Release Notes for the Cisco ASA Series, 9.16(x)

First Published: 2021-05-26

Last Modified: 2024-03-27

Release Notes for the Cisco ASA Series, 9.16(x)

This document contains release information for Cisco ASA software Version 9.16(x).

Important Notes

- **ASDM signed-image support in 9.16(3.19)/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)
- **SNMPv3 users using MD5 hashing and DES encryption are no longer supported, and the users will be removed when you upgrade to 9.16(1)**—Be sure to change any user configuration to higher security algorithms using the **snmp-server user** command before you upgrade.
- **SSH host key action required in 9.16(1)**—In addition to RSA, we added support for the EDDSA and ECDSA host keys for SSH. The ASA tries to use keys in the following order if they exist: EDDSA, ECDSA, and then RSA. When you upgrade to 9.16(1), the ASA will fall back to using the existing RSA key. However, we recommend that you generate higher-security keys as soon as possible using the **crypto key generate** {**eddsa** | **ecdsa**} command. Moreover, if you explicitly configure the ASA to use the RSA key with the **ssh key-exchange hostkey rsa** command, you must generate a key that is 2048 bits or higher. For upgrade compatibility, the ASA will use smaller RSA host keys only when the default host key setting is used. RSA support will be removed in a later release.
- **In 9.16 and later, certificates with RSA keys are not compatible with ECDSA ciphers**—When you use the ECDHE_ECDSA cipher group, configure the trustpoint with a certificate that contains an ECDSA-capable key.
- **RSA keys using that are smaller than 2048 cannot be generated in 9.16(1)**—You can no longer generate RSA keys smaller than 2048 using the **crypto key generate rsa** command.

  For SSH, existing smaller keys can continue to be used after upgrading, but we recommend that you upgrade to a larger size, or to a higher security key type.

  For other features, existing certificates signed with RSA key sizes smaller than 2048 cannot be used in ASA 9.16.1 and later. You can use the **crypto ca permit-weak-crypto** command to allow use of existing smaller keys, but even with this command, you cannot generate new smaller RSA keys..
- **ssh version command removed in 9.16(1)**—This command has been removed. Only SSH version 2 is supported.
- **SAMLv1 feature removed in 9.16(1)**—Support for SAMLv1 was removed.

- **No support for DH groups 2, 5, and 24 in 9.16(1)**—Support has been removed for the DH groups 2, 5, and 24 in SSL DH group configuration. The **ssl dh-group** command has been updated to remove the command options **group2**, **group5**, and **group24**.
- **Cisco announces the feature deprecation for Clientless SSL VPN effective with ASA version 9.17(1)**—Limited support will continue on releases prior to 9.17(1).
- **No support in ASA 9.15(1) and later for the ASA 5525-X, ASA 5545-X, and ASA 5555-X**—ASA 9.14(x) is the last supported version. For the ASA FirePOWER module, the last supported version is 6.6.
- **For the Firepower 1010, invalid VLAN IDs can cause problems**—Before you upgrade to 9.15(1) or later, make sure you are not using a VLAN for switch ports in the range 3968 to 4047. These IDs are for internal use only, and 9.15(1) includes a check to make sure you are not using these IDs. For example, if these IDs are in use after upgrading a failover pair, the failover pair will go into a suspended state. See CSCvw33057 for more information.
- **Chacha-poly ciphers**—AnyConnect has an updated list of supported cryptographic algorithms: AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.10, which are proposed to the ASA when starting TLS-based VPN traffic.

System Requirements

ASDM requires a computer with a CPU with at least 4 cores. Fewer cores can result in high memory usage.

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 9.16(4)

Released: October 13, 2022

There are no new features in this release.

New Features in ASA 9.16(3)

Released: April 6, 2022

There are no new features in this release.

New Features in ASA 9.16(2)

Released: August 18, 2021

There are no new features in this release.

New Features in ASA 9.16(1)

Released: May 26, 2021

Feature	Description
Firewall Features	
New Section 0 for system-defined NAT rules.	A new Section 0 has been added to the NAT rule table. This section is exclusively for the use of the system. Any NAT rules that the system needs for normal functioning are added to this section, and these rules take priority over any rules you create. Previously, system-defined rules were added to Section 1, and user-defined rules could interfere with proper system functioning. You cannot add, edit, or delete Section 0 rules, but you will see them in **show nat detail** command output.
The default SIP inspection policy map drops non-SIP traffic.	For SIP-inspected traffic, the default is now to drop non-SIP traffic. The previous default was to allow non-SIP traffic on ports inspected for SIP. We changed the default SIP policy map to include the **no traffic-non-sip** command.
Ability to specify the IMSI prefixes to be dropped in GTP inspection.	GTP inspection lets you configure IMSI prefix filtering, to identify the Mobile Country Code/Mobile Network Code (MCC/MNC) combinations to allow. You can now do IMSI filtering on the MCC/MNC combinations that you want to drop. This way, you can list out the unwanted combinations, and default to allowing all other combinations. We added the following command: **drop mcc**.
Configure the maximum segment size (MSS) for embryonic connections	You can configure a service policy to set the server maximum segment size (MSS) for SYN-cookie generation for embryonic connections upon reaching the embryonic connections limit. This is meaningful for service policies where you are also setting embryonic connection maximums. New/Modified commands: **set connection syn-cookie-mss**.
Improved CPU usage and performance for many-to-one and one-to-many connections.	The system no longer creates local host objects and locks them when creating connections, except for connections that involve dynamic NAT/PAT and scanning threat detection and host statistics. This improves performance and CPU usage in situations where many connections are going to the same server (such as a load balancer or web server), or one endpoint is making connections to many remote hosts. We changed the following commands: **clear local-host** (deprecated), **show local-host**

Feature	Description
Platform Features	
ASAv support for VMware ESXi 7.0	The ASAv virtual platform supports hosts running on VMware ESXi 7.0. New VMware hardware versions have been added to the vi.ovf and esxi.ovf files to enable optimal performance and usability of the ASAv on ESXi 7.0. No modified commands. No modified screens.
Intel QuickAssist Technology (QAT) on ASAv	The ASAv supports hardware crypto acceleration for ASAv deployments that use the Intel QuickAssist (QAT) 8970 PCI adapter. Hardware crypto acceleration for the ASAv using QAT is supported on VMware ESXi and KVM only. No modified commands. No modified screens.
ASAv on OpenStack	The ASAv virtual platform has added support for OpenStack. No modified commands. No modified screens.
High Availability and Scalability Features	
Improved PAT port block allocation for clustering on the Firepower 4100/9300	The improved PAT port block allocation ensures that the control unit keeps ports in reserve for joining nodes, and proactively reclaims unused ports. To best optimize the allocation, you can set the maximum nodes you plan to have in the cluster using the **cluster-member-limit** command. The control unit can then allocate port blocks to the planned number of nodes, and it will not have to reserve ports for extra nodes you don't plan to use. The default is 16 nodes. You can also monitor syslog 747046 to ensure that there are enough ports available for a new node. New/Modified commands: **cluster-member-limit**, **show nat pool cluster** [**summary**], **show nat pool ip detail**
show cluster history command improvements	We have added additional outputs for the **show cluster history** command. New/Modified commands: **show cluster history brief**, **show cluster history latest**, **show cluster history reverse**, **show cluster history time**
Firepower 1140 maximum contexts increased from 5 to 10	The Firepower 1140 now supports up to 10 contexts.
Certificate Features	
Enrollment over Secure Transport (EST) for certification	ASA supports certificate enrollment using the Enrollment over Secure Transport (EST). However, you can configure to use EST enrollments only with RSA and ECDSA keys. You cannot use EdDSA keypair for a trustpoint configured for EST enrollment. New/Modified commands: **enrollment protocol**, **crypto ca authenticate**, and **crypto ca enroll**

