Release Notes for the Cisco Secure Firewall ASA, 9.23(x)

First Published: 2025-03-11

Last Modified: 2025-08-18

Release Notes for the Cisco Secure Firewall ASA, 9.23(x)

This document contains release information for ASA software version 9.23(x).

Important Notes

- **The ASA SSH stack was deprecated in 9.23**—You can no longer use the ASA SSH stack. The Cisco SSH stack is now the only stack. Because the Cisco SSH stack does not support EDDSA, before you upgrade you must change your configuration for a supported key pair:

  1. Generate the default key pair.

     crypto key generate {**ecdsa elliptic-curve** *size* | **rsa modulus** *size*}

     Do not add the **label** keyword; SSH only uses the default key pair (named Default-*type*-Key).

  2. If you configured the **ssh key-exchange hostkey eddsa** command, you need to remove it with the **no** form. If you use this command, you may get unexpected results.

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 Secure Firewall 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 9.23(1)

Released: March 5, 2025

Feature	Description
Platform Features	
Secure Firewall 1230/1240/1250	The Secure Firewall 1230/1240/1250 is a 1RU rackmountable firewall.
Increased connection limits for the Secure Firewall 4200	Connection limits have been increased: • 4225: 80M → **90M** • 4245: 80M → **180M**
Firewall Features	
Support for the RADIUS Message-Authenticator attribute.	The Message-Authenticator attribute is used to protect against Blast-RADIUS attacks. If you have upgraded your RADIUS server so it supports the message authenticator, you can enable this option to help protect against these attacks. When enabled, all requests and responses must have the message authenticator, or authentication will fail. We added the following command: **message-authenticator-required**.
New Umbrella API.	You can now configure Umbrella using the Umbrella Open API, which uses an API key with a Secret key. We added the following command: **token-request-credential**
Flow offload is enabled by default for the Secure Firewall 3100/4200	Flow offload is now enabled by default. Added/modified commands: **flow-offload enable**.
High Availability and Scalability Features	

Feature	Description
Multiple context support for all Secure Firewall 1200 models	We added support for multiple context mode for the Secure Firewall 1210/1220: • Secure Firewall 1210CE—5 contexts. • Secure Firewall 1210CP—5 contexts. • Secure Firewall 1220CX—10 contexts. Switchports are not supported in multiple context mode, and you must convert all interfaces to router interfaces before you can convert to multiple context mode. The Secure Firewall 1230/1240/1250 also supports multiple context mode in its initial release: • Secure Firewall 1230—25 contexts. • Secure Firewall 1240—25 contexts. • Secure Firewall 1250—25 contexts.
Cluster redirect: flow offload support for the Secure Firewall 4200 asymmetric cluster traffic	For asymmetric flows, cluster redirect lets the forwarding node offload flows to hardware. This feature is enabled by default. When traffic for an existing flow is sent to a different node, then that traffic is redirected to the owner node over the cluster control link. Because asymmetric flows can create a lot of traffic on the cluster control link, letting the forwarder offload these flows can improve performance. Added/modified commands: **flow-offload cluster-redirect**, **show conn**, **show flow-offload flow**, , **show flow-offload flow protocol**, **show flow-offload info**.
Improved role-switch time during failover	When a failover occurs, the new active device generates multicast packets for each MAC address entry and sends them to all bridge group interfaces, prompting the upstream switches to update their routing tables. This task of generating and sending multicast packets to the bridge interfaces now runs asynchronously in the data plane, allowing critical failover tasks in the control plane to proceed without delays. This enhancement improves role-switch time during a failover and reduces downtime.
MTU ping test on cluster node join	When a node joins the cluster, it checks MTU compatibility by sending a ping to the control node with a packet size matching the cluster control link MTU. If the ping fails, a notification is generated so you can fix the MTU mismatch on connecting switches and try again.
Interface Features	
Secure Firewall 1210CP IEEE 802.3bt support (PoE++ and Hi-PoE)	See the following improvements related to support for IEEE 802.3bt: • PoE++ and Hi-PoE—Up to 90W per port. • Single- and dual-signature powered devices (PDs). • Power budgeting is done on a first-come, first-served basis. • Power budget fields were added to **show power inline**. New/Modified commands: **power inline**, **show power inline**

