Release Notes for the Cisco ASA Series, 9.12(x)

Release Notes for the Cisco ASA Series, 9.12(x)

This document contains release information for Cisco ASA software Version 9.12(x).

Important Notes

- **ASDM signed-image support in 9.12(4.50)/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 or later**—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.

- **Upgrade ROMMON for the ISA 3000 to Version 1.0.5 or later**——There is a new ROMMON version for the ISA 3000 (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 1.0.5 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.

- **SSH security improvements and new defaults in 9.12(1)**—See the following SSH security improvements:
  - SSH version 1 is no longer supported; only version 2 is supported. The **ssh version 1** command will be migrated to **ssh version 2**.
  - Diffie-Hellman Group 14 SHA256 key exchange support. This setting is now the default (**ssh key-exchange group dh-group14-sha256**). The former default was Group 1 SHA1. Make sure that your SSH client supports Diffie-Hellman Group 14 SHA256. If it does not, you may see an error such as "Couldn't agree on a key exchange algorithm." For example, OpenSSH supports Diffie-Hellman Group 14 SHA256.
  - HMAC-SHA256 integrity cipher support. The default is now the high security set of ciphers (hmac-sha2-256 only as defined by the **ssh cipher integrity high** command). The former default was the medium set.

- **Diffie-Hellman Group 1 Removal in 9.12(1)**— Diffie-Hellman Group 1 used by the ASA IKE and IPsec modules is considered insecure and has been removed.

  IKEv1: The following subcommands were removed:

  - **crypto ikev1 policy** *priority*:
    - **group 1**

  IKEv2: The following subcommands were removed:

  - **crypto ikev2 policy** *priority*
    - **group 1**

  IPsec: The following subcommands were removed:

  - **crypto ipsec profile *name***
    - **set pfs group1**

  SSL: The following commands were removed:

  - **ssl dh-group group1**

  Crypto Map: The following commands were removed:

  - **crypto map** *name sequence* **set pfs group1**
  - **crypto dynamic-map** *name sequence* **set pfs group1**
  - **crypto map** *name sequence* **set ikev1 phase1-mode aggressive group1**

- **No support in 9.10(1) and later for the ASA FirePOWER module on the ASA 5506-X series and the ASA 5512-X**—The ASA 5506-X series and 5512-X no longer support the ASA FirePOWER module in 9.10(1) and later due to memory constraints. You must remain on 9.9(x) or lower to continue using this module. Other module types are still supported. If you upgrade to 9.10(1) or later, the ASA configuration to send traffic to the FirePOWER module will be erased; make sure to back up your configuration before you upgrade. The FirePOWER image and its configuration remains intact on the SSD. If you want to downgrade, you can copy the ASA configuration from the backup to restore functionality.
- **The NULL-SHA TLSv1 cipher is deprecated and removed in 9.12(1)**—Because NULL-SHA doesn't offer encryption and is no longer considered secure against modern threats, it will be removed when listing supported ciphers for TLSv1 in the output of **tls-proxy** mode commands/options and **show ssl ciphers all**. The **ssl cipher tlsv1 all** and **ssl cipher tlsv1 custom NULL-SHA** commands will also be deprecated and removed.
- **Local CA server is deprecated in 9.12(1), and will be removed in a later release**—When ASA is configured as local CA server, it is enabled to issue digital certificates, publish Certificate Revocation Lists (CRLs), and securely revoke issued certificates. This feature has become obsolete and hence the **crypto ca server** command is deprecated.
- **The default trustpool is removed in 9.12(1)**—In order to comply with PSB requirement, SEC-AUT-DEFROOT, the "default" trusted CA bundle is removed from the ASA image. As a result, **crypto ca trustpool import default** and **crypto ca trustpool import clean default** commands are also

removed along with other related logic. However, in existing deployments, certificates that were previously imported using these command will remain in place.

- **The ssl encryption command is removed in 9.12(1)**—In 9.3(2) the deprecation was announced and replaced by **ssl cipher**. In 9.12(1), **ssl encryption** is removed and no longer supported.

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 9.12(4)

Released: May 26, 2020

Feature	Description
Routing Features	
Multicast IGMP interface state limit raised from 500 to 5000	The multicast IGMP state limit per interface was raised from 500 to 5000. New/Modified commands: **igmp limit**
Troubleshooting Features	
show tech-support command enhanced	The **show ssl objects** and **show ssl errors** command was added to the output of the **show tech-support** command. New/Modified commands: **show tech-support**
VPN Features	

Feature	Description
Support for configuring the maximum in-negotiation SAs as an absolute value	You can now configure the maximum in-negotiation SAs as an absolute value up to 15000 or a maximum value derived from the maximum device capacity; formerly, only a percentage was allowed. New/Modified commands: **crypto ikev2 limit max-in-negotiation-sa value**

New Features in ASA 9.12(3)

Released: November 25, 2019

There are no new features in this release.

New Features in ASA 9.12(2)

Released: May 30, 2019

Feature	Description
Platform Features	
Firepower 9300 SM-56 support	We introduced the following security modules: SM-56. Requires FXOS 2.6.1.157 No modified commands.
Administration Features	
Setting the SSH key exchange mode is restricted to the Admin context	You must set the SSH key exchange in the Admin context; this setting is inherited by all other contexts. New/Modified commands: **ssh key-exchange**

New Features in ASA 9.12(1)

Released: March 13, 2019

Feature	Description
Platform Features	
ASA for the Firepower 4115, 4125, and 4145	We introduced the Firepower 4115, 4125, and 4145. Requires FXOS 2.6.1. No modified commands.

Feature	Description
Support for ASA and FTD on separate modules of the same Firepower 9300	You can now deploy ASA and FTD logical devices on the same Firepower 9300. Requires FXOS 2.6.1. No modified commands.
Firepower 9300 SM-40 and SM-48 support	We introduced the following two security modules: SM-40 and SM-48. Requires FXOS 2.6.1. No modified commands.
Firewall Features	
GTPv1 release 10.12 support.	The system now supports GTPv1 release 10.12. Previously, the system supported release 6.1. The new support includes recognition of 25 additional GTPv1 messages and 66 information elements. In addition, there is a behavior change. Now, any unknown message IDs are allowed. Previously, unknown messages were dropped and logged. No modified commands.
Cisco Umbrella Enhancements.	You can now identify local domain names that should bypass Cisco Umbrella. DNS requests for these domains go directly to the DNS servers without Umbrella processing. You can also identify which Umbrella servers to use for resolving DNS requests. Finally, you can define the Umbrella inspection policy to fail open, so that DNS requests are not blocked if the Umbrella server is unavailable. New/Modified commands: **local-domain-bypass**, **resolver**, **umbrella fail-open**.
The object group search threshold is now disabled by default.	If you enabled object group search, the feature was subject to a threshold to help prevent performance degradation. That threshold is now disabled by default. You can enable it by using the **object-group-search threshold** command. New/Modified command: **object-group-search threshold**.
Interim logging for NAT port block allocation.	When you enable port block allocation for NAT, the system generates syslog messages during port block creation and deletion. If you enable interim logging, the system generates message 305017 at the interval you specify. The messages report all active port blocks allocated at that time, including the protocol (ICMP, TCP, UDP) and source and destination interface and IP address, and the port block. New/Modified command: **xlate block-allocation pba-interim-logging** *seconds*.
VPN Features	
New **condition** option for **debug aaa**.	The **condition** option was added to the **debug aaa** command. You can use this option to filter VPN debugging based on group name, user name, or peer IP address. New/Modified commands: **debug aaa condition**
Support for RSA SHA-1 in IKEv2	You can now generate a signature using the RSA SHA-1 hashing algorithm for IKEv2. New/Modified commands: **rsa-sig-sha1**

