down
CSCum28756	ASA: Auth failures for SNMPv3 polling after unit rejoins cluster
CSCuq80704	ASA classifies TCP packets as PAWS failure incorrectly
CSCut07712	ASA - TO the box traffic break due to int. missing in asp table routing
CSCuu50708	ASA Traceback on 9.1.5.19
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
CSCuy22155	ASA generates unexpected syslog messages with mcast routing disabled
CSCuy43438	L2TP over IPSec can not be connected after disconnection from client.
CSCuy55468	Unicorn Proxy Thread causing CP contention
CSCuy60793	Duplicate link-local address observed after failover

Caveat ID Number	Description
CSCuy89288	AnyConnect DTLS on-demand DPDs are not sent intermittently
CSCuz77293	OSPF multicast filter rules missing in cluster slave
CSCva10054	ASA ASSERT traceback in DATAPATH due to sctp inspection
CSCva22048	ASA: SIP Call Drops with PAT when same media port used in multiple calls
CSCva32092	OSPFv3/IPv6 flapping every 30 min between ASA cluster and 4500
CSCva35990	Traceback on CP Process with H323 inspection, rip h323_service_early_msg
CSCva39094	ASA traceback in CLI thread while making MPF changes
CSCva43992	IKEv2 RA cert auth. Unable to allocate new session. Max sessions reached
CSCva69346	Unable to relay DHCP discover packet from ASA when NAT is matched
CSCva70095	ASA negotiates TLS1.2 when server in tls-proxy
CSCva70979	failover descriptor is not updated in Port Channel interfaces
CSCva71783	ICMP error packets in response to reply packets are dropped
CSCva76568	ASA : Enabling IKEv1/IKEv2 opens RADIUS ports
CSCva81412	ASR9000 BGP Graceful Restart doesnt work as expected
CSCva88796	AnyConnect Sessions Cannot Connect Due to Stuck L2TP Uauth Sessions
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
CSCva98240	SIP: Address from Route: header not translated correctly
CSCvb05667	H.323 inspection causes Traceback in Thread Name: CP Processing
CSCvb08776	Internal ATA Compact Flash size is incorrectly shown in "show version"
CSCvb15265	ASA Page fault traceback in Thread Name: DATAPATH
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
CSCvb29688	Stale VPN Context entries cause ASA to stop encrypting traffic despite fix for CSCup37416

Caveat ID Number	Description
CSCvb30445	ASA may generate DATAPATH Traceback with policy-based routing enabled
CSCvb31055	ASA Multiple Context SNMP PAT Interface Missing
CSCvb33009	Cisco ASA Signature Verification Misleading Digital Signing Text On Boot
CSCvb33013	Cisco ASA Remove Mis-leading Secure Boot commands on non-SB hardware
CSCvb38522	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
CSCvb39147	Lower NFS throughput rate on Cisco ASA platform
CSCvb40818	nlp information seen in ipv6 commands
CSCvb40847	ASA not sending Authen Session End log if user logs out manually
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
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

Caveat ID Number	Description
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
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
CSCvb75266	ASA - ACL remark displayed incorrectly in the Packet Tracer tool's XML output
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
CSCvb88358	webvpn-I7-rewriter: 5515 9.1.6 Content Rewrite Problem for ASA Web Bookmark
CSCvb89988	WebVPN: Internal page login button not working through rewriter
CSCvb90108	Inconsistent Upper Bounds for Failover Replication Rate Limiting
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"
CSCvb92548	ASA matches incorrect ACL with object-group-search enabled
CSCvb92823	ASA SIP inspection may delay transmission of 200 OK when embedded with NOTIFY
CSCvb99424	ASA IKEv2 RA VPN does not clearly communicate "No License" status to AnyConnect user
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

Caveat ID Number	Description
CSCvc05005	ASA cluster TCP/SSL ports are not displayed on LISTEN state
CSCvc06150	ASA unable to add multiple attribute entries in a certificate map
CSCvc07112	Implement detection and auto-fix capability for scheduler corruption problems
CSCvc07330	ASAv may crash when running webvpn
CSCvc11628	Pre-fill feature extracts username from wrong cert (cert 1-machine) for double cert vs.(cert 2-user)
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
CSCvc22193	DSCP Markings Not Copied to Outer IP Header With IPsec Encapsulation
CSCvc23838	Cisco ASA Heap Overflow in Webvpn CIFS
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
CSCvc46502	FTD Cluster 9K block depletion with fragmented Traffic
CSCvc48640	ASA not update access-list dynamically when forward-reference enable is configured