Feature	Description
License Features	
Flexible Permanent License Reservation for ASA Virtual	For an ASA Virtual, you can configure any model-specific license for permanent license reservation irrespective of the RAM and vCPUs. You can switch between the permanent license reservation licenses irrespective of the memory allocated to the ASA Virtual. You can also change the memory and vCPUs assigned to the ASA Virtual without changing the model license. If you downgrade the ASA Virtual to versions earlier than 9.23.1, the license status becomes Unregistered. We recommend that you do not downgrade an ASA Virtual with flexible permanent license reservation. We added the following command: **license smart flex-model**
Administrative, Monitoring, and Troubleshooting Features	
Automated Certificate Management Environment (ACME) protocol for TLS device certificates.	You can configure Automated Certificate Management Environment (ACME) protocol to ASA trustpoint to manage the TLS device certificates. ACME enables simplified certificate management through auto renewal, domain validation, and easy enrolling and revoking of certificates. You can choose to use the Let's Encrypt CA server or use any other ACME server for the authentication. ACME uses http01 method for authentication. New or modified commands: **crypto ca trustpoint enrollment protocol crypto ca authenticate**
VPN Features	
Distributed site-to-site VPN with clustering on the Secure Firewall 4200	An ASA cluster on the Secure Firewall 4200 supports site-to-site VPN in distributed mode. Distributed mode provides the ability to have many site-to-site IPsec IKEv2 VPN connections distributed across members of an ASA cluster, not just on the control node (as in centralized mode). This significantly scales VPN support beyond centralized VPN capabilities and provides high availability. New or modified commands: **cluster redistribute vpn-sessiondb**, **show cluster vpn-sessiondb**, **vpn-mode** , **show cluster resource usage**, **show vpn-sessiondb** , **show conn detail**, **show crypto ikev2 stats**
IPsec flow offload for traffic on the cluster control link on the Secure Firewall 4200 in distributed site-to-site VPN mode	For asymmetric flows in distributed site-to-site VPN mode, IPsec flow offload now lets the flow owner decrypt IPsec traffic in hardware that was forwarded over the cluster control link. This feature is not configurable and is always available when you enable IPsec flow offload. Added/modified commands: **flow-offload-ipsec**, **show crypto ipsec sa detail**.

Upgrade the Software

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

Upgrade Link

To complete your upgrade, see the ASA upgrade guide.

Upgrade Path: ASA Appliances

What Version Should I Upgrade To?

On the Cisco Support & Download site, the suggested release is marked with a gold star. For example:

Figure 1: Suggested Release

View Your Current Version

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.

Upgrade Guidelines

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.

For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the ASA Security Advisories.

Upgrade Paths

This table provides upgrade paths for ASA.

Note ASA 9.20 was the final version for the Firepower 2100.

ASA 9.18 was the final version for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300.

ASA 9.16 was the final version for the ASA 5506-X, 5508-X, and 5516-X.

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.

Table 1: Upgrade Path

Current Version	Interim Upgrade Version	Target Version
9.22	—	Any of the following: → 9.23

Current Version	Interim Upgrade Version	Target Version
9.20	—	Any of the following: → 9.23 → 9.22
9.19	—	Any of the following: → 9.23 → 9.22 → 9.20
9.18	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19
9.17	—	Any of the following: → 9.22 → 9.20 → 9.19 → 9.18
9.16	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17

Current Version	Interim Upgrade Version	Target Version
9.15	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.14	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.13	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

Current Version	Interim Upgrade Version	Target Version
9.12	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.10	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.9	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12

Current Version	Interim Upgrade Version	Target Version
9.8	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.7	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.6	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12

Current Version	Interim Upgrade Version	Target Version
9.5	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.4	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.3	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12

Current Version	Interim Upgrade Version	Target Version
9.2	—	Any of the following: → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
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
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.12