Feature	Description
View the default SSL configuration for both DES and 3DES encryption licenses as well as available ciphers	You can now view the default SSL configuration with and without the 3DES encryption license. In addition, you can view all the ciphers supported on the device. New/Modified commands: **show ssl information**
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**
High Availability and Scalability Features	
Per-site gratuitous ARP for clustering	The ASA now generates gratuitous ARP (GARP) packets to keep the switching infrastructure up to date: the highest priority member at each site periodically generates GARP traffic for the global MAC/IP addresses. When using per-site MAC and IP addresses, packets sourced from the cluster use a site-specific MAC address and IP address, while packets received by the cluster use a global MAC address and IP address. If traffic is not generated from the global MAC address periodically, you could experience a MAC address timeout on your switches for the global MAC address. After a timeout, traffic destined for the global MAC address will be flooded across the entire switching infrastructure, which can cause performance and security concerns. GARP is enabled by default when you set the site ID for each unit and the site MAC address for each Spanned EtherChannel. New/Modified commands: **site-periodic-garp interval**
Multiple context mode HTTPS resource management	You can now set the maximum number of non-ASDM HTTPS sessions in a resource class. By default, the limit is set to 6 per context, the maximum. You can use up to 100 HTTPS sesssions across all contexts. New/Modified commands: **limit-resource http**
Routing Features	
OSPF Keychain support for authentication	OSPF authenticates the neighbor and route updates using MD5 keys. In ASA, the keys that are used to generate the MD5 digest had no lifetime associated with it. Thus, user intervention was required to change the keys periodically. To overcome this limitation, OSPFv2 supports MD5 authentication with rotating keys. Based on the accept and send lifetimes of Keys in KeyChain, OSPF authenticates, accepts or rejects keys and forms adjacency. New/Modified commands: **accept-lifetime**, **area virtual-link authentication**, **cryptographic-algorithm**, **key**, **key chain**, **key-string**, **ospf authentication**, **send-lifetime**
Certificate Features	
Local CA configurable FQDN for enrollment URL	To make the FQDN of the enrollment URL configurable instead of using the ASA's configured FQDN, a new CLI option is introduced. This new option is added to the **smpt** mode of **crypto ca server**. New/Modified commands: **fqdn**
Administrative, Monitoring, and Troubleshooting Features	

Feature	Description
enable password change now required on a login	The default **enable** password is blank. When you try to access privileged EXEC mode on the ASA, you are now required to change the password to a value of 3 characters or longer. You cannot keep it blank. The **no enable password** command is no longer supported. At the CLI, you can access privileged EXEC mode using the **enable** command, the **login** command (with a user at privilege level 2+), or an SSH or Telnet session when you enable **aaa authorization exec auto-enable**. All of these methods require you to set the enable password. This password change requirement is not enforced for ASDM logins. In ASDM, by default you can log in without a username and with the **enable** password. New/Modified commands: **enable password**
Configurable limitation of admin sessions	You can configure the maximum number of aggregate, per user, and per-protocol administrative sessions. Formerly, you could configure only the aggregate number of sessions. This feature does not affect console sessions. Note that in multiple context mode, you cannot configure the number of HTTPS sessions, where the maximum is fixed at 5 sessions. The **quota management-session** command is also no longer accepted in the system configuration, and is instead available in the context configuration. The maximum aggregate sessions is now 15; if you configured 0 (unlimited) or 16+, then when you upgrade, the value is changed to 15. New/Modified commands: **quota management-session**, **show quota management-session**
Notifications for administrative privilege level changes	When you authenticate for enable access (**aaa authentication enable console**) or allow privileged EXEC access directly (**aaa authorization exec auto-enable**), then the ASA now notifies users if their assigned access level has changed since their last login. New/Modified commands: **show aaa login-history**
NTP support on IPv6	You can now specify an IPv6 address for the NTP server. New/Modified commands: **ntp server**
SSH stronger security	See the following SSH security improvements: • Diffie-Hellman Group 14 SHA256 key exchange support. This setting is now the default. The former default was Group 1 SHA1. • HMAC-SHA256 integrity cipher support. The default is now the high security set of ciphers (hmac-sha2-256 only). The former default was the medium set. New/Modified commands: **ssh cipher integrity** , **ssh key-exchange group dh-group14-sha256**
Allow non-browser-based HTTPS clients to access the ASA	You can allow non-browser-based HTTPS clients to access HTTPS services on the ASA. By default, ASDM, CSM, and REST API are allowed. New/Modified commands: **http server basic-auth-client**
Capture control plane packets only on the cluster control link	You can now capture control plane packets only on the cluster control link (and no data plane packets). This option is useful in the system in multiple context mode where you cannot match traffic using an ACL. New/Modified commands: **capture interface cluster cp-cluster**

Feature	Description
debug conn command	The **debug conn** command was added to provide two history mechanisms that record connection processing. The first history list is a per-thread list that records the operations of the thread. The second history list is a list that records the operations into the conn-group. When a connection is enabled, processing events such as a connection lock, unlock, and delete are recorded into the two history lists. When a problem occurs, these two lists can be used to look back at the processing to determine the incorrect logic. New/Modified commands: **debug conn**
show tech-support includes additional output	The output of the **show tech-support** is enhanced to display the output of the following: • **show ipv6 interface** • **show aaa-server** • **show fragment** New/Modified commands: **show tech-support**

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
9.10(x)	—	Any of the following: → 9.12(x)
9.9(x)	—	Any of the following: → 9.12(x)
9.8(x)	—	Any of the following: → 9.12(x)
9.7(x)	—	Any of the following: → 9.12(x) → 9.8(x)
9.6(x)	—	Any of the following: → 9.12(x) → 9.8(x)
9.5(x)	—	Any of the following: → 9.12(x) → 9.8(x)
9.4(x)	—	Any of the following: → 9.12(x) → 9.8(x)
9.3(x)	—	Any of the following: → 9.12(x) → 9.8(x)
9.2(x)	—	Any of the following: → 9.12(x) → 9.8(x)

Current Version	Interim Upgrade Version	Target Version
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4)	—	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → **9.12(x)** → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4) → 9.0(4)

Current Version	Interim Upgrade Version	Target Version
8.4(1) through 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.2(x) and earlier	→ 9.0(4)	Any of the following: → **9.12(x)** → 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 9.12(x)

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

Caveat ID Number	Description
CSCuw51499	TCM doesn't work for ACE addition/removal, ACL object/object-group edits
CSCvu29395	Crash observed while performing master role change with active IGMP joins
CSCvg59385	ASA scansafe connector takes too long to failover to secondary CWS Tower

Caveat ID Number	Description
CSCvj93609	ASA traceback on spin_lock_release_actual
CSCvm77115	Lina Traceback due to invalid TSC values
CSCvm85823	Not able to ssh, ssh_exec: open(pager) error on console
CSCvo76866	Traceback on 2100 - watchdog
CSCvo80853	Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability
CSCvp04134	Traceback in HTTP Cli Exec when upgrading to 9.12.1
CSCvp57417	Upon downgrade of an ASAv, the firewall may traceback and reload
CSCvp67033	ASA: Cannot distinguish name aliases for IPv6 and displays a "incomplete command" error message
CSCvp70833	ASA/FTD: Twice nat Rule with same service displaying error "ERROR: NAT unable to reserve ports"
CSCvp94478	ASA scp quite slow
CSCvq12070	Not able to establish more than 2 simultaneous ASDM sessions
CSCvq34340	FTD traffic outage due to 9344 block size depletion caused by the egress-optimization feature
CSCvq37913	VPN-sessiondb does not replicate to standby ASA
CSCvq50587	ASA/FTD may traceback and reload in Thread Name 'BGP Router'
CSCvq51284	FPR 2100, low block 9472 causes packet loss through the device.
CSCvq55426	Adding an ipv6 default route causes CLI to hang for 50 seconds
CSCvq61601	OpenSSL vulnerability CVE-2019-1559 on FTD
CSCvq65864	Traceback in HTTP Cli Exec with rest-api agent enabled
CSCvq70536	FTD: Deployment failure when breaking HA and graceful-restart is present on config
CSCvq73534	Cisco ASA Software Kerberos Authentication Bypass Vulnerability
CSCvq76198	Traffic interruptions for FreeBSD systems
CSCvq78126	V route is missing even after setting the reverse route in Crypto map config in HA-IKEv2
CSCvq83060	SNMP: Cannot get failover link information from oid in multiple mode
CSCvq87797	Multiple context 5585 ASA, transparent context losing mangement interface configuration.
CSCvq88644	Traceback in tcp-proxy