Caveat ID Number	Description
CSCvc52072	Webvpn portal not displayed correctly 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.
CSCvc55674	ASA: IPSec SA failed to come up
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
CSCvc61818	CTP after failed attempt sends the domain along with the username
CSCvc61845	RDP plugin activex Full Screen option is not available with ASA 9.6.2 version
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
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
CSCvc79569	mac-address auto command uses default prefix of 1 on ASA5585-X
CSCvc82146	ASA traceback in threadname Datapath
CSCvc85369	ASA does not respond to IPv6 MLD Query.
CSCvc86554	Traceback: ASA 9.5(2)11 crash Active
CSCvc87914	ASA traceback and Reload on Config Sync Failure
CSCvc88115	ASA Clustering IDFW not updating user mappings
CSCvc88411	1550-byte block depletion seen due to Radius Accounting packets

Caveat ID Number	Description
CSCvc91266	ASA BFD echo function fails if RPF is enabled first.
CSCvc92982	Unable to delete Configured Auto NAT from FMC
CSCvc93947	ASA(9.1.7.12):Connection entries created for multicast streams through standby ASA.
CSCvc97734	Deployment fails when management-only enabled on port-channel interface
CSCvd01736	L2TP connects only sometimes when DHCP used
CSCvd03261	ASAv Goes Unresponsive / VPN fails to function after restart
CSCvd03343	Unable to configure SSH public key auth for non-system contexts
CSCvd06527	SNMPv3 linkup/linkdown should be generated through admin context
CSCvd08200	Slow Memory leak in ASA
CSCvd08479	ACL last hit-cnt counter shows incorrect time
CSCvd08709	asymetric path icmp traffic fails through distributed clustering
CSCvd08983	ASA using TACACS authentication and configured 'password-policy lifetime' will deny access
CSCvd09066	asav-aws: In AWS, excessive console output causes reload CLI to fail
CSCvd18126	ASA traceback in thread name DATAPATH
CSCvd20818	ASA IKEv1: Always accept NAT-T encapsulation mode in transform payload
CSCvd21154	5585 does not unbundle its data intfs for 30 seconds after leaving cluste
CSCvd21541	Cannot delete port-object once created under the Service object group in ASA 944
CSCvd21665	ASA w/ RRI and OSPF : Fails to flush route from ASP routing table
CSCvd23016	ASA may traceback when copying capture out using tftp
CSCvd23471	ASA may traceback while loading a large context config during bootup
CSCvd24066	ASA drops web traffic when IM inspection is enabled.
CSCvd26939	SNMP lists same Hostname for all Firepower Threat Defense managed devices
CSCvd28859	ASA: PBR Memory leak for ICMP traffic
CSCvd39113	Cluster C-Hash table is updated with one more unit despite the new unit didn't join the setup
CSCvd41052	Scheduler Queue Corruption leads to connectivity failures or failover problems after 9.6(2)
CSCvd41423	CRL must be signed by certificate containing cRLSign key usage

Caveat ID Number	Description
CSCvd47781	ASA traceback while doing in-service upgrade
CSCvd49262	Traceback when trying to save/view access-list with giant object groups (display_hole_og)
CSCvd50389	RT#687120: Bookmark Issue with clientless VPN - SAML
CSCvd53884	ASA FirePOWER module data plane down after reload of module
CSCvd55983	Traceback in Thread Name: dhcp_daemon
CSCvd56292	Default "global_policy" service-policy removed after reboot
CSCvd58417	DCERPC inspection drops packets and breaks communication
CSCvd62509	ASA traceback in Thread Name: accept/http when ASDM is displaying "Access Rules"
CSCvd63718	ASA-FP9300 Crashed in thread name IPSEC MESSAGE HANDLER
CSCvd65797	ASA May crash when changing a NAT related object to fqdn
CSCvd77893	ASA may generate an assert traceback while modifying access-group
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](#).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.