Feature	Description
Support for new EdDSA key	The new key option, EdDSA, was added to the existing RSA and ECDSA options. New/Modified commands: **crypto key generate**, **crypto key zeroize**, **show crypto key mypubkey**
Command to override restrictions on certificate keys	Support to use SHA1with RSA Encryption algorithm for certification and support for certificates with RSA key sizes smaller than 2048 were removed. You can use **crypto ca permit-weak-crypto** command to override these restrictions. New/Modified commands: **crypto ca permit-weak-crypto**
Administrative and Troubleshooting Features	
SSH security improvements	SSH now supports the following security improvements: • Host key format—**crypto key generate** {**eddsa** | **ecdsa**}. In addition to RSA, we added support for the EdDSA and ECDSA host keys. The ASA tries to use keys in the following order if they exist: EdDSA, ECDSA, and then RSA. If you explicitly configure the ASA to use the RSA key with the **ssh key-exchange hostkey rsa** command, you must generate a key that is 2048 bits or higher. For upgrade compatibility, the ASA will use smaller RSA host keys only when the default host key setting is used. RSA support will be removed in a later release. • Key exchange algorithms—**ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • Encryption algorithms—**ssh cipher encryption chacha20-poly1305@openssh.com** • SSH version 1 is no longer supported—The **ssh version** command is removed. New/Modified commands: **crypto key generate eddsa**, **crypto key zeroize eddsa** , **show crypto key mypubkey**, **ssh cipher encryption chacha20-poly1305@openssh.com**, **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**}, **ssh key-exchange hostkey**, **ssh version**
Monitoring Features	
SNMPv3 Authentication	You can now use SHA-224 and SHA-384 for user authentication. You can no longer use MD5 for user authentication. You can no longer use DES for encryption. New/Modified commands: **snmp-server user**
VPN Features	

Feature	Description
Support for IPv6 on Static VTI	ASA supports IPv6 addresses in Virtual Tunnel Interfaces (VTI) configurations. A VTI tunnel source interface can have an IPv6 address, which you can configure to use as the tunnel endpoint. If the tunnel source interface has multiple IPv6 addresses, you can specify which address to be used, else the first IPv6 global address in the list is used by default. The tunnel mode can be either IPv4 or IPv6, but it must be the same as IP address type configured on VTI for the tunnel to be active. An IPv6 address can be assigned to the tunnel source or the tunnel destination interface in a VTI. New/Modified commands: **tunnel source interface**, **tunnel destination**, **tunnel mode**
Support for 1024 VTI interfaces per device	The number of maximum VTIs to be configured on a device has been increased from 100 to 1024. Even if a platform supports more than 1024 interfaces, the VTI count is limited to the number of VLANs configurable on that platform. For example, ASA 5510 supports 100 VLANs, the tunnel count would be 100 minus the number of physical interfaces configured. New/Modified commands: None
Support for DH group 15 in SSL	Support has been added for DH group 15 for SSL encryption. New/Modified commands: **ssl dh-group group15**
Support for DH group 31 for IPsec encryption	Support has been added for DH group 31 for IPsec encryption. New/Modified commands: **set pfs**
Support to limit the SA in IKEv2 queue	Support has been added to limit the number of queues in SA-INIT packets. New/Modified commands: **crypto ikev2 limit queue sa_init**
Option to clear IPsec statistics	CLIs have been introduced to clear and reset IPsec statistics. New/Modified commands: **clear crypto ipsec stats** and **clear ipsec stats**

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 9.14 was the final version for the ASA 5525-X, 5545-X, and 5555-X.

ASA 9.12 was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.

ASA 9.2 was the final version for the ASA 5505.

ASA 9.1 was the final version for the ASA 5510, 5520, 5540, 5550, and 5580.

Current Version	Interim Upgrade Version	Target Version
9.15	—	Any of the following: → **9.16**
9.14	—	Any of the following: → **9.16** → 9.15
9.13	—	Any of the following: → **9.16** → 9.15 → 9.14
9.12	—	Any of the following: → **9.16** → 9.15 → 9.14

Current Version	Interim Upgrade Version	Target Version
9.10	—	Any of the following: → **9.16** → 9.15 → 9.14 → 9.12
9.9	—	Any of the following: → **9.16** → 9.15 → 9.14 → 9.12
9.8	—	Any of the following: → **9.16** → 9.15 → 9.14 → 9.12
9.7	—	Any of the following: → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.6	—	Any of the following: → **9.16** → 9.15 → 9.14 → 9.12 → 9.8

Current Version	Interim Upgrade Version	Target Version
9.5	—	Any of the following: → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.4	—	Any of the following: → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.3	—	Any of the following: → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.2	—	Any of the following: → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4)	—	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
9.1(1)	→ 9.1(2)	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.14 → **9.12** → 9.8 → 9.6 → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.6(1)	→ 9.0(4)	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → **9.12** → 9.8 → 9.1(7.4)
8.4(5+)	—	Any of the following: → **9.12** → 9.8 → 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** → 9.8 → 9.1(7.4)
8.3	→ 9.0(4)	Any of the following: → **9.12** → 9.8 → 9.1(7.4)
8.2 and earlier	→ 9.0(4)	Any of the following: → **9.12** → 9.8 → 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 9.16(x)

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

Identifier	Headline
CSCvz41551	FP2100: ASA/FTD with threat-detection statistics may traceback and reload in Thread Name 'lina'
CSCwb09606	FP2100: ASA/FTD high availability is not resilient to unexpected lacp process termination

Identifier	Headline
CSCwb66635	Failover IPSec session and tunnel ID out of sync
CSCwc23844	ASAv high CPU and stack memory allocation errors despite over 30% free memory
CSCwc77519	FPR1120-ASA:Primary takes active role after reloading
CSCwc82205	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwc83995	RX queue getting stuck, causing the packets silently drop between chassis and blade
CSCwd02864	Changing the buffer size impacting logging to buffer
CSCwd04210	ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT
CSCwd07278	ASA/FTD tmatch compilation check when unit joins the cluster, when TCM is off
CSCwd11862	FPR1010 Trunk port traffic stops working after upgrade to 9.16 or higher.
CSCwd12896	TCP Normalizer silent actions causing connections to fail
CSCwd13103	Traffic is dropped with unclear snort verdict 'block-packet'
CSCwd13977	Port-channel members use backplane interface MAC after a reload
CSCwd15831	FTD Requesting Certificate Unexpectingly
CSCwd16689	ASA traceback due to block data corruption
CSCwd16850	More information is required on Syslog 202010 messages for troubleshooting
CSCwd17533	Nested core observed in FTD4115 with lina_assert in calq_platform_entry_callback
CSCwd17984	ASA - FP1120 unexpected traceback seen in version 9.16.2.14
CSCwd19053	ASA/FTD may traceback with large number of network objects deployment using distribute-list
CSCwi31091	OSPF Redistribution route-map with prefix-list not working after upgrade

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 9.16(4)

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

Identifier	Headline
CSCvw82067	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic
CSCvx56021	FTD: CTS SGT propagation gets enabled after reload
CSCvy50598	BGP table not removing connected route when interface goes down