Caveat ID Number	Description
CSCvq89361	Cisco Firepower 1000 Series SSL/TLS Denial of Service Vulnerability
CSCvq99107	Hot swap of SFP is not taking effect on the ASA
CSCvr03705	We need to have default route with AD and tunneled at the same time for the same next hub.
CSCvr07460	ASA traceback and reload related to crypto PKI operation
CSCvr09399	Dynamic flow-offload can't be disabled
CSCvr09468	ASA traceback and reload for the CLI "Show nat pool"
CSCvr10777	ASA Traceback in Ikev2 Daemon
CSCvr13278	PPPoE session not coming up after reload.
CSCvr13823	Cisco Firepower Threat Defense Software Management Access List Bypass Vulnerability
CSCvr15503	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA
CSCvr20449	Policy deployment is reported as successful on the FMC but it is actually failed
CSCvr20757	Block leak on ASA while running Cisco Umbrella DNS inspection
CSCvr20876	low memory causes kernel to invoke - oom and reload device - modified rlimit for KP
CSCvr21803	Mac address flap on switch with wrong packet injected on ingress FTD interface
CSCvr25768	ASA may traceback on display_hole_og
CSCvr29638	HA FTD on FPR2110 traceback after deploy ACP from FMC
CSCvr42344	Traceback on snp_policy_based_route_lookup when deleting a rule from access-list configured for PBR
CSCvr50266	Dual stack ASAv failover triggered by reload issue
CSCvr50509	Some 3DES related configurations are lost after booted
CSCvr50630	ASA Traceback: SCTP bulk sync and HA synchronization
CSCvr51426	ASA is not sending the mask in the accounting packets
CSCvr51998	ASA Static route disappearing from asp table after learning default route via BGP
CSCvr54054	Mac Rewrite Occurring for Identity Nat Traffic
CSCvr55400	FTD/LINA traceback and reload observed in thread name: cli_xml_server
CSCvr55518	Missing clean up on rule creation failure.

Caveat ID Number	Description
CSCvr55825	Cisco ASA and FTD Software Path Traversal Vulnerability
CSCvr56031	FTD/LINA Traceback and reload observed in thread name: cli_xml_server
CSCvr57605	ASA after reload had license context count greater than platform limits
CSCvr58411	RRI on static HUB/SPOKE config is not working on HUB when a new static SPOKE is added or deleted
CSCvr60111	configurations getting wiped off from standby, while deployment fails on active
CSCvr66768	Lina Traceback during FTD deployment when PBR config is being pushed
CSCvr68146	Unable to auto-rejoin FTD cluster
CSCvr68872	Secondary unit exceed platform context count limit in split brain scenario when failover link down
CSCvr79974	Configuration might not replicated if packet loss on the failover Link
CSCvr81457	FTD traceback when TLS tracker (tls_trk_sniff_for_tls) attempted to free a block.
CSCvr83372	I/O error occurred while writing; fd='28', error='Resource temporarily unavailable (11)'
CSCvr85295	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote
CSCvr86077	ASA Traceback/pagefault in Datapath due to re_multi_match_ascii
CSCvr90079	HSTS config option not updated on show run all
CSCvr90965	FTDv Deployment in Azure causes unrecoverable traceback state due to no dns domain-lookup any"
CSCvr92168	Cisco ASA and Cisco FTD Software OSPF Packets Processing Memory Leak Vulnerability
CSCvr92327	ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'
CSCvr93978	ASA traceback and reload on Thread DATAPATH-0-2064
CSCvs01422	Lina traceback when changing device mode of FTD
CSCvs02954	ASA OSPF: Prefix removed from the RIB when topology changes, then added back when another SPF is run
CSCvs03023	Clustering module needs to skip the hardware clock update to avoid the timeout error and clock jump
CSCvs04179	ASA - 9.8.4.12 traceback and reload in ssh or fover_rx Thread
CSCvs05262	Decrement TTL display wrong result

Caveat ID Number	Description
CSCvs07668	FTD traceback and reload on thread DATAPATH-1-15076 when SIP inspection is enabled
CSCvs07982	ASA TRACEBACK: sctpProcessNextSegment - SCTP_INIIT_CHUNK
CSCvs09533	FP2100 Traceback and reload when processing traffic through more than two inline sets
CSCvs15276	ERROR: entry for ::/0 exists when configuring ipv6 icmp
CSCvs15972	Network Performance Degradation when SSL policy is enabled
CSCvs16073	snmp poll failure with host and host-group configured
CSCvs27264	mroute entries on ASA not getting refreshed.
CSCvs28213	ASA Traceback in Thread Name SSH with assertion slib_malloc.c
CSCvs28580	Traceback when processing SSL traffic under heavy load
CSCvs29779	ASA may traceback and reload while waiting for "DATAPATH-12-1899" process to finish.
CSCvs31443	ASA reporting negative memory values on "%ASA-5-321001: Resource 'memory' limit'" message
CSCvs31470	OSPF Hello causing 9K block depletion, control point CPU 100% and cluster unstable.
CSCvs32023	Turn off egress-optimization processing
CSCvs33102	ASA/FTD may traceback and reload in Thread Name 'EIGRP-IPv4'
CSCvs33852	After upgrade to version 9.6.4.34 is not possible to add an access-group
CSCvs38785	Inconsistent timestamp format in syslog
CSCvs39589	ASA doesn't honor SSH Timeout When Data Channel is not Negotiated
CSCvs40230	ICMP not working and failed with inspect-icmp-seq-num-not-matched
CSCvs40531	AnyConnect 4.8 is not working on the FPR1000 series
CSCvs43154	Secondary ASA is unable to join the failover due to aggressive warning messages.
CSCvs45548	reactivation-mode timed causing untimely reactivation of failed server
CSCvs47252	ASA traceback and reload when running command "clear capture /"
CSCvs48437	ASA cannot send syslog to two UDP ports at same time
CSCvs50459	Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability

Caveat ID Number	Description
CSCvs52169	ASA sends malformed RADIUS message when device-id from AnyConnect is too long
CSCvs53705	Anyconnect sessions limited incorrectly
CSCvs55603	ICMP Reply Dropped when matched by ACL
CSCvs59056	ASA/FTD Tunneled Static Routes are Ignored by Suboptimal Lookup if Float-Conn is Enabled
CSCvs59966	false reported value for OID "cipSecGlobalActiveTunnels" - same as ASDM
CSCvs63484	SAML tokens are not removed from hash table
CSCvs70260	IKEv2 vpn-filter drops traffic with implicit deny after volume based rekey collision
CSCvs71698	Management default route conflicts with default data routing
CSCvs73663	ASA Traceback on IPsec message handler Thread
CSCvs76605	Wrong Module version listed for FXOS 2.6(1.174)
CSCvs77818	Traceback: spin_lock_fair_mode_enqueue: Lock (np_conn_shrlock_t) is held for a long time
CSCvs79023	ASA/FTD Traceback in Thread Name: DATAPATH due to DNS inspection
CSCvs80157	ASA Traceback Thread Name: IKE Daemon
CSCvs80536	FP41xx incorrect interface applied in ASA capture
CSCvs82726	Placeholder to address CSCvs31470 in Multi-Context Mode
CSCvs85196	ASA SIP connections drop after several consecutive failovers: pinhole timeout/closed by inspection
CSCvs87795	ASA: backup context failed to "ERROR: No such file or directory"
CSCvs88413	Port-channel bundling is failing after upgrade to 9.8 version
CSCvs90100	ASA/FTD may traceback and reload in Thread Name 'License Thread'
CSCvs91389	FTD Traceback Lina process
CSCvs91869	FPR-1000 Series Random Number Generation Error
CSCvs97863	Reduce number of fsync calls during close in flash file system
CSCvs97908	Invalid scp session terminates other active http, scp sessions
CSCvt01397	Deployment is marked as success although LINA config was not pushed
CSCvt02409	9.12.2.151 snp_cluster_ingress traceback on FPR9300 3-node cluster nested VLAN traffic