Upgrade Path: ASA Logical Devices for the Firepower 4100/9300

- FXOS: From FXOS 2.2.2 and later, you can upgrade directly to any higher version. (FXOS 2.0.1–2.2.1 can upgrade as far as 2.8.1. For versions earlier than 2.0.1, you need to upgrade to each intermediate version.) Note that you cannot upgrade FXOS to a version that does not support your current logical device version. You will need to upgrade in steps: upgrade FXOS to the highest version that supports your current logical device; then upgrade your logical device to the highest version supported with that FXOS version. For example, if you want to upgrade from FXOS 2.2/ASA 9.8 to FXOS 2.13/ASA 9.19, you would have to perform the following upgrades:

  1. FXOS 2.2 → FXOS 2.11 (the highest version that supports 9.8)
  2. ASA 9.8 → ASA 9.17 (the highest version supported by 2.11)
  3. FXOS 2.11 → FXOS 2.13
  4. ASA 9.17 → ASA 9.19

- Firewall Threat Defense: Interim upgrades may be required for Firewall Threat Defense, in addition to the FXOS requirements above. For the exact upgrade path, refer to the Firewall Management Center upgrade guide for your version.
- ASA: ASA lets you upgrade directly from your current version to any higher version, noting the FXOS requirements above.

Table 2: Firepower 4100/9300 Compatibility with ASA and Firewall Threat Defense

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.17	Firepower 4112	**9.23 (recommended)** 9.22 9.20 9.19 9.18	**7.7** (recommended) 7.6 7.4 7.3 7.2
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.23 (recommended)** 9.22 9.20 9.19 9.18	**7.7** (recommended) 7.6 7.4 7.3 7.2
2.16	Firepower 4112	**9.22** (recommended) 9.20 9.19 9.18 9.17	**7.6** (recommended) 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.22** (recommended) 9.20 9.19 9.18 9.17	**7.6** (recommended) 7.4 7.3 7.2 7.1

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.14(1)	Firepower 4112	**9.20** (recommended) 9.19 9.18 9.17 9.16 9.14	**7.4** (recommended) 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.20** (recommended) 9.19 9.18 9.17 9.16 9.14	**7.4** (recommended) 7.3 7.2 7.1 7.0 6.6
2.13	Firepower 4112	**9.19** (recommended) 9.18 9.17 9.16 9.14	**7.3** (recommended) 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.19** (recommended) 9.18 9.17 9.16 9.14	**7.3** (recommended) 7.2 7.1 7.0 6.6

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.12	Firepower 4112	**9.18** (recommended) 9.17 9.16 9.14	**7.2** (recommended) 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18** (recommended) 9.17 9.16 9.14 9.12	**7.2** (recommended) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18** (recommended) 9.17 9.16 9.14 9.12	**7.2** (recommended) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.11	Firepower 4112	**9.17** (recommended) 9.16 9.14	**7.1** (recommended) 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17** (recommended) 9.16 9.14 9.12	**7.1** (recommended) 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17** (recommended) 9.16 9.14 9.12 9.8	**7.1** (recommended) 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.10 **Note** For compatibility with 7.0.2+ and 9.16(3.11)+, you need FXOS 2.10(1.179)+.	Firepower 4112	**9.16** (recommended) 9.14	**7.0** (recommended) 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16** (recommended) 9.14 9.12	**7.0** (recommended) 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16** (recommended) 9.14 9.12 9.8	**7.0** (recommended) 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.8	Firepower 4112	**9.14**	**6.6** **Note** 6.6.1+ requires FXOS 2.8(1.125)+.
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14** (recommended) 9.12 **Note** Firepower 9300 SM-56 requires ASA 9.12(2)+	**6.6** (recommended) **Note** 6.6.1+ requires FXOS 2.8(1.125)+. 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14** (recommended) 9.12 9.8	**6.6** (recommended) **Note** 6.6.1+ requires FXOS 2.8(1.125)+. 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.6(1.157) **Note** You can now run ASA 9.12+ and FTD 6.4+ on separate modules in the same Firepower 9300 chassis	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** **Note** Firepower 9300 SM-56 requires ASA 9.12.2+	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommended) 9.8	**6.4** (recommended) 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	Not supported
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommended) 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Note** 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	**6.2.3** (recommended) **Note** 6.2.3.16+ requires FXOS 2.3.1.157+
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Note** 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	Firewall Threat Defense versions are EoL
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Note on Downgrades

Downgrade of FXOS images is not officially supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device.