Identifier	Headline
CSCvy67765	FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working
CSCvy73130	FP4100 platform: Active-Standby changed to dual Active after running "show conn" command
CSCvy86817	Cruz ASIC CLU filter has the incorrect src/dst IP subnet when a custom CCL IP subnet is set
CSCvz09106	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
CSCvz36903	ASA traceback and reload while allocating a new block for cluster keepalive packet
CSCvz60142	ASA/FTD stops serving SSL connections
CSCvz68713	PLR license reservation for ASAv5 is requesting ASAv10
CSCvz69729	Unstable client processes may cause LINA zmqio traceback on FTD
CSCvz71596	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
CSCvz88020	ASAv: coredumpfsys is formatted during bootup
CSCwa03341	Standby's sub interface mac doesn't revert to old mac with no mac-address command
CSCwa36535	Standby unit failed to join failover due to large config size.
CSCwa43311	Snort blocking and dropping packet, with bigger size(1G) file download
CSCwa47737	ASA/FTD may hit a watchdog traceback related to snmp config writing
CSCwa49480	SNMP OID , stop working after around one hour and a half - FTD
CSCwa59907	LINA observed traceback on thread name "snmp_client_callback_thread"
CSCwa61361	ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR
CSCwa62025	IPv6: Some of egress interfaces of global and user vrf routes are missing in asp table
CSCwa68552	All type-8 passwords are lost upon upgrade from ASA 9.12-9.15 to 9.16, failover gets disabled
CSCwa72530	FTD: Time gap/mismatch seen when new node joins a Cluster Control node under history
CSCwa72929	SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCwa73172	ASA reload and traceback in Thread Name: PIX Garbage Collector
CSCwa75966	ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped

Identifier	Headline
CSCwa82850	ASA Failover does not detect context mismatch before declaring joining node as "Standby ready"
CSCwa95079	ASA/FTD Traceback and reload due to NAT configuration
CSCwa97917	ISA3000 in boot loop after powercycle
CSCwa99931	ASA/FTD: Tuning of update_mem_reference process
CSCwb02060	snmp-group host with Invalid host range and subnet causing traceback and reload
CSCwb03704	ASA/FTD datapath threads may run into deadlock and generate traceback
CSCwb04000	ASA/FTD: DF bit is being set on packets routed into VTI
CSCwb05291	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
CSCwb06847	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwb07981	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
CSCwb08644	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
CSCwb16920	CPU profile cannot be reactivated even if previously active memory tracking is disabled
CSCwb17187	SNMP cores are generated every minute while running snmpwalk on HA
CSCwb17963	Unable to identify dynamic rate liming mechanism & not following msg limit per/sec at syslog server.
CSCwb19648	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
CSCwb24039	ASA traceback and reload on routing
CSCwb25809	Single Pass - Traceback due to stale ifc
CSCwb28123	FTD HA deployment fails with error "Deployment failed due to major version change on device"
CSCwb31551	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
CSCwb31699	Primary takes active role after reload
CSCwb32841	NAT (any,any) statements in-states the failover interface and resulting on Split Brain events
CSCwb40001	Long delays when executing SNMP commands

Identifier	Headline
CSCwb43018	Implement SNP API to check ifc and ip belongs to HA LU or CMD interface
CSCwb50405	ASA/FTD Traceback in crypto hash function
CSCwb51707	ASA Traceback and reload in process name: lina
CSCwb53172	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
CSCwb53191	Certificate validation fails post upgrade to 9.17.1
CSCwb53328	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url
CSCwb54791	ASA DHCP server fails to bind reserved address to Linux devices
CSCwb57615	Configuring pbr access-list with line number failed.
CSCwb59465	ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem
CSCwb59488	ASA/FTD Traceback in memory allocation failed
CSCwb63827	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS
CSCwb67040	FP4112|4115 Traceback & reload on Thread Name: netfs_thread_init
CSCwb68642	ASA traceback in Thread Name: SXP CORE
CSCwb69503	ASA unable to configure aes128-gcm@openssh.com when FIPS enabled
CSCwb71460	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
CSCwb73248	FW traceback in timer infra / netflow timer
CSCwb74571	PBR not working on ASA routed mode with zone-members
CSCwb79812	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
CSCwb80559	FTD offloads SGT tagged packets although it should not
CSCwb80862	ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
CSCwb83388	ASA HA Active/standby tracebacks seen approximately every two months.
CSCwb83691	ASA/FTD traceback and reload due to the initiated capture from FMC
CSCwb85633	Snmpwalk output of memory does not match show memory/show memory detail
CSCwb87498	Lina traceback and reload during EIGRP route update processing.

Identifier	Headline
CSCwb88651	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwb89963	ASA Traceback & reload in thread name: Datapath
CSCwb90074	ASA: Multiple Context Mixed Mode SFR Redirection Validation
CSCwb90532	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
CSCwb92709	We can't monitor the interface via "snmpwalk" once interface is removed from context.
CSCwb93932	ASA/FTD traceback and reload with timer services assertion
CSCwb94190	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.
CSCwb94312	Unable to apply SSH settings to ASA version 9.16 or later
CSCwb97251	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCwc02488	ASA/FTD may traceback and reload in Thread Name 'None'
CSCwc03069	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
CSCwc07262	Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3).
CSCwc09414	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwc10483	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
CSCwc10792	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete
CSCwc11511	FTD: SNMP failures after upgrade to 7.0.2
CSCwc11597	ASA tracebacks after SFR was upgraded to 6.7.0.3
CSCwc11663	ASA traceback and reload when modifying DNS inspection policy via CSM or CLI
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc13994	ASA - Restore not remove the new configuration for an interface setup after backup
CSCwc18312	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload
CSCwc18524	ASA/FTD Voltage information is missing in the commnad "show environment"
CSCwc23356	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-20-7695'
CSCwc23695	ASA/FTD can not parse UPN from SAN field of user's certificate
CSCwc24906	ASA/FTD traceback and reload on Thread id: 1637
CSCwc26648	FTD Traceback and reload in process name lina
CSCwc27797	ASA mgmt ip cannot be released

Identifier	Headline
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc28532	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwc28806	ASA Traceback and Reload on process name Lina
CSCwc28928	ASA: SLA debugs not showing up on VTY sessions
CSCwc32246	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
CSCwc36905	ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c
CSCwc38567	ASA/FTD may traceback and reload while executing SCH code
CSCwc40381	ASA : HTTPS traffic authentication issue with Cut-through Proxy enabled
CSCwc44289	FTD - Traceback and reload when performing IPv4 <> IPv6 NAT translations
CSCwc45108	ASA/FTD: GTP inspection causing 9344 sized blocks leak
CSCwc45397	ASA HA - Restore in primary not remove new interface configuration done after backup
CSCwc48375	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
CSCwc49095	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwc50887	FTD - Traceback and reload on NAT IPv4<>IPv6 for UDP flow redirected over CCL link
CSCwc50891	MPLS tagging removed by FTD
CSCwc51326	FXOS-based Firepower platform showing 'no buffer' drops despite high values for RX ring watermarks
CSCwc52351	ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP
CSCwc53280	ASA parser accepts incomplete network statement under OSPF process and is present in show run
CSCwc54217	syslog related to failover is not outputted in FPR2140
CSCwc54984	IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response
CSCwc60037	ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context
CSCwc61912	ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6