Caveat ID Number	Description
CSCvt04560	SCTP heartbeats failing across the firewall in Cluster deploymnet.
CSCvt05862	IPv6 DNS server resolution fails when the server is reachable over the management interface.
CSCvt06606	Flow offload not working with combination of FTD 6.2(3.10) and FXOS 2.6(1.169)
CSCvt06841	Incorrect access-list hitcount seen when configuring it with a capture on ASA
CSCvt11661	DOC - Clarify the meaning of mp-svc-flow-control under show asp drop
CSCvt11742	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCvt12463	ASA: Traceback in thread Unicorn Admin Handler
CSCvt13822	ASA: VTI rejecting IPSec tunnel due to no matching crypto map entry
CSCvt15163	Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability
CSCvt21041	FTD Traceback in thread 'ctm_ipsec_display_msg'
CSCvt22356	Health-check monitor-interface debounce-time in ASA Cluster resets to 9000ms after ASA reboot
CSCvt23643	VPN failover recovery is taking approx. 30 seconds for data to resume
CSCvt24328	FTD: Traceback and reload related to lina_host_file_open_raw function
CSCvt25225	ASA: Active unit HA traceback and reload during Config Sync state during OSPF sync
CSCvt26031	ASAv Unable to register smart licensing with IPv6
CSCvt26067	Active FTP fails when secondary interface is used on FTD
CSCvt27585	Observed Crash in KP while performing Failover Switch from Standby.
CSCvt28182	sctp-state-bypass is not getting invoked for inline FTD
CSCvt33785	IPSec SAs are not being created for random VPN peers
CSCvt35945	Encryption-3DES-AES should not be required when enabling ssh version 2 on 9.8 train
CSCvt45863	Crypto ring stalls when the length in the ip header doesn't match the packet length
CSCvt46289	ASA LDAPS connection fails on Firepower 1000 Series
CSCvt46830	FPR2100 'show crypto accelerator statistics' counters do not track symmetric crypto
CSCvt51987	Traffic outage due to 80 size block exhaustion on the ASA
CSCvt64035	remote acess mib - SNMP 64 bit only reporting 4Gb before wrapping around

Caveat ID Number	Description
CSCvt64952	"Show crypto accelerator load-balance detail" has missing and undefined output
CSCvt65982	Route Fallback doesn't happen on Slave unit, upon RRI route removal.
CSCvt66351	NetFlow reporting impossibly large flow bytes
CSCvt68294	Adjust Firepower 4120 Maximum VPN Session Limit to 20,000
CSCvt70664	ASA: acct-session-time accounting attribute missing from Radius Acct-Requests for AnyConnect
CSCvt73407	TACACS Fallback authorization fails for Username enable_15 on ASA device.
CSCvt73806	FTD traceback and reload on FP2120 LINA Active Box. VPN
CSCvt75241	Redistribution of VPN advertised static routes fail after reloading the FTD on FPR2100
CSCvt78068	Time sync do not work correctly for FTD on FP1000/1100 series platform
CSCvt86188	SNMP traps can't be generated via diagnostic interface

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 9.12(4)

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

Caveat ID Number	Description
CSCuw51499	TCM doesn't work for ACE addition/removal, ACL object/object-group edits
CSCvg59385	ASA scansafe connector takes too long to failover to secondary CWS Tower
CSCvj93609	ASA traceback on spin_lock_release_actual
CSCvm77115	Lina Traceback due to invalid TSC values
CSCvm85823	Not able to ssh, ssh_exec: open(pager) error on console
CSCvo76866	Traceback on 2100 - watchdog
CSCvo80853	Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability
CSCvp04134	Traceback in HTTP Cli Exec when upgrading to 9.12.1
CSCvp57417	Upon downgrade of an ASAv, the firewall may traceback and reload
CSCvp57643	FTD/ASA - Cluster/HA - Master/Active unit does not update all the route changes to Slaves/Standby

Caveat ID Number	Description
CSCvp67033	ASA: Cannot distinguish name aliases for IPv6 and displays a "incomplete command" error message
CSCvp70833	ASA/FTD: Twice nat Rule with same service displaying error "ERROR: NAT unable to reserve ports"
CSCvp94478	ASA scp quite slow
CSCvq12070	Not able to establish more than 2 simultaneous ASDM sessions
CSCvq34340	FTD traffic outage due to 9344 block size depletion caused by the egress-optimization feature
CSCvq37913	VPN-sessiondb does not replicate to standby ASA
CSCvq50587	ASA/FTD may traceback and reload in Thread Name 'BGP Router'
CSCvq50944	OSPFv3 neighborship is flapping every ~30 minutes
CSCvq51284	FPR 2100, low block 9472 causes packet loss through the device.
CSCvq55426	Adding an ipv6 default route causes CLI to hang for 50 seconds
CSCvq61601	OpenSSL vulnerability CVE-2019-1559 on FTD
CSCvq65864	Traceback in HTTP Cli Exec with rest-api agent enabled
CSCvq70536	FTD: Deployment failure when breaking HA and graceful-restart is present on config
CSCvq73534	Cisco ASA Software Kerberos Authentication Bypass Vulnerability
CSCvq76198	Traffic interruptions for FreeBSD systems
CSCvq78126	V route is missing even after setting the reverse route in Crypto map config in HA-IKEv2
CSCvq83060	SNMP: Cannot get failover link information from oid in multiple mode
CSCvq87797	Multiple context 5585 ASA, transparent context losing mangement interface configuration.
CSCvq88644	Traceback in tcp-proxy
CSCvq89361	Cisco Firepower 1000 Series SSL/TLS Denial of Service Vulnerability
CSCvq99107	Hot swap of SFP is not taking effect on the ASA
CSCvr03705	We need to have default route with AD and tunneled at the same time for the same next hub.
CSCvr07460	ASA traceback and reload related to crypto PKI operation
CSCvr09399	Dynamic flow-offload can't be disabled

Caveat ID Number	Description
CSCvr09468	ASA traceback and reload for the CLI "Show nat pool"
CSCvr10777	ASA Traceback in Ikev2 Daemon
CSCvr13278	PPPoE session not coming up after reload.
CSCvr13823	Cisco Firepower Threat Defense Software Management Access List Bypass Vulnerability
CSCvr15503	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA
CSCvr20449	Policy deployment is reported as successful on the FMC but it is actually failed
CSCvr20757	Block leak on ASA while running Cisco Umbrella DNS inspection
CSCvr20876	low memory causes kernel to invoke - oom and reload device - modified rlimit for KP
CSCvr21803	Mac address flap on switch with wrong packet injected on ingress FTD interface
CSCvr25768	ASA may traceback on display_hole_og
CSCvr29638	HA FTD on FPR2110 traceback after deploy ACP from FMC
CSCvr42344	Traceback on snp_policy_based_route_lookup when deleting a rule from access-list configured for PBR
CSCvr50266	Dual stack ASAv failover triggered by reload issue
CSCvr50509	Some 3DES related configurations are lost after booted
CSCvr50630	ASA Traceback: SCTP bulk sync and HA synchronization
CSCvr51426	ASA is not sending the mask in the accounting packets
CSCvr51998	ASA Static route disappearing from asp table after learning default route via BGP
CSCvr54054	Mac Rewrite Occurring for Identity Nat Traffic
CSCvr55400	FTD/LINA traceback and reload observed in thread name: cli_xml_server
CSCvr55518	Missing clean up on rule creation failure.
CSCvr55825	Cisco ASA and FTD Software Path Traversal Vulnerability
CSCvr56031	FTD/LINA Traceback and reload observed in thread name: cli_xml_server
CSCvr57605	ASA after reload had license context count greater than platform limits
CSCvr58411	RRI on static HUB/SPOKE config is not working on HUB when a new static SPOKE is added or deleted
CSCvr60111	configurations getting wiped off from standby, while deployment fails on active