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 9.23(x)

There are no open bugs in this release.

Resolved Bugs in Version 9.23(1)

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

Identifier	Headline
CSCvx44261	SNMPv3: Special characters used in FXOS SNMPv3 configuration causes authentication errors
CSCvx74133	App-instance showing as Started instead of Online
CSCvz59859	FXOS fault F1758 description should not be specific to subinterfaces
CSCvz70310	ASA may fail to create NAT rule for SNMP with: "error NAT unable to reserve ports."
CSCwb77894	Firepower 1000/2100 may boot to ROMMON mode
CSCwc76419	Unnecessary FAN error logs needs to be removed from thermal file
CSCwd60102	ASA: Delay in new chunk memory allocation when the firewall process a high number of new connections
CSCwd67100	ASA traceback and reload on Datapath process
CSCwe02012	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe18462	ASA/FTD: Improve GTP Inspection Logging
CSCwe18467	ASA/FTD: GTP Inspection engine serviceability
CSCwe88492	Banner login does not display when configured
CSCwe92324	FPR31xx - SNMP poll reports incorrect FanTray Status at Down while actually operational
CSCwf39108	Firewall rings may get stuck and cause packet loss when asp load-balance per-packet auto is used
CSCwf75694	ASA - The GTP inspection dropped the message 'Delete PDP Context Response' due to an invalid TEID=0
CSCwf84318	ASA/FTD traceback and reload on thread DATAPATH
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwh09113	FPR1010 in HA failed to send or receive to GARP/ARP with error "edsa_rcv: out_drop"
CSCwh12120	Incorrect exit interface choose for VTI traffic next-hop
CSCwh17965	[Display]FXOS: PC member interface is shown as down & unassociated/unassigned after reload/crash
CSCwh18967	Include "show env tech" in FXOS FPRM troubleshoot
CSCwh24932	ASA software on FP3110 showing incorrect serial number in show inventory output

Identifier	Headline
CSCwh27886	Chassis Manager shows HTTP 500 Internal Server error in specific cases
CSCwh43230	Strong Encryption license is not getting applied to ASA firewalls in HA.
CSCwh43945	FTD/ASA traceback and reload may occur when ssl packet debugs are enabled
CSCwh50221	4200 Series: Portchannel in cluster may stay down sometimes when LACP is in active mode
CSCwh51438	Add support for 10G-T-X module
CSCwh51872	Message asa_log_client exited 1 time(s) seen multiple times
CSCwh54477	The FMC is showing "The password encryption key has not been set" alert for a 11xx/21xx/31xx device
CSCwh60971	NAT pool is not working properly despite is not reaching the 32k object ID limit.
CSCwh68068	Firepower WCCP router-id changes randomly when VRFs are configured
CSCwh69843	WM DT - ASA in transparent mode doesn't send equal IPv6 Router Advertisement packets to all nodes
CSCwh71008	CSF 4200: PSU Fan speed is critical
CSCwh71050	FXOS : Duplication of NTP entry results in Error message : Unreachable Or Invalid Ntp Server
CSCwh71161	ASA|FTD: Traceback & reload in thread Name: update_mem_reference
CSCwh82305	Lina core at swapcontext on Standby FTD during policy deployment
CSCwh83021	ASA/FTD HA pair EIGRP routes getting flushed after failover
CSCwh92345	crypto_archive file generated after the software upgrade.
CSCwh95025	GTP connections, under certain circumstances do not get cleared on issuing clear conn.
CSCwh95443	Datapath hogs causing clustering units to get kicked out of the cluster
CSCwh96055	Management DNS Servers may be unreacheable if data interface is used as the gateway
CSCwh99398	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-34-17852'
CSCwi02754	FTD 1120 Traceback and reload on standby unit with SNMP enabled.
CSCwi03407	Traceback on FP2140 without any trigger point.
CSCwi04351	FTD upgrade failling on script 999_finish/999_zz_install_bundle.sh
CSCwi06797	ASA/FTD traceback and reload on thread DATAPATH
CSCwi13134	Hardware bypass not working as expected in FP3140