Identifier	Headline
CSCwc70962	FTD/ASA "Write Standby" enables ECDSA ciphers causing AC SSLv3 handshake failure
CSCwc73224	Call home configuration on standby device is lost after reload
CSCwc74858	FTD - Traceback in Thread Name: DATAPATH
CSCwc79366	During the deployment time, device got stuck processing the config request.
CSCwc81960	Unable to configure 'match ip address' under route-map when using object-group in access list
CSCwc88897	ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy
CSCwc94085	Unable to establish DTLSv1.2 with FIPS enabled after upgrade from 6.6.5.
CSCwd03810	ASA Custom login page is not working through webvpn after an upgrade

Resolved Bugs in Version 9.16(3)

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

Identifier	Headline
CSCvi58484	Cluster: ping sourced from FTD/ASA to external IPs may if reply lands on different cluster unit
CSCvs27336	Traceback on ASA by Smart Call Home process
CSCvt15348	ASA show processes cpu-usage output is misleading on multi-core platforms
CSCvu96436	Traceback of master and one slave when a particular lock is contended for long
CSCvv43190	Crypto engine errors when GRE header protocol field doesn't match protocol field in inner ip header
CSCvv48942	Snmpwalk showing traffic counter as 0 for failover interface
CSCvw62288	ASA: 256 byte block depletion when syslog rate is high
CSCvx14489	snmpwalk fails on ipv6 interface post a failover
CSCvx36885	ASA reload and traceback in DATAPATH
CSCvx75683	The 'show cluster info trace' output is overwhelmed by 'tag does not exist' messages
CSCvx79526	Cisco ASA and FTD Software Resource Exhaustion Denial of Service Vulnerability
CSCvx80830	VPN conn fails from same user if Radius server sends a dACL and vpn-simultaneous-logins is set to 1

Identifier	Headline
CSCvx95652	ASAv Azure: Some or all interfaces might stop passing traffic after a certain period of run time
CSCvx97053	Unable to configure ipv6 address/prefix to same interface and network in different context
CSCvy04343	ASA in PLR mode,"license smart reservation" is failing.
CSCvy04430	Management Sessions fail to connect after several weeks
CSCvy21334	Active tries to send CoA update to Standby in case of "No Switchover"
CSCvy32366	After upgrading ASA to 9.15(1)10, ASDM 7.15(1)150 One Time Password (OTP) field does not appear
CSCvy33501	FDM failover pair - new configured sVTI IPSEC SA is not synced to standby. FDM shows HA not in sync
CSCvy33676	UN-NAT created on FTD once a prior dynamic xlate is created
CSCvy35737	FTD traceback and reload during anyconnect package verification
CSCvy40401	L2L VPN session bringup fails when using NULL encryption in ipsec configuration
CSCvy47108	Remote Access IKEv2 VPN session cannot be established because of stuck Uauth entry
CSCvy52924	FTD loses OSPF network statements config for all VRF instances upon reboot
CSCvy53461	RSA keys & Certs get removed post reload on WS-SVC-ASA-SM1-K7 with ASA code 9.12.x
CSCvy55439	FTDv throughput degredation due to frequent PDTS read/write
CSCvy56395	ASA traceback and reload due to snmp encrypted community string when key config is present
CSCvy57905	VTI tunnel interface stays down post reload on KP/WM platform in HA
CSCvy58268	Block 80 and 256 exhaustion snapshots are not created
CSCvy60831	ASA/FTD Memory block location not updating for fragmented packets in data-path
CSCvy64911	Debugs for: SNMP MIB value for crasLocalAddress is not showing the IP address
CSCvy69453	WM Standby device do not send out coldstart trap after reboot.
CSCvy74781	The standby device is sending the keep alive messages for ssl traffic after the failover
CSCvy74984	ASAv on Azure loses connectivity to Metadata server once default outside route is used
CSCvy75724	ZMQ OOM due to less Msglyr pool memory in low end platforms

Identifier	Headline
CSCvy78525	VRF route lookup for TCP ping is missing
CSCvy79952	ASA/FTD traceback and reload after downgrade
CSCvy82668	SSH session not being released
CSCvy89144	Cisco ASA and FTD Web Services Denial of Service Vulnerability
CSCvy90836	ASA Traceback and reload in Thread Name: SNMP ContextThread
CSCvy91668	PAT pool exhaustion with stickiness traffic could lead to new connection drop.
CSCvy93480	Cisco ASA and FTD Software IKEv2 Site-to-Site VPN Denial of Service Vulnerability
CSCvy96325	FTD/ASA: Adding new ACE entries to ACP causes removal and re-add of ACE elements in LINA
CSCvy96625	Roll back changes introduced by CSCvr33428 and CSCvy39659
CSCvy96803	FTD traceback and reload in Process Name lina related to SNMP functions
CSCvy96895	ASA disconnects the VTY session using of Active IP address and Standby MAC address after failed over
CSCvy98458	FP21xx -traceback "Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header"
CSCvy99217	IKEv2: SA Error code should be translated to human friendly reason
CSCvz00032	Cisco Firepower Threat Defense Software TCP Proxy Denial of Service Vulnerability
CSCvz00032	FTD tracebacks and reloads on Thread name Lina
CSCvz00383	FTD lina traceback and reload in thread Name Checkheaps
CSCvz00699	Traceback in webvpn and reload experienced periodically after ASA upgrade
CSCvz00961	AnyConnect connection failure related to ASA truncated/corrupt config
CSCvz02398	Crypto archive generated with SE ring timeout on 7.0
CSCvz03524	PKI "OCSP revocation check" failing due to sha256 request instead of sha1
CSCvz05189	FTD reload with Lina traceback during xlate replication in Cluster
CSCvz05468	Multiple SSH host entries in platform settings as first feature enable/deploy will break SSH on LINA
CSCvz05541	ASA55XX: Expansion module interfaces not coming up after a software upgrade
CSCvz07614	ASA: Orphaned SSH session not allowing us to delete a policy-map from CLI
CSCvz08387	ASP drop capture output may display incorrect drop reason

Identifier	Headline
CSCvz09109	Cluster CCL interface capture shows full packets although headers-only is configured
CSCvz15529	ASA traceback and reload thread name: Datapath
CSCvz17923	Dispatcher doesn't account for asynclock pend q work under some conditions result lower cpu util
CSCvz20544	ASA/FTD may traceback and reload in loop processing Anyconnect profile
CSCvz20679	FTDv - Lina Traceback and reload
CSCvz21886	Twice nat's un-nat not happening if nat matches a pbr acl that matches a port number instead of IP
CSCvz23157	SNMP agent restarts when show commands are issued
CSCvz24765	device rebooted with snmpd core
CSCvz25454	ASA: Drop reason is missing from 129 lines of asp-drop capture
CSCvz29233	ASA: ARP entries from custom context not removed when an interface flap occurs on system context
CSCvz30333	FTD/Lina may traceback when "show capture" command is executed
CSCvz30933	ASA tracebacks and reload when clear configure snmp-server command is issued
CSCvz33468	ASA/FTD - NAT stops translating source addresses after changes to object-groups in manual NAT Rule
CSCvz34831	If ASA fails to download DACL it will never stop trying
CSCvz37306	ASDM session is not served for new user after doing multiple context switches in existing user
CSCvz38332	FTD/ASA - Stuck in boot loop after upgrade from 9.14.2.15 to 9.14.3
CSCvz38361	BGP packets dropped for non directly connected neighbors
CSCvz38692	ASAv traceback in snmp_master_callback_thread and reload
CSCvz39646	ASA/AnyConnect - Stale RADIUS sessions
CSCvz40352	ASA traffic dropped by Implicit ACL despite the fact of explicit rules present on Access-list
CSCvz43414	Internal ldap attribute mappings fail after HA failover
CSCvz43455	ASAv observed traceback while upgrading hostscan
CSCvz44339	FTD - Deployment will fail if you try to delete an SNMP host with ngfw-interface and host-group
CSCvz44645	FTD may traceback and reload in Thread Name 'lina'