Caveat ID Number	Description
CSCvr66768	Lina Traceback during FTD deployment when PBR config is being pushed
CSCvr68146	Unable to auto-rejoin FTD cluster
CSCvr68872	Secondary unit exceed platform context count limit in split brain scenario when failover link down
CSCvr79974	Configuration might not replicated if packet loss on the failover Link
CSCvr81457	FTD traceback when TLS tracker (tls_trk_sniff_for_tls) attempted to free a block.
CSCvr83372	I/O error occurred while writing; fd='28', error='Resource temporarily unavailable (11)'
CSCvr85295	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote
CSCvr86077	ASA Traceback/pagefault in Datapath due to re_multi_match_ascii
CSCvr90079	HSTS config option not updated on show run all
CSCvr90965	FTDv Deployment in Azure causes unrecoverable traceback state due to no dns domain-lookup any"
CSCvr92168	Cisco ASA and Cisco FTD Software OSPF Packets Processing Memory Leak Vulnerability
CSCvr92327	ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'
CSCvr93978	ASA traceback and reload on Thread DATAPATH-0-2064
CSCvs01422	Lina traceback when changing device mode of FTD
CSCvs02954	ASA OSPF: Prefix removed from the RIB when topology changes, then added back when another SPF is run
CSCvs03023	Clustering module needs to skip the hardware clock update to avoid the timeout error and clock jump
CSCvs04179	ASA - 9.8.4.12 traceback and reload in ssh or fover_rx Thread
CSCvs05262	Decrement TTL display wrong result
CSCvs07668	FTD traceback and reload on thread DATAPATH-1-15076 when SIP inspection is enabled
CSCvs07982	ASA TRACEBACK: sctpProcessNextSegment - SCTP_INIIT_CHUNK
CSCvs09533	FP2100 Traceback and reload when processing traffic through more than two inline sets
CSCvs15276	ERROR: entry for ::/0 exists when configuring ipv6 icmp
CSCvs15972	Network Performance Degradation when SSL policy is enabled

Caveat ID Number	Description
CSCvs16073	snmp poll failure with host and host-group configured
CSCvs27264	mroute entries on ASA not getting refreshed.
CSCvs28213	ASA Traceback in Thread Name SSH with assertion slib_malloc.c
CSCvs28580	Traceback when processing SSL traffic under heavy load
CSCvs29779	ASA may traceback and reload while waiting for "DATAPATH-12-1899" process to finish.
CSCvs31443	ASA reporting negative memory values on "%ASA-5-321001: Resource 'memory' limit'" message
CSCvs31470	OSPF Hello causing 9K block depletion, control point CPU 100% and cluster unstable.
CSCvs32023	Turn off egress-optimization processing
CSCvs33102	ASA/FTD may traceback and reload in Thread Name 'EIGRP-IPv4'
CSCvs33852	After upgrade to version 9.6.4.34 is not possible to add an access-group
CSCvs38785	Inconsistent timestamp format in syslog
CSCvs39589	ASA doesn't honor SSH Timeout When Data Channel is not Negotiated
CSCvs40230	ICMP not working and failed with inspect-icmp-seq-num-not-matched
CSCvs40531	AnyConnect 4.8 is not working on the FPR1000 series
CSCvs43154	Secondary ASA is unable to join the failover due to aggressive warning messages.
CSCvs45548	reactivation-mode timed causing untimely reactivation of failed server
CSCvs47252	ASA traceback and reload when running command "clear capture /"
CSCvs48437	ASA cannot send syslog to two UDP ports at same time
CSCvs50459	Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability
CSCvs52169	ASA sends malformed RADIUS message when device-id from AnyConnect is too long
CSCvs53705	Anyconnect sessions limited incorrectly
CSCvs55603	ICMP Reply Dropped when matched by ACL
CSCvs59056	ASA/FTD Tunneled Static Routes are Ignored by Suboptimal Lookup if Float-Conn is Enabled
CSCvs59966	false reported value for OID "cipSecGlobalActiveTunnels" - same as ASDM
CSCvs63484	SAML tokens are not removed from hash table

Caveat ID Number	Description
CSCvs70260	IKEv2 vpn-filter drops traffic with implicit deny after volume based rekey collision
CSCvs71698	Management default route conflicts with default data routing
CSCvs73663	ASA Traceback on IPsec message handler Thread
CSCvs76605	Wrong Module version listed for FXOS 2.6(1.174)
CSCvs77818	Traceback: spin_lock_fair_mode_enqueue: Lock (np_conn_shrlock_t) is held for a long time
CSCvs79023	ASA/FTD Traceback in Thread Name: DATAPATH due to DNS inspection
CSCvs80157	ASA Traceback Thread Name: IKE Daemon
CSCvs80536	FP41xx incorrect interface applied in ASA capture
CSCvs82726	Placeholder to address CSCvs31470 in Multi-Context Mode
CSCvs85196	ASA SIP connections drop after several consecutive failovers: pinhole timeout/closed by inspection
CSCvs87795	ASA: backup context failed to "ERROR: No such file or directory"
CSCvs88413	Port-channel bundling is failing after upgrade to 9.8 version
CSCvs90100	ASA/FTD may traceback and reload in Thread Name 'License Thread'
CSCvs91389	FTD Traceback Lina process
CSCvs91869	FPR-1000 Series Random Number Generation Error
CSCvs97863	Reduce number of fsync calls during close in flash file system
CSCvs97908	Invalid scp session terminates other active http, scp sessions
CSCvt01397	Deployment is marked as success although LINA config was not pushed
CSCvt02409	9.12.2.151 snp_cluster_ingress traceback on FPR9300 3-node cluster nested VLAN traffic
CSCvt03598	Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability
CSCvt04560	SCTP heartbeats failing across the firewall in Cluster deploymnet.
CSCvt05862	IPv6 DNS server resolution fails when the server is reachable over the management interface.
CSCvt06606	Flow offload not working with combination of FTD 6.2(3.10) and FXOS 2.6(1.169)
CSCvt06841	Incorrect access-list hitcount seen when configuring it with a capture on ASA
CSCvt11661	DOC - Clarify the meaning of mp-svc-flow-control under show asp drop