Identifier	Headline
CSCwi20045	ASA/FTD may traceback and reload in Thread Name 'lina' due to a watchdog in 9.16.3.23 code
CSCwi31480	Alert: Decommission failed, reason: Internal error is not cleared from FCM or CLI after acknowledge
CSCwi31966	FTD ADI debugs may show incorrect server_group and/or realm_id for SAML-authenticated sessions
CSCwi33956	"boot config" is not working after reload on FPR1140
CSCwi36311	use kill tree function in SMA instead of SIGTERM
CSCwi36843	Detailed logging related to reason behind sub-interface admin state change during operations
CSCwi38957	Policy Apply failed moving from FDM to FMC
CSCwi40193	Hairpinning of DCE/RPC/FTP traffic during the suboptimal lookup
CSCwi43492	ASA traceback and reload on Thread Name: DATAPATH
CSCwi44208	low memory/stress causing traceback in SNMP
CSCwi44912	ISA3000 Traceback and reload boot loop
CSCwi45878	ASA/FTD: DNS Load Balancing with SAML does not work with VPN Load Balancing
CSCwi46641	FTDv may traceback and reload in Thread Name 'PTHREAD-3744' when changing interface status
CSCwi48699	ASA traceback and reload on Thread Name: pix_flash_config_thread
CSCwi49770	ASA|FTD Traceback & reload in thread name Datapath
CSCwi49884	TCP MSS is changed back to the default value when a VTI or loopback interface is created
CSCwi53987	SSL protocol settings does not modify the FDM GUI certificate configuration or disable TLSv1.1
CSCwi56667	ASA Traceback and reload on Thread Name "fover_parse" on Standby after Failover Group changes
CSCwi57476	interface idb logging log rotation to FXOS logrotate utility
CSCwi57670	RAVPN SAML: External browser gives misleading message when FTD/ASA fails to parse assertion
CSCwi57783	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Access Control Rules Bypass Vulnerability
CSCwi60285	ASA/FTD may traceback and reload in Thread Name 'lina'

Identifier	Headline
CSCwi61135	Debugs failed to be enabled on SSH session
CSCwi62796	ASA/FTD Traceback and reload related to SSL/DTLS traffic processing
CSCwi63743	ASA/FTD may traceback and reload in Thread Name "appAgent_monitor_nd_thread" & Rip: _lina_assert.
CSCwi64829	traceback and reload around function HA
CSCwi65116	DHCPv6:ASA traceback on Thread Name: DHCPv6 CLIENT.
CSCwi66461	WARN msg(speed not compatible, suspended) while creating port-channel on Victoria CE
CSCwi66676	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
CSCwi67998	Policy deployment failures on TPK MI chassis after redeploying same instance
CSCwi68604	Error logs generated for ssh access to ASA when eddsa is used as kex hostkey
CSCwi68625	Continuous snmpd restarts observed if SNMP host is configured before the IP is configured
CSCwi68833	ASA/FTD: Memory leak caused by Failover not freeing dnscrypt key cache due to unsyned umbrella flow
CSCwi69091	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi70492	Firewall is in App Sync error in pseudo-standby mode and uses IPs from Active unit
CSCwi71998	"Stream: TCP normalization error in NO_TIMESTAMP" is seen when SSL Policy decrypt all is used
CSCwi74214	ASA/FTD traceback and reload in Thread Name: IKEv2 Daemon when moving from active to standby HA
CSCwi75198	Standby FTD experiencing periodic traceback and reload
CSCwi76002	Memory exhaustion due to absence of freeing up mechanism for tmatch
CSCwi76361	Transparent firewall MAC filter does not capture frames with STP-UplinkFast dst MAC consistently
CSCwi76642	FXOS capture in Container mode behaves erratically
CSCwi77415	ASDM connection lost issue is observed in ASAv device due to config issue
CSCwi79037	IKEv2 client services is not getting enabled - XML profile is not downloaded
CSCwi79042	FTD/Lina traceback and reload of HA pairs, in data path, after adding NAT policy
CSCwi79393	Policy Deployment Fails when removing the Umbrella DNS Policy from Security Intelligence