Identifier	Headline
CSCvz48407	Traceback and reload in Thread Name: DATAPATH-15-18621
CSCvz50712	TLS server discovery uses incorrect source IP address for probes in AnyConnect deployment
CSCvz50922	FPR2100: Unable to form L2L VPN tunnels when using ESP-Null encryption
CSCvz51258	show tech-support output can be confusing when there crashinfo, need to clean up/make more intuitive
CSCvz53142	ASA does not use the interface specified in the name-server command to reach IPv6 DNS servers
CSCvz54471	ASA:Failed ASA in HA pair not recovering by itself, after an "HA state progression failed"
CSCvz55302	FTD/ASA Traceback and reload due to SSL null checks under low memory conditions
CSCvz55395	TCP connections are cleared after configured idle-timeout even though traffic is present
CSCvz55849	FTD Traceback and Reload on process LINA
CSCvz57710	conf t is converted to disk0:/t under context-config mode
CSCvz58376	Snort down after deploying the policy
CSCvz58710	ASA traceback due to SCTP traffic.
CSCvz60578	Cluster unit in MASTER_POST_CONFIG state should transition to Disabled state after an interva
CSCvz61160	ASA traceback on DATAPATH when handling ICMP error message
CSCvz61431	"Netsnmp_update_ma_config: ERROR Failed to build req"messages seen during cluster configuration sync
CSCvz61658	CPU hogs in update_mem_reference
CSCvz64470	ASA/FTD Traceback and reload due to memory corruption when generating ICMP unreachable message
CSCvz66795	ASA traceback and reload in SSH process when executing the command "show access-list"
CSCvz67003	ASDM session count and quota management's count mismatch. 'Lost connection firewall' msg in ASDM
CSCvz67816	IPV6 DNS PTR query getting modified on FTD
CSCvz68336	SSL decryption not working due to single connection on multiple in-line pairs
CSCvz69571	ASA log shows wrong value of the transferred data after the anyconnect session terminated.

Identifier	Headline
CSCvz70316	LINA may generate traceback and reload
CSCvz70595	Traceback observed on ASA while handling SAML handler
CSCvz70958	High Control Plane CPU on StandBy due to dhcpp_add_ipl_stby
CSCvz71064	Deleting The Context From ASA taking Almost 2 Minutes with ikev2 tunnel
CSCvz72771	ASA/FTD may traceback and reload. "c_assert_cond_terminate" in stack trace
CSCvz73146	FTD - Traceback in Thread Name: DATAPATH
CSCvz73709	ASA/FTD Standby unit fails to join HA
CSCvz75988	Inconsistent logging timestamp with RFC5424 enabled
CSCvz76746	While implementing management tunnel a user can use open connect to bypass anyconnect.
CSCvz76848	FTD traceback and reload when using DTLS1.2 on RA tunnels
CSCvz76966	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DNS DoS
CSCvz77744	OSPFv3: FTD Wrong "Forwarding address" added in ospfv3 database
CSCvz78816	ASA disconnects the ssh, https session using of Active IP address and Standby MAC address after FO
CSCvz81888	NTP will not change to *(synced) status after upgrade to asa-9.15.1/9.16.1.28 from asa-9.14.3
CSCvz82562	ASA/FTD: site-to-site VPN - traffic incorrectly fragmented
CSCvz84850	ASA/FTD traceback and reload caused by "timer services" function
CSCvz85437	FTD 25G, 40G and 100G interfaces down after upgrade of FXOS and FTD to 2.10.1.159 and 6.6.4
CSCvz86256	Primary ASA should send GARP as soon as split-brain is detected and peer becomes cold standby
CSCvz88149	Lina traceback and reload during block free causing FTD boot loop
CSCvz89126	ASDM session/quota count mismatch in ASA when multiple context switchover is done from ASDM
CSCvz89327	OSPFv2 flow missing cluster centralized "c" flag
CSCvz89545	SSL VPN performance degraded and significant stability issues after upgrade
CSCvz90375	Low available DMA memory on ASA 9.14 at boot reduces AnyConnect sessions supported

Identifier	Headline
CSCvz90722	With object-group in crypto ACL sum of hitcnt mismatches with the individual elements
CSCvz91218	Statelink hello messages dropped on Standby unit due to interface ring drops on high rate traffic
CSCvz92016	ASA Privilege Escalation with valid user in AD
CSCvz92932	ASA show tech execution causing spike on CPU and impacting to IKEv2 sessions
CSCvz94153	NTP sync on IPV6 will fail if the IPV4 address is not configured
CSCvz95108	FTD Deployment failure post upgrade due to major version change on device
CSCvz95743	Loss of NTP sync following an upgrade
CSCvz95949	FP1120 9.14.3 : temporary split brain happened after active device reboot
CSCvz96462	IP Address 'in use' though no VPN sessions
CSCvz99222	Clear and show conn for inline-set is not working
CSCwa02929	FTD Blocks Traffic with SSL Flow Error CORRUPT_MESSAGE
CSCwa03275	BGP routes shows unresolved and dropping packet with asp-drop reason "No route to host"
CSCwa03347	IPv6 PIM packets are dropped in ASP with invalid-ip-length drop reason
CSCwa04461	Cisco ASA Software and FTD Software Remote Access SSL VPN Denial of Service
CSCwa08262	AnyConnect users with mapped group-policies take attributes from default GP under the tunnel-group
CSCwa11052	SNMP Stopped Responding After Upgrading to Version- 9.14(2)15
CSCwa13873	ASA Failover Split Brain caused by delay on state transition after "failover active" command run
CSCwa14485	Cisco Firepower Threat Defense Software Denial of Service Vulnerability
CSCwa14725	ASA/FTD traceback and reload on IKE Daemon Thread
CSCwa15185	ASA/FTD: remove unwanted process call from LUA
CSCwa18858	ASA drops non DNS traffic with reason "label length 164 bytes exceeds protocol limit of 63 bytes"
CSCwa18889	Clock drift observed between Lina and FXOS on multi-instance
CSCwa19443	Flow Offload - Compare state values remains in error state for longer periods
CSCwa19713	Traffic dropped by ASA configured with BVI interfaces due to asp drop type "no-adjacency"