Caveat ID Number	Description
CSCvt11742	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCvt12463	ASA: Traceback in thread Unicorn Admin Handler
CSCvt13822	ASA: VTI rejecting IPSec tunnel due to no matching crypto map entry
CSCvt15163	Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability
CSCvt21041	FTD Traceback in thread 'ctm_ipsec_display_msg'
CSCvt22356	Health-check monitor-interface debounce-time in ASA Cluster resets to 9000ms after ASA reboot
CSCvt23643	VPN failover recovery is taking approx. 30 seconds for data to resume
CSCvt24328	FTD: Traceback and reload related to lina_host_file_open_raw function
CSCvt25225	ASA: Active unit HA traceback and reload during Config Sync state during OSPF sync
CSCvt26031	ASAv Unable to register smart licensing with IPv6
CSCvt26067	Active FTP fails when secondary interface is used on FTD
CSCvt27585	Observed Crash in KP while performing Failover Switch from Standby.
CSCvt28182	sctp-state-bypass is not getting invoked for inline FTD
CSCvt33785	IPSec SAs are not being created for random VPN peers
CSCvt35945	Encryption-3DES-AES should not be required when enabling ssh version 2 on 9.8 train
CSCvt45863	Crypto ring stalls when the length in the ip header doesn't match the packet length
CSCvt46289	ASA LDAPS connection fails on Firepower 1000 Series
CSCvt46830	FPR2100 'show crypto accelerator statistics' counters do not track symmetric crypto
CSCvt51987	Traffic outage due to 80 size block exhaustion on the ASA
CSCvt52782	ASA traceback Thread name - webvpn_task
CSCvt64035	remote acess mib - SNMP 64 bit only reporting 4Gb before wrapping around
CSCvt64952	"Show crypto accelerator load-balance detail" has missing and undefined output
CSCvt65982	Route Fallback doesn't happen on Slave unit, upon RRI route removal.
CSCvt66351	NetFlow reporting impossibly large flow bytes
CSCvt68294	Adjust Firepower 4120 Maximum VPN Session Limit to 20,000

Caveat ID Number	Description
CSCvt70664	ASA: acct-session-time accounting attribute missing from Radius Acct-Requests for AnyConnect
CSCvt73407	TACACS Fallback authorization fails for Username enable_15 on ASA device.
CSCvt73806	FTD traceback and reload on FP2120 LINA Active Box. VPN
CSCvt75241	Redistribution of VPN advertised static routes fail after reloading the FTD on FPR2100
CSCvt78068	Time sync do not work correctly for FTD on FP1000/1100 series platform
CSCvt86188	SNMP traps can't be generated via diagnostic interface

Resolved Bugs in Version 9.12(3)

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

Caveat ID Number	Description
CSCvf83160	Traceback on Thread Name: DATAPATH-2-1785
CSCvh13869	ASA IKEv2 unable to open aaa session: session limit [2048] reached
CSCvj61580	ASA traceback with Thread: DATAPATH-8-2035
CSCvk22322	ASA Traceback (watchdog timeout) when syncing config from active unit (inc. cachefs_umount)
CSCvk29685	Traceback in DATAPATH on ASA
CSCvm36362	Route tracking failure
CSCvm40288	Port-Channel issues on HA link
CSCvm64400	IKEv2: IKEv2-PROTO-2: Failed to allocate PSH from platform
CSCvm70274	tcp proxy: ASA traceback on DATAPATH
CSCvn76875	Graceful Restart BGP does not work intermittently
CSCvn77388	SDI - SUSPENDED servers cause 15sec delay in the completion of a authentication with a good server
CSCvn78593	Control-plane ACL doesn't work correctly on FTD
CSCvn78870	ASA Multicontext traceback and reload due to allocate-interface out of range command
CSCvn86777	Deployment on FTD with low memory results on interface nameif to be removed - finetune mmap thresh
CSCvo03700	ASA may traceback in thread logger when cluster is enabled on slave unit
CSCvo14961	ASA may traceback and reload while waiting for "dns_cache_timer" process to finish.

Caveat ID Number	Description
CSCvo17775	EIGRP breaks when new sub-interface is added and "mac-address auto" is enabled
CSCvo28118	Traceback in VPN Clustering HA timer thread when member tries to join the cluster
CSCvo43795	OSPF Process ID doesnot change even after clearing OSPF process
CSCvo45755	ASA SCP transfer to box stall mid-transfer
CSCvo47390	ASA traceback in thread SSH
CSCvo47562	VPN sessions failing due to PKI handles not freed during rekeys
CSCvo48838	Lina does not properly report the error for configuration line that is too long
CSCvo51265	Cisco Adaptive Security Appliance Software Secure Copy Denial of Service Vulnerability
CSCvo58847	Enhancement to address high IKE CPU seen due to tunnel replace scenario
CSCvo60580	ASA traceback and reloads when issuing "show inventory" command
CSCvo62031	ASA Traceback and reload while running IKE Debug
CSCvo65741	ASA: BGP routes is cleared on routing table after failover occur and bgp routes are changed
CSCvo66534	Traceback and reload citing Datapath as affected thread
CSCvo68184	management-only of diagnostic I/F on secondary FTD get disappeared
CSCvo72462	Do not decrypt rule causes traffic interruptions.
CSCvo73250	ENH: ACE details for warning "found duplicate element"
CSCvo74350	ASA may traceback and reload. Potentially related to WebVPN traffic
CSCvo74397	ENH: Add process information to "Command Ignored, configuration in progress..."
CSCvo78789	Cisco Adaptive Security Appliance Smart Tunnel Vulnerabilities
CSCvo80501	Standby Firewall reloads with a traceback upon doing a manual failover
CSCvo83169	Cisco ASA Software and FTD Software FTP Inspection Denial of Service Vulnerability
CSCvo86038	Simultaneous FINs on flow-offloaded flows lead to stale conns
CSCvo87930	HTTP with ipv6 using w3m is failing
CSCvo88762	FTD inline/transparent sends packets back through the ingress interface
CSCvo90153	ASA unable to authenticate users with special characters via https
CSCvo97979	The delay command in interface configuration is modified after rebooted
CSCvp04134	Traceback in HTTP Cli Exec when upgrading to 9.12.1

Caveat ID Number	Description
CSCvp04186	cts import-pac tftp: syntax does not work
CSCvp07143	DTLS 1.2 and AnyConnect oMTU
CSCvp10132	AnyConnect connections fail with TCP connection limit exceeded error
CSCvp12052	ASA may traceback and reload. suspecting webvpn related
CSCvp12582	Option to display port number on access-list instead of well known port name on ASA
CSCvp14674	ASAv Azure: Route table BGP propagation setting reset when ASAv fails over
CSCvp16536	ASA traceback and reload observed in Datapath due to SIP inspection.
CSCvp18878	ASA: Watchdog traceback in Datapath
CSCvp19549	FTD lina cored with Thread name: cli_xml_server
CSCvp19910	Unable to process gtpv1 identification req message for header TEID : 0
CSCvp19998	ASA drops GTPV1 SGSN Context Req message with header TEID:0
CSCvp23109	ASA HA IKEv2 generic RA - AnyConnect Premium All In Use incorrect on standby
CSCvp24728	Random SGT tags added by FTD
CSCvp29692	FIPS mode gets disabled after rollback from a failed policy deploy
CSCvp32617	"established tcp" does not work post 9.6.2
CSCvp33341	Cisco ASA and Firepower Threat Defense Software WebVPN Cross-Site Scripting Vulnerability
CSCvp35141	ASA sends invalid redirect response for POST request
CSCvp35384	IKEv2 RA Generic client - stuck outgoing asp table entry - traffic encrypted with stale SPI
CSCvp43066	DHCP NACK silently dropped by ASA sent from DHCP server if configured as DHCP relay
CSCvp45882	Cisco ASA Software and FTD Software SIP Inspection Denial of Service Vulnerability
CSCvp49576	FTD traceback due to watchdog on xlate_detach
CSCvp49790	Cisco ASA Software and FTD Software OSPF LSA Processing Denial of Service Vulnerability
CSCvp55901	LINA traceback on ASA in HA Active Unit repeatedly
CSCvp59864	IP Address stuck in local pool and showing as "In Use" even when the AnyConnect client disconnects
CSCvp63068	Thread Name: CP DP SFR Event Processing traceback