Identifier	Headline
CSCwi84314	ASA CLI hangs with 'show run' on multiple SSH
CSCwi84615	some stdout logs not rotated by logrotate
CSCwi85689	TLS Server Identify: 'show asp table socket' output shows multiple TLS_TRK entries
CSCwi87382	Traceback and reload on Primary unit while running debugs over the SSH session
CSCwi90371	ASA:request to add "logging list" option to the "logging history" command.
CSCwi90399	FTD/ASA system clock resets to year 2023
CSCwi90571	Access to website via Clientless SSL VPN Fails
CSCwi90751	FTD/ASA - SNMP queries using snmpwalk are not displaying all "nameif" interfaces
CSCwi90998	ASA SNMP Polling Failure for environmental FXOS DME MIB (.1.3.6.1.4.1.9.9.826.2)
CSCwi94356	Lina traceback and reload in Thread Name: cli_xml_request_process
CSCwi95228	"crypto ikev2 limit queue sa_init" resets after reboot
CSCwi95639	ASA/FTD Optimise Fail-to-Wire (FTW) modules trigger in Reload/Crash scenarios
CSCwi95708	FTD: Hostname Missing from Syslog Message
CSCwi95796	FTD SNMP OID 1.3.6.1.4.1.9.9.109.1.1.1.1.7 always returns 0% for SysProc Average
CSCwi95871	SSH/SNMP connections to non-admin contexts fail after software upgrade
CSCwi95994	Chromium-based browsers have SSL connection conflicts when FIPS CC is enabled on the firewall.
CSCwi97836	ASA traceback and reload after configuring capture on nlp_int_tap and deleting context
CSCwi97839	FTD traceback assert in vni_idb_get_mode and reloaded
CSCwi97948	EIGRP bandwidth is changing after upgrade or after "shutdown"/"no shutdown" commands
CSCwi99429	Policy deployment failure rollback didnt reconfigure the FTD devices
CSCwj02505	ASA Checkheaps traceback while entering same engineID twice
CSCwj03764	In Spoke dual ISP case if ISP2 is down, VTI tunnels related to ISP1 flapping.
CSCwj03937	ENH: FTD Add debug message to indicate "No CRL found in User identity Certificate"
CSCwj04154	Intermittent loss of management traffic due to DHCP service failing to start
CSCwj05151	ASA/FTD may traceback and reload in Thread Name DATAPATH due to GTP Spin Lock Assertion

Identifier	Headline
CSCwj05484	ASA upgrade from 9.16 to 9.18 causing change in AAA ldap attribute values by adding extra slash '\'
CSCwj08015	FTW no longer working in NM3 on Warwick
CSCwj08980	ICMP replies randomly does not reaching the sender node when initiated from the node.
CSCwj09999	FP 3100 MTU change on management interface is NOT persistent across reboots (returns to default MTU)
CSCwj11331	Web Contents files appear as text/plain when they should be application/octet-stream
CSCwj13910	Crypto IPSEC SA Output Showing NO SA ERROR With IPSEC Offload Enabled
CSCwj14832	SAML: Single sign-on AnyConnect token verification failure is seen after successful authentication
CSCwj14927	FTD: Primary takes active role after reloading
CSCwj15125	ASA/FTD may traceback and reload in Thread Name 'lina' related to Netflow timer infra
CSCwj16279	username containing '@' character works for asa login but fails for 'connect fxos'
CSCwj17447	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-6-26174'
CSCwj19653	FTD - Trace back and reload due to NAT involving fqdn objects
CSCwj20067	ASA: Warning messages not displayed when Static interface NAT are configured
CSCwj21880	FTD with Interface object optimization enabled is blocking traffic after renaming of zone names
CSCwj22235	Lina traceback and reload due to mps_hash_memory pointing to null hash table
CSCwj22990	After upgrading the ASA, “Slot 1: ATA Compact Flash memory” shows a ditterent value
CSCwj25975	FTD/ASA : CSR generation with comma between “Company Name” attribute does not work expected
CSCwj30980	Addition of debugs & a show command to capture the ID usage in the CTS SXP flow.
CSCwj31475	F1758 FXOS Fault Observed in ASA Appliances Following FXOS Upgrade
CSCwj31816	TLS Secure Client sessions cannot be established on FTD Due to RSA-PSS Signing Algorithm
CSCwj31918	Segmentation fault with "logger_msg_dispatch" while HA sync
CSCwj32035	Clientless VPN users are unable to reach pages with HTTP Basic Authentication
CSCwj33487	ASA/FTD may traceback and reload while handling DTLS traffic