Identifier	Headline
CSCwa28822	FTD moving UI management from FDM to FMC causes traffic to fail
CSCwa28895	FTD SSL Proxy should allow configurable or dynamic maximum TCP window size
CSCwa30114	"Error:NAT unable to reserve ports" when using a range of ports in an object service
CSCwa33898	Cisco Adaptive Security Appliance Software Clientless SSL VPN Heap Overflow Vulnerability
CSCwa34287	ASA: Loss of NTP sync following a reload after upgrade
CSCwa35200	Some syslogs for AnyConnect SSL are generated in admin context instead of user context
CSCwa36672	ASA on FPR4100 traceback and reload when running captures using ASDM
CSCwa36678	Random FTD reloads with the traceback during deployment from FMC
CSCwa38277	ASA NAT66 with big range as a pool don't works with IPv6
CSCwa40719	Traceback: Secondary firewall reloading in Threadname: fover_parse
CSCwa41834	ASA/FTD traceback and reload due to pix_startup_thread
CSCwa42594	ASA: IP Header check validation failure when GTP Header have SEQ and EXT field
CSCwa53489	Lina Traceback and Reload Due to invalid memory access while accessing Hash Table
CSCwa55562	Different CG-NAT port-block allocated for same source IP causing per-host PAT port block exhaustion
CSCwa55878	FTD Service Module Failure: False alarm of "ND may have gone down"
CSCwa56449	ASA traceback in HTTP cli EXEC code
CSCwa56975	DHCP Offer not seen on control plane
CSCwa57115	New access-list are not taking effect after removing non-existance ACL with objects.
CSCwa58686	ASA/FTD Change in OGS compilation behavior causing boot loop
CSCwa60574	ASA traceback and reload on snp_ha_trans_alloc_msg_muxbuf_space function
CSCwa61218	Polling OID "1.3.6.1.4.1.9.9.171.1.3.2.1.2" gives negative index value of the associated tunnel
CSCwa65389	ASA traceback and reload in Unicorn Admin Handler when change interface configuration via ASDM
CSCwa67884	Conditional flow-offload debugging produces no output
CSCwa68660	FTP inspection stops working properly after upgrading the ASA to 9.12.4.x
CSCwa74900	Traceback and reload after enabling debug webvpn cifs 255

Identifier	Headline
CSCwa77073	SNMP is responding to snmpgetbulk with unexpected order of results
CSCwa79494	Traffic keep failing on Hub when IPSec tunnel from Spoke flaps
CSCwa79980	SNMP get command in FPR does not show interface index.
CSCwa81795	Cisco ASA and FTD Software VPN Authorization Bypass Vulnerability
CSCwa85043	Traceback: Lina traceback and reload on thread name: Logger
CSCwa85138	Multiple issues with transactional commit diagnostics
CSCwa87315	ASA/FTD may traceback and reload in Thread Name 'IP Address Assign'
CSCwa87597	ASA/FTD Failover: Joining Standby reboots when receiving configuration replication from Active mate
CSCwa89243	SNMP no longer responds to polls after upgrade to 9.15.1.17
CSCwa91090	SSL handshake logging showing unknown session during AnyConnect TLSv1.2 Session establishment
CSCwa94894	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-4-9608'
CSCwa96327	Incorrect ifHighSpeed value for a interfaces that are port channel members
CSCwa96759	Lina may traceback and reload on tcpmod_proxy_handle_mixed_mode
CSCwa97784	ASA: Jumbo sized packets are not fragmented over the L2TP tunnel
CSCwa98684	Console has an excessive rate of warnings during policy deployment
CSCwb00595	Mempool_DMA allocation issue / memory leakage
CSCwb01700	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA
CSCwb01919	FP2140 ASA 9.16.2 HA units traceback and reload at lua_getinfo (getfuncname)
CSCwb09219	ASA/FTD: OCSP may fail to work after upgrade due to "signer certificate not found"
CSCwb11939	ASA/FTD MAC modification is seen in handling fragmented packets with INSPECT on
CSCwb15795	Audit message not generated by: no logging enable from ASAv9.12
CSCwb18252	FTD/ASA: Traceback on BFD function causing unexpected reboot
CSCwb34035	ASA CLI gets hung randomly while configuring SNMP

Resolved Bugs in Version 9.16(2)

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

Caveat ID Number	Description
CSCum03297	ENH: ASA should save the timestamp of the MAXHOG in 'show proc cpu-hog'
CSCvg66052	2 CPU Cores continuously spike on firepower appliances
CSCvr11958	AWS FTD: Deployment failure with ERROR: failed to set interface to promiscuous mode
CSCvv71097	traceback: ASA reloaded snp_fdb_destroy_fh_callback+104
CSCvw46630	FTD: NLP path dropping return ICMP destination unreachable messages
CSCvw62526	ASA traceback and reload on engineering ASA build - 9.12.3.237
CSCvw71405	FPR1120 running ASA traceback and reload in crypto process.
CSCvx11917	FTD active unit might drop interface failover messages with host-move-pkt drop reason
CSCvx20872	ASA/FTD Traceback and reload due to netflow refresh timer
CSCvx23833	IKEv2 rekey - Invalid SPI for ESP packet using new SPI received right after Create_Child_SA response
CSCvx26308	ASA traceback and reload due to strcpy_s: source string too long for dest
CSCvx38124	Core-local block alloc failure on cores where CP is pinned leading to drops
CSCvx48490	SSL Decrypted https flow EOF events showing 'Initiator/Responder' Packets as 0
CSCvx50980	ASA CP CPU wrong calculation leads to high percentage (100% CP CPU)
CSCvx65178	SNMP bulkget not working for specific OIDs in firewall mib and device performance degradation
CSCvx77768	Traceback and reload due to Umbrella
CSCvx79793	Slow file transfer or file upload with SSL policy is applied with Decrypt resign action
CSCvx85922	ASA/FTD may traceback and reload when saving/writitng the configuration to memory
CSCvx87709	FPR 2100 running ASA in HA. Traceback and reload on watchdog during failover
CSCvx90486	In some cases snmwapwalk for ifXTable may not return data interfaces
CSCvx94398	Secondary ASA could not get the startup configuration
CSCvx97632	ASA traceback and reload when copying files with long destination filenames using cluster command
CSCvy01752	Traceback on FPR 4115 in Thread - Lic HA Cluster
CSCvy03006	improve debugging capability for uauth
CSCvy07491	ASA traceback when re-configuring access-list

Caveat ID Number	Description
CSCvy09217	HA goes to active-active state due to cipher mismatch
CSCvy09436	DHCP reservation fails to apply reserved address for some devices
CSCvy10583	ASA Traceback and Reload in Thread Name: DATAPATH
CSCvy16179	ASA cluster Traceback with Thread Name: Unicorn Admin Handler even when running fix for CSCuz67596
CSCvy17078	Traceback: ASA on FPR 2110 traceback and reload on process Lina
CSCvy17365	REST API Login Page Issue
CSCvy17470	ASA Traceback and reload on the A/S failover pair at IKEv2.
CSCvy18138	PIM Register Sent counter does not increase when encapsulated packets with register flag sent to RP
CSCvy19136	Web portal persistent redirects when certificate authentication is used.
CSCvy23349	FTD unnecessarily ACKing TCP flows on inline-pair deployment
CSCvy31229	No space left disk space is full on /ngfw
CSCvy33105	Ambiguous command error is shown for 'show route bgp' or 'show route isis' if DNS lookup is enabled
CSCvy36694	FTDv 6.7 on Azure is unable to set 1000 speed on GigabitEthernet interfaces
CSCvy39621	ASA/FTD sends continuous Radius Access Requests Even After Max Retry Count is Reached
CSCvy39659	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-15-14815'
CSCvy43447	FTD traceback and reload on Lic TMR Thread on Multi Instance FTD
CSCvy47108	Remote Access IKEv2 VPN session cannot be established because of stuck Uauth entry
CSCvy48159	ASA Traceback & reload on process name lina due to memory header validation
CSCvy48730	ASA/FTD may traceback and reload in Thread Name 'Unicorn Proxy Thread'
CSCvy49732	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCvy50011	ASA traceback in IKE Daemon process and reload
CSCvy51659	Long OCSP timeout may cause AnyConnect authentication failure
CSCvy52074	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
CSCvy52924	FTD loses OSPF network statements config for all VRF instances upon reboot
CSCvy55356	CPU hogs less than 10 msec are produced contrary to documentation