Caveat ID Number	Description
CSCvp67392	ASA/FTD HA Data Interface Heartbeat dropped due to Reverse Path Check
CSCvp70020	After reboot, "ssh version 1 2" added to running-config
CSCvp71180	MCA+AAA+OTP with RADIUS challenge fails to send aggauth handle in challenge
CSCvp72412	Time zone in syslogs messages
CSCvp76944	Cisco ASA and FTD Software WebVPN CPU Denial of Service Vulnerability
CSCvp80775	Unsupported runtime JavaScript exception handling in the client side WebVPN rewriter
CSCvp84546	ASA 9.9.2 Clientless WebVPN - HTML entities are incorrectly decoded when processing HTML
CSCvp85736	Cluster master reload cause ping failure to the Management virtual IP
CSCvq00005	FTD Traceback and Reload on LINA Caused by SSL Decryption DND Preservation
CSCvq01459	LINA Traceback after upgrade to 9.12.2.1
CSCvq05113	ASA failover LANTEST messages are sent on first 10 interfaces in the configuration.
CSCvq11513	Traceback: "saml identity-provider" command will crash multi-context ASAs
CSCvq12070	Not able to establish more than 2 simultaneous ASDM sessions
CSCvq12411	ASA may traceback due to SCTP traffic despite fix CSCvj98964
CSCvq13442	When deleting context the ssh key-exchange goes to Default GLOBALLY!
CSCvq21607	"ssl trust-point" command will be removed when restoring backup via CLI
CSCvq24134	ASA IKEv2 - ASA sends additional delete message after initiating a phase 2 rekey
CSCvq24494	FP2100 - Flow oversubscribing ring/CPU core causing disruption to working flows on FP2100 platforms
CSCvq25626	Watchdog on ASAv when logging to buffer
CSCvq26794	GTP response messages with non existent cause are getting dropped with error message TID is 0
CSCvq27010	Memory leak observed when ASA-SFR dataplane communication flaps
CSCvq34160	traceback and reload when establishing ASDM connection to fp1000 series platform
CSCvq39317	ASA is unable to verify the file integrity
CSCvq44665	FTD/ASA : Traceback in Datapath with assert snp_tcp_intercept_assert_disabled
CSCvq46587	After failover, Active unit tcp sessions are not removed when timeout reached
CSCvq54667	SSL VPN may not be able to establish due to SSL negotiation issue

Caveat ID Number	Description
CSCvq57591	When only IP communication is disrupted on failover link LANTEST msg is not sent on data interfaces
CSCvq60131	ASA traceback observed when moving EZVPN spokes to the device.
CSCvq63024	Dual stacked ASAv manual failover issues
CSCvq64742	ASA5515-K9 standby traceback in Thread Name ssh
CSCvq65241	ASA Traceback on Saleen in Thread Name: IPv6 IDB
CSCvq65864	Traceback in HTTP Cli Exec when upgrading to 96.4.0.41
CSCvq69111	Traceback: Cluster unit lina assertion in thread name:Cluster controller
CSCvq70468	ASA cluster does not flush OSPF routes
CSCvq70775	FPR2100 FTD Standby unit leaking 9K blocks
CSCvq75743	ASA:BGP recursive route lookup for destination 3 hop away is failing.
CSCvq77547	Connections fail to replicate in failover due to failover descriptor mis-match on port-channels
CSCvq80318	ASA generates incorrect error message about PCI cfg space when enumerating Internal-Data0/1
CSCvq80735	Cannot add neighbor in BGP when the neighbor is on the same subnet as one interface
CSCvq91645	Flow Offload Hashing Change of Behavior
CSCvq92126	ASA traceback in Thread IPsec Message Handler
CSCvr10777	ASA Traceback in Ikev2 Daemon
CSCvr20757	ASAv becomes unusable while running Cisco Umbrella
CSCvr25768	ASA may traceback on display_hole_og
CSCvr50266	Dual stack ASAv failover triggered by reload issue
CSCvr66768	Lina Traceback during FTD deployment when PBR config is being pushed
CSCvr85295	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote

Resolved Bugs in Version 9.12(2)

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

Caveat ID Number	Description
CSCvj00363	ASA may traceback and reload with combination of packet-tracer and captures

Caveat ID Number	Description
CSCvj06993	ASA HA with NSF: NSF is not triggered properly when there is an Interface failure in ASA HA
CSCvj82652	Deployment changes are not pushed to the device due to disk0 mounted on read-only
CSCvk15393	ASA device reloads with Thread Name : ha_trans_data_tx
CSCvk29263	SSH session stuck after committing changes within a Configure Session.
CSCvm00066	ASA is stuck on "reading from flash" for several hours
CSCvm50421	ASA traceback on slave/standby during sync config due to OSPF/EIGRP and IPv6 used together in ACE
CSCvn13880	Unit traceback at Thread PIM IPv4 or IGMP IPv4 due to timer events when multicast routing is enabled
CSCvn17347	Traceback and reload when displaying CPU profiling results
CSCvn22833	ADI process fails to start on ASA on Firepower 4100
CSCvn25949	Digitial Signature Verification Failed during upload of Rest-Api image to ASA
CSCvn31347	ACL Unable to configure an ACL after access-group configuration error
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
CSCvn46358	overloading of the lina msglyr infra due to the sending of VPN status messages
CSCvn55007	DTLS fails after rekey
CSCvn67137	ASA5506 may slowly leak memory when using NetFlow
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
CSCvn72650	FTD Address not mapped traceback on 6.3.0.x release
CSCvn75368	FPR platform IPsec VPN goes down intermittently
CSCvn78674	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvn80394	ASA SNMP CPU Hogs
CSCvn94100	"Process Name: lina" | ASA traceback caused by Netflow
CSCvn95711	Traceback on Thread Name: Unicorn Admin Handler after adding protocol to IKEV2 ipsec-proposal
CSCvn96898	Memory Leak in DMA_Pool in binsize 1024 with SCP download

Caveat ID Number	Description
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
CSCvo04444	Ikev2 tunnel creation fails
CSCvo06216	Support more than 255 chars for Split DNS-commit issue in hanover for CSCuz22961
CSCvo09046	Upgrading ASA cluster to 9.10.1.7 cause low memory
CSCvo11077	Memory leak found in IPsec when we establish and terminate a new IKEv1 tunnel.
CSCvo11406	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvo12057	DHCPRelay does not consume DHCP Offer packet with Unicast flag
CSCvo13497	Unable to remove access-list with 'log default' keyword
CSCvo15497	Tunnel Group: 'no ikev2 local-authentication pre-shared-key' removes local cert authen
CSCvo19247	Traceback while processing an outbound SSL packet
CSCvo20847	Active FTP fails through Cluster due to xlate allocation corruption upon sync
CSCvo21210	PDTS has incorrect numa node info resulting in incorrect load balancing
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
CSCvo38051	segfault in ctm_ipsec_pfkey_parse_msg at ctm_ipsec_pfkey.c:602
CSCvo39356	Traceback at Thread Name: IP Address Assign
CSCvo42174	ASA IPSec VPN EAP Fails to Load Valid Certificate in PKI
CSCvo43679	FTD Lina traceback, due to packet looping in the system by normaliser
CSCvo45230	ASA5506 - IBR - not able to ping with hostname if the interface is in BVI in IBR mode
CSCvo55151	crypto ipsec inner-routing-lookup should not be allowed to be configured with VTI present
CSCvo56675	ASA or FTD traceback and reload due to failover state change or xlates cleared
CSCvo62077	SFR VPN Event Memory Leak

Caveat ID Number	Description
CSCvo63240	Smart Tunnel bookmarks don't work after upgrade giving certificate error
CSCvo93872	Memory leak while inspecting GTP traffic
CSCvp16482	ASA on FXOS platforms reloads when establishing simultaneous ASDM sessions
CSCvp36425	ASA 5506/5508/5516 traceback in Thread Name octnic_hm_thread

Resolved Bugs in Version 9.12(1)