Identifier	Headline
CSCwj33580	IKEv2 tunnels flap due to fragmentation and throttling caused by multiple ciphers/proposal
CSCwj33891	ASA/FTD Cluster memory exhaustion caused by NAT process during release of port blocks allocations
CSCwj34881	Command to show counters for access-policy filtered with a source IP address gives incorrect result
CSCwj34975	Multiple context interfaces fail to pass traffic
CSCwj35701	Dns-guard prematurely closing conn due to timing condition
CSCwj38871	ASA traceback with thread name SSH
CSCwj38928	High latency observed on FPR31xx
CSCwj40761	ASA/FTD may traceback in Threadname: **CTM KC FPGA stats handler**
CSCwj43345	SNMP poll for some OIDs may cause CPU hogs and high latency can be observed for ICMP packets
CSCwj43902	FTDv - The interface connected to the AWS GW may have connection issues for DHCP or an idle state.
CSCwj44398	when set the route-map in route RIP on FTD, routes update is not working after FTD reload
CSCwj48704	ASA traceback and reload when accessing file system from ASDM
CSCwj48801	High latency observed on FPR42xx
CSCwj49958	Crypto IPSEC Negotiation Failing At "Failed to compute a hash value"
CSCwj50406	All IPV6 BGP routes configured in device flapping
CSCwj53725	Traceback observed while applying 'no failover' and 'failover' in the ASA standby
CSCwj54717	Radius secret key of over 14 characters for external authentication does not get deployed (FPR3100)
CSCwj55036	ASA/FTD: A delay in an async crypto command induces a traceback and subsequently a reload.
CSCwj55081	FPR3K loses connectivity to FMC via mgmt data interface on reboot of FPR3K
CSCwj56099	ASA: Running the failsafe-exit command caused the interface to enter a DISABLED state
CSCwj57435	Cleanup stale logrotate files
CSCwj59861	ASA/FTD may traceback and reload in Thread Name 'lina' due to SCP/SSH process

Identifier	Headline
CSCwj61086	High CPU usage in svc_sam_dme process during deployment post breaking cluster or deleting inline-set
CSCwj62723	Error message spammed to console on Firepower 2100 devices while enabling SSH config
CSCwj65587	Snmpwalk throws Error messages #"snmp/error: truncating integer value > 32 bits"
CSCwj68096	Console Access Stuck for ASAv hosted in CSP after Upgrade to 9.18.3.56
CSCwj68783	FTD/ASA-HA configs not in sync as the command sync process is sending configs with special chars
CSCwj69780	SNMP host group content change results in SNMP process termination on management interface
CSCwj72013	PAT communication via using PAT pool fails for about 40 seconds when a device joins a cluster
CSCwj73053	ASA may traceback and reload in Thread Name 'DATAPATH-21-16432'
CSCwj73061	SNMP OID for CPUTotal1min omits snort cpu cores entries when polled
CSCwj74323	ASAv Memory leak involving PKI/Crypto for VPN
CSCwj74716	tpk_mi upgrade failed from 7.4.1.1 > 7.6.0 000_start/000_00_run_cli_kick_start.sh.
CSCwj77700	FTD LINA Traceback and Reload idfw_proc Thread
CSCwj81031	snmpd core seen in ASA/FTD
CSCwj81743	FTD - Trace back and reload due to NAT involving fqdn objects
CSCwj81886	[WM RM]The member interface of the Port-channel is missing on the ASA(1G & 10G) post SFP JOJI/reboot
CSCwj82127	IP-SGT mappings on Lina-side are not being removed, when FMC pxGrid connection is disabled
CSCwj82285	ASA/FTD may traceback and reload in Thread Name 'sdi_work'
CSCwj82736	TLS Handshake Fails if Fragmented Client Hello Packet is Received Out of Order
CSCwj83185	FTD/ASA : Standby FTD traceback and reload after enabling memory tracking
CSCwj83238	Rommon Upgrade failed due to mismatch in descriptor table.
CSCwj83533	FAN is working as expected but FAN LED is in off state.
CSCwj83634	Seeing message "reg_fover_nlp_sessions: failover ioctl C_FOREG failed"
CSCwj86116	High LINA CPU observed due to NetFlow configuration