Caveat ID Number	Description
CSCvy56395	ASA traceback and reload due to snmp encrypted community string when key config is present
CSCvy58268	Block 80 and 256 exhaustion snapshots are not created
CSCvy60100	SNMP v3 configuration lost after reboot for HA
CSCvy61008	Time out of sync between Lina and FXOS
CSCvy63949	ASA direct authentication timeouts even if direct authentication traffic is passing through the ASA
CSCvy64492	ASAv adding non-identity L2 entries for own addresses on MAC table and dropping HA hellos
CSCvy66711	Cisco ASA 9.16.1 and FTD 7.0.0 IPsec Denial of Service Vulnerability
CSCvy69189	FTD HA stuck in bulk state due to stuck vpnfol_sync/Bulk-sync keytab
CSCvy69787	ASAv on AWS TenGigabit interface is learning 1000mbps instead of 10000Mbps
CSCvy72846	ASA accounting reports incorrect Acct-Session-Time
CSCvy73554	ASA: "deny ip any any" entry in crypto ACL prevents IKEv2 remote AnyConnect access connections
CSCvy74781	The standby device is sending the keep alive messages for ssl traffic after the failover
CSCvy79952	ASA/FTD traceback and reload after downgrade
CSCvy82794	ASA/FTD traceback and reload when negating snmp commands
CSCvy92990	FTD traceback and reload related to SSL after upgrade to 7.0
CSCvy96803	FTD traceback and reload in Process Name lina related to SNMP functions
CSCvz00699	Traceback in webvpn and reload experienced periodically after ASA upgrade
CSCvz30933	ASA tracebacks and reload when clear configure snmp-server command is issued

Resolved Bugs in Version 9.16(1)

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

Caveat ID Number	Description
CSCvc07112	Implement detection and auto-fix capability for scheduler corruption problems
CSCve02555	Functionality to include SNMP OID for retrieving 'show asp drop' information
CSCvg69380	ASA - rare cp processing corruption causes console lock
CSCvm82290	ASA core blocks depleted when host unreachable in IRB/TFW configuration

Caveat ID Number	Description
CSCvo34210	ASA running 9.6.4.20 Traceback in threadname Unicorn Proxy Thread
CSCvp69936	ASA : Traceback on tcp_intercept Thread name : Threat detection
CSCvr13713	ENH: Need to log console messages on 2100 similar to 4100/9300 running ASA
CSCvr85295	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote
CSCvs13204	ASAv failover traffic on SR-IOV interfaces might be dropped due to interface-down
CSCvs72450	FXOS - Recover hwclock of service module from corruption due to simultaneous write collision
CSCvs82926	Critical RPM alert on FRP 1000 and FPR2100 Series with ASA 'Chassis 0 Cooling Fan OK' SCH message
CSCvs84542	ASA traceback with thread: idfw_proc
CSCvt71529	ASA traceback and reload during SSL handshake
CSCvt75760	Traceback/Page-fault in Clientless WebVPN due to HTTP cleanup
CSCvu34228	FTD LINA traceback & reload while processing snort return verdict
CSCvu94846	When enabling inline tap mode you may experience between 20-50% performance reduction
CSCvu98222	FTD Lina engine may traceback in datapath after enabling SSL decryption policy
CSCvv15572	ASA traceback observed when "config-url" is entered while creating new context
CSCvv17585	Netflow template not sent under certain circumstances
CSCvv19230	ASAv Anyconnect users unexpectedly disconnect with reason: Idle Timeout
CSCvv34851	6.7.0-1992: duplicate connection events with empty SSL info in one of them
CSCvv40406	FTD/ASA creates coredump file with "!" character in filename (lina changes).
CSCvv56644	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv60998	FPR2100 1 Gig Fiber SFP Interfaces down in ASA appliance mode
CSCvv65184	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv66005	ASA traceback and reload on inspect esmtp
CSCvv67500	ASA 9.12 random traceback and reload in DATAPATH
CSCvv70984	ASA traceback while modifying the bookmark SSL Ciphers configuration

Caveat ID Number	Description
CSCvv72466	OSPF network commands go missing in the startup-config after upgrading the ASA
CSCvv73017	Traceback due to fover and ssh thread
CSCvv80782	Traceback leads to the purg_process
CSCvv85029	ASA5555 traceback and reload on Thread Name: ace_work
CSCvv86861	Traceback in KP in timer while running VPN, EMIX and SNMP traffic for overnight.
CSCvv86926	Unexpected traceback and reload on FTD creating a Core file
CSCvv87232	ASA: High number of CPU hog in igb_saleen_io_sfp_mod_poll_thread process
CSCvv88017	ASA: EasyVPN HW Client triggers duplicate phase 2 rekey causing disconnections across the tunnel
CSCvv89708	ASA/FTD may traceback in thread name fover_FSM_thread and reload
CSCvv90720	ASA/FTD: Mac address-table flap seen on connected switch after a HA switchover
CSCvv94165	FTD 6.6 : High CPU spikes on snmpd process
CSCvv94701	ASA keeps reloading with "octnic_hm_thread". After the reload, it takes very long time to recover.
CSCvv97877	Secondary unit not able to join the cluster
CSCvw00161	ASA traceback and reload due to VPN thread on firepower 2140
CSCvw07000	Snort busy drops with PDTS Tx queue stuck
CSCvw12008	ASA traceback and reload while executing "show tech-support" command
CSCvw12100	ASA stale VPN Context seen for site to site and AnyConnect sessions
CSCvw16619	Offloaded traffic not failed over to secondary route in ECMP setup
CSCvw18614	ASA traceback in the LINA process
CSCvw21844	FTD traceback and reload on DATAPATH thread when processing encapsulated flows
CSCvw22881	radius_rcv_auth can shoot up control plane CPU to 100%.
CSCvw22986	Secondary unit stuck in Bulk sync infinitely due to interface of Primary stuck in init state
CSCvw23199	ASA/FTD Traceback and reload in Thread Name: Logger
CSCvw24084	FTD might crash in SNMP with rip Netsnmp_config_req_dequeue_and_send+269 at snmp/snmp_config_utils.c
CSCvw24556	TCP File transfer (Big File) not properly closed when Flow offload is enabled

Caveat ID Number	Description
CSCvw26171	ASA syslog traceback while strncpy NULL string passed from SSL library
CSCvw26331	ASA traceback and reload on Thread Name: ci/console
CSCvw26544	Cisco ASA and FTD Software SIP Denial of Service Vulnerability
CSCvw27301	IKEv2 with EAP, MOBIKE status fails to be processed.
CSCvw28814	SNMP process crashed, while upgrading the QP to v9.14.1.109
CSCvw30252	ASA/FTD may traceback and reload due to memory corruption in SNMP
CSCvw31569	Director/Backup flows are left behind and traffic related to this flow is blackholed
CSCvw32518	ASASM traceback and reload after upgrade up to 9.12(4)4 and higher
CSCvw36662	TACACS+ ASCII password change request not handled properly
CSCvw37259	VPN syslogs are generated at a rate of 600/s until device goes into a hang state
CSCvw38614	AZURE ASA/FTD NIC MAC address might get re-ordered upon a reboot
CSCvw42999	9.10.1.11 ASA on FPR2110 traceback and reloads randomly
CSCvw43486	ASA/FTD Traceback and reload during PBR configuration change
CSCvw44122	ASA: "class-default" class-map redirecting non-DNS traffic to DNS inspection engine
CSCvw45863	ASAv snmp traceback on reload
CSCvw46885	ASA/FTD traceback and reload related to SNMP and management-access configuration
CSCvw47321	IPSec transport mode traffic corruption for inbound traffic for some FPR platforms
CSCvw48517	DAP stopped working after upgrading the ASA to 9.13(1)13
CSCvw51307	ASA/FTD traceback and reload in process name "Lina"
CSCvw51462	IPv4 Default Tunneled Route Rejected
CSCvw51950	FPR 4K: SSL trust-point removed from new active ASA after manual Failover
CSCvw51985	ASA: AnyConnect sessions cannot be resumed due to ipv6 DACL failure
CSCvw52609	Cisco ASA and FTD Software Web Services Buffer Overflow Denial of Service Vulnerability
CSCvw53427	ASA Fails to process HTTP POST with SAML assertion containing multiple query parameters
CSCvw53596	FPR4120 - Lina watchdog traceback in cli_xmlserver_thread
CSCvw53796	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerability