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)
CSCvb21927	IKEv2 certificate authentication PRF SHA2 interoperability 3rd party
CSCvc62565	Failover crypto IPsec IKEv2 config does not match when sync with standby
CSCvd13180	AVT : Missing Content-Security-Policy Header in ASA 9.5.2
CSCvd21406	Multiple PAT rules with "any" and named interface cause 305006 "portmap translation creation failed"
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
CSCve95403	ASA boot loop caused by logs sent after FIPS boot test
CSCvf85831	asdm displays error uploading image
CSCvg00565	ASA crashes in glib/g_slice when do "debug menu" self testing
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
CSCvg78582	ENH: ASA 9.8.2 Missing HTTP Secure Header X-XSS-Protection
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvh55035	Firepower Threat Defense device unable to stablish ERSPAN with Nexus 9000

Caveat ID Number	Description
CSCvh55340	ASA Running config through REST-API Full Backup does not contain the specified context configuration
CSCvh77456	Cisco Firepower Threat Defense Software FTP Inspection Denial of Service Vulnerability
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
CSCvh83849	DHCP Relay With Dual ISP and Backup IPSEC Tunnels Causes Flapping
CSCvh86252	Change the blacklist flow timeout inline with snort timeout
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'
CSCvi01312	webvpn: multiple rendering issues on Confluence and Jira applications
CSCvi03103	BGP ASN cause policy deployment failures.
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
CSCvi65512	FTD: AAB might force a snort restart with relatively low load on the system
CSCvi71622	Traceback in DATAPATH on standby FTD
CSCvi77643	Hanging downloads and slow downloads on a FPR4120 due to http inspect

Caveat ID Number	Description
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
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
CSCvi99743	Standby traceback in Thread "Logger" after executing "failover active" with telnet access
CSCvj01704	ASA is getting traceback with reboot only on Spyker aftr shutdown SFR module
CSCvj18111	FTD: Flow-preserve N1 flag shouldn't apply for IPS interfaces
CSCvj22491	Cluster: Enhance ifc monitor debounce-time for interface down->up scenario
CSCvj37924	CWE-20: Improper Input Validation
CSCvj39858	Traceback: Thread Name: IPsec message handler
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
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
CSCvj49883	ASA traceback on Firepower Threat Defense 2130-ASA-K9
CSCvj50008	WebVPN HSTS header is missing includeSubDomains response per RFC 6797
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!

Caveat ID Number	Description
CSCvj65581	Excessive logging from ftdrpcd process on 2100 series appliances
CSCvj67258	Change 2-tuple and 4-tuple hash table to lockless
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
CSCvj85516	Packet capture fails for interface named "management" on Firepower Threat Defense
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
CSCvj92444	ASA keeps Type 7 NSSA after losing neighbor
CSCvj95451	webvpn-l7-rewriter: Bookmark logout fails on IE
CSCvj97159	ASA IKEv2 capture type isakmp setting incorrect "Initiator Request" flag on decrypted IKE_AUTH_Reply
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

Caveat ID Number	Description
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)
CSCvk04592	Flows get stuck in lina conn table in half-closed state
CSCvk07522	webvpn: Bookmark fails to render on Firefox and Chrome. IE fine.
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
CSCvk14258	Crash output reports hardware ASP-## for ASA5585-SSP-##. Should correctly report full model name.
CSCvk14537	SSH/Telnet Management sessions may get stuck in pc ftpc_suspend
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
CSCvk24297	IKEv2 RA with EAP fails due to Windows 10 version 1803 IKEv2 fragmentation feature enabled.
CSCvk25729	Large ACL taking long time to compile on boot causing outage
CSCvk26887	Certificate import from Local CA fails due to invalid Content-Encoding
CSCvk27686	ASA may traceback and reload when acessing qos metrics via ASDM/Telnet/SSH
CSCvk28023	WebVPN: Grammar Based Parser fails to handle META tags
CSCvk29263	SSH session stuck after committing changes within a Configure Session.
CSCvk30228	ASAv and FTDv deployment fails in Microsoft Azure and/or slow console response
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
CSCvk30775	ENH: Addition of 'show fragment' to 'show tech' output
CSCvk30779	ENH: Addition of 'show ipv6 interface' to 'show tech' output

Caveat ID Number	Description
CSCvk30783	ENH: Addition of 'show aaa-server' to 'show tech' output
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 configued with active mode
CSCvk37890	Firepower 2110, Webvpn conditional debugging causes Threat Defense to traceback
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
CSCvk46038	ERROR: The entitlement is already acquired while the configuration is cached.
CSCvk47583	ASA WebVPN - incorrect rewriting for SAP Netweaver
CSCvk48437	ASA - VTI tunnel interface nameif not available for SNMP in "snmp-server host" command
CSCvk50732	AnyConnect 4.6 Web-deploy fails on MAC using Safari 11.1.x browsers
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
CSCvk62896	ASA IKEv2 traceback while deleting SAs
CSCvk66529	FTD on FPR 9300 corrupts TCP headers with pre-filter enabled
CSCvk66771	The CPU profiler stops running without having hit the threshold and without collecting any samples.
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

Caveat ID Number	Description
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.
CSCvm01053	ASA 9.8(2)24 traceback on FPR9K-SM-44
CSCvm06114	RDP bookmark plugin won't launch
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.
CSCvm15880	FPR 9k ASA cluster multicon mode/vpn-mode distribute causes a reboot-loop if transparent mode conf
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.
CSCvm36138	With v1 host configured, a v2c walk from that host succeeds
CSCvm43975	Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability
CSCvm49283	Make Object Group Search Threshold disabled by default, and configurable. Causes outages.
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

Caveat ID Number	Description
CSCvm67316	ASA: Add additional IKEv2/IPSec debugging for CSCvm70848
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
CSCvm82930	FTD: SSH to ASA Data interface fails if overlapping NAT statement is configured
CSCvm86443	Only first line of traceroute is captured in event manager output
CSCvm87970	Webvpn Clientless- password management issue
CSCvm88004	SSH Service on ASA echoes back each typed/pasted character in its own packet
CSCvm91014	NTP synchronization don't work when setting BVI IF as NTP source interface
CSCvm92359	Blocks exhaustion snapshot was not captured on ASA
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.
CSCvn04688	ASA AAA Authentication using TACACs does not work when the Server Host Key is set to 128 characters
CSCvn09322	FTD device rebooted after taking Active State for less than 5 minutes
CSCvn09367	Prevent administrators from installing CXSC module on ASA 5500-X
CSCvn09612	ASA/FTD Connection Idle Timers Not Increasing For Inactive Offloaded Sessions
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
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

Caveat ID Number	Description
CSCvn30393	ASA Traceback in emweb/https during Anyconnect Auth/DAP assessment
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
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
CSCvn49180	ASA/FTD:MAC address not refreshing after changing member-interface of CCL link
CSCvn56095	selective acking not happening with SSL crypto hardware offload
CSCvn61662	ASA 5500-X may reload without crashinfo written due to CXSC module continuously reloading
CSCvn62470	anyconnect client dns request dropped by ASA with umbrella enabled
CSCvn62787	To support multiple retry on devcmd failure to CRUZ during flow table configuration update.
CSCvn64418	ISA300 interop issue with Nokia 7705 router
CSCvn66248	Configuring "boot config" has no effect if file was modified off-box and copied back on
CSCvn67222	DPD doesn't work following a failover, which can (in rare cases) cause an outage if things fail back
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
CSCvn77636	ASA/webvpn: FF and Chrome: Bookmark is not rendered with Grammar Based Parser
CSCvn94100	"Process Name: lina" | ASA traceback caused by Netflow
CSCvn97517	WebVPN: URL-Entry disabled / "Go to" address within embedded toolbar is not taking effect

Caveat ID Number	Description
CSCvo06216	Support more than 255 chars for Split DNS-commit issue in hanover for CSCuz22961
CSCvo09046	Upgrading ASA cluster to 9.10.1.7 cause low memory

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.