Identifier	Headline
CSCwj86320	Standby Unit Interfaces enter "Waiting" Status Post-FTD Upgrade Due to Incorrect "Hello" Message MAC
CSCwj87501	ASA/FTD may traceback and reload in Thread Name 'fover_FSM_thread'
CSCwj87770	FPR2100-ASA Unable to generate CSR without FXOS IP address on SAN field
CSCwj88400	FTD may traceback and reload in process name lina while processing appAgent msg reply
CSCwj89264	FTD HA: Traceback and reload in netsnmp_oid_compare_ll
CSCwj91341	Failsafe mode default values are unattainable on some platforms need adjustment per platform/mode
CSCwj92784	RAVPN: Failure to create SGT-IP mapping due to ID table exhaustion
CSCwj95590	Browser redirects to logon page when the user clicks the WebVPN bookmark
CSCwj99362	"show inventory" output shows Name: "power supply 0" on Firepower
CSCwk00604	ASA Fails to initiate AAA Authentication with IKEv2-EAP and Windows Native VPN Client
CSCwk02804	WebVPN connections stuck in CLOSEWAIT state
CSCwk02928	ASA/FTD may traceback and reload in Thread Name PTHREAD
CSCwk04290	FPR 21xx - Traceback in Process Name: lina-mps during normal operations
CSCwk04492	ASA CLI hangs with 'show run' with multiple ssh sessions
CSCwk05800	ASA/FTD SNMP polling fails due to overlapping networks in snmp-server host-group
CSCwk05851	"set ip next-hop" line deleted from config at reload if IP address is matched to a NAME
CSCwk06573	Serviceablity : Improve routing infra debugs and add new for error conditions
CSCwk07934	Clock skew between FXOS and Lina causes SAML assertion processing failure
CSCwk08476	FTD/ASA traceback and reload due to 'show bgp summary' memory leak
CSCwk08576	command to print the debug menu setting of service worker
CSCwk09612	Clock skew: FXOS clock diverges from Lina NTP time ~1-10 secs
CSCwk10884	Connectivity failure due to mismatch between l2_table and subinterface mac address
CSCwk11983	High LINA CPU observed due to NetFlow due to 'flow-export delay flow-create' configuration
CSCwk11989	Accepting duplicate object/group-object into object-group from multiple ssh sessions
CSCwk12497	Traceback and reload on active unit due to HA break operation.

Identifier	Headline
CSCwk12698	SNMP polling of admin context mgmt interface fails to show all interfaces across all contexts
CSCwk13812	ASA/FTD incorrectly forwards extended community attribute after upgrade.
CSCwk14657	Bring back support for portal-access-rule for weblaunch for RAVPN sessions
CSCwk14685	FTD : Management interface showing down despite being up and operational
CSCwk14909	Traffic drop with 'rule-transaction-in-progress' after failover with TCM cfgd in multi-ctx mode
CSCwk16332	ASA/FTD traceback and reload with high rate of SIP connections
CSCwk17854	FTD doesn't send Type A query after receiving a refuse error from one DNS server in AAAA query.
CSCwk20882	ESP sequence number of 0 being sent after SA establishment/rekey
CSCwk21561	Add warning message when configuring CCL MTU
CSCwk21562	Radius server configuration for FTD external authentication is not