Caveat ID Number	Description
CSCvw53884	M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
CSCvw54640	FPR-4150 - ASA traceback and reload with thread name DATAPATH
CSCvw58414	Name of anyconnect custom attribute of type dynamic-split-exclude-domains is changed after reload
CSCvw59035	Connection issues to directly connected IP from FTD BVI address
CSCvw63862	ASA: Random L2TP users cannot access resources due to stale ACL filter entries
CSCvw71766	ASA traceback and reload in Thread: Ikev2 Daemon
CSCvw74940	ASA traceback in IKE Daemon and reload
CSCvw81897	ASA: OpenSSL Vulnerability CVE-2020-1971
CSCvw82629	ASA Tracebacks when making "configuration session" changes regarding an ACL.
CSCvw83572	BVI HTTP/SSH access is not working in versions 9.14.1.30 or above
CSCvw83780	FTD Firewall may traceback and reload when modifying ACLs
CSCvw84339	Managed device backup fails, for FTD, if hostname exceeds 30 characters
CSCvw84786	ASA traceback and reload on Thread name snmp_alarm_thread
CSCvw87788	ASA traceback and reload webvpn thread
CSCvw89365	ASA/FTD may traceback and reload during certificate changes.
CSCvw93139	Cisco ASA and FTD Software for FP 1000/2100 Series Command Injection Vulnerability
CSCvw95301	ASA traceback and reload with Thread name: ssh when capture was removed
CSCvw95368	ASA: Traceback at emweb/https and reload when Remote Access VPN is enabled
CSCvw96488	Traceback in inspect_h323_ras+1810
CSCvw97821	ASA: VPN traffic does not pass if no dACL is provided in CoA
CSCvw98840	ASA: dACL with no IPv6 entries is not applied to v6 traffic after CoA
CSCvw99916	ASAv: SNMP result for used memory value incorrect after upgrade to 9.14
CSCvx01805	AppAgent gets deregistered due to hearbeat failure during config sync up on Firepower 2100s
CSCvx02869	Traceback in Thread Name: Lic TMR
CSCvx03764	Offload rewrite data needs to be fixed for identity nat traffic and clustering environment

Caveat ID Number	Description
CSCvx04057	When SGT name is unresolved and used in ACE, line is not being ignored/inactive
CSCvx04643	ASA reload is removing 'content-security-policy' config
CSCvx05381	Cisco ASA and FTD Software Command Injection Vulnerability
CSCvx05385	ASA may generate a traceback in Logger thread during configuration sync in HA
CSCvx06385	Fail-to-wire ports in FPR 2100 flapping after upgrade to 6.6.1
CSCvx08734	ASA: default IPv6/IPv4 route tunneled does not work
CSCvx09123	M500IT Model Solid State Drives on ISA3000 may go unresponsive after 3.2 Years in service
CSCvx09535	ASA Traceback: CRL check for an Anyconnect client with a revoked certificate triggers reload
CSCvx11295	ASA may traceback and reload on thread Crypto CA
CSCvx11460	Firepower 2110 silently dropping traffic with TFC enabled on the remote end
CSCvx13694	ASA/FTD traceback in Thread Name: PTHREAD-4432
CSCvx15040	DHCP Proxy Offer is getting drop on the ASA/FTD
CSCvx16317	Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed
CSCvx17664	ASA may traceback and reload in Thread Name 'webvpn_task'
CSCvx17780	FPR-2100-ASA : SNMP Walk for ifType is showing "other" for ASA interfaces in the latest versions
CSCvx17842	Prevent lina from traceback due to object loop sent by FMC. Fail the deployment instead.
CSCvx20303	ASA/FTD may traceback in after changing snmp host-group object
CSCvx22695	ASA traceback and reload during OCSP response data cleanup
CSCvx25719	X-Frame-Options header is not set in webvpn response pages
CSCvx25836	ASA traceback & reload due to "show crashinfo" adding a new output log
CSCvx26221	Traceback into snmp at handle_agentx_packet / snmp takes long time to come up on FP1k and 5508
CSCvx26808	FTD traceback and reload on process lina on FPR2100 series
CSCvx27430	ASA: Unable to import PAC file if FIPS is enabled.
CSCvx29771	Firewall CPU can increase after a bulk routing update with flow offload

Caveat ID Number	Description
CSCvx29814	IP address in DHCP GIADDR field is reversed after sending DHCP DECLINE to DHCP server
CSCvx29832	CPU performance degrade with lots of route updates with flow offload enabled
CSCvx30314	ASA 9.15.1.7 traceback and reload in ssl midpath
CSCvx34237	ASA reload with FIPS failure
CSCvx41171	Concurrent modification of ACL configuration breaks output of "show running-config" completely
CSCvx42081	FPR4150 ASA Standby Ready unit Loops to failed and remove config to install it again
CSCvx42197	ASA EIGRP route stuck after neighbour disconnected
CSCvx43335	FTD cluster physical interface will not be up in inline mode even fxos interface state up.
CSCvx44401	FTD/ASA traceback in Thread Name : Unicorn Proxy Thread
CSCvx47230	X-Frame-Options header support for older versions of IE and windows platforms
CSCvx50366	Traceback in Thread Name: fover_health_monitoring_thread
CSCvx52122	ASA traceback and reload in SNMP Notify Thread while deleting transparent context
CSCvx54235	ASP capture dispatch-queue-limit shows no packets
CSCvx54396	Deployment failures on FTD when multicast is enabled.
CSCvx54606	FTD 6.6.1/6.7.0 is sending SNMP Ifspeed OID (1.3.6.1.2.1.2.2.1.5) response value = 0
CSCvx57417	Smart Tunnel Code signing certifcate renewal
CSCvx59120	COA Received before data tunnel comes up results in tear down of parent session
CSCvx63647	ASA traceback and reload on Thread Name: CTM Daemon
CSCvx68128	ASA internal deadlock leads to loss of feature functionality (syslogs, reload, ASDM, anyconnect)
CSCvx69405	ASA Traceback and reload in Thread Name: SNMP ContextThread
CSCvx71434	ASA/FTD Traceback and reload in Thread Name: pix_startup_thread due to asa_run_ttyS0 script
CSCvx72904	Optimise ifmib polls
CSCvx76233	ASA traceback and reload in thread ci/console when copying a system image to flash
CSCvx79793	Slow file transfer or file upload with SSL policy is applied with Decrypt resign action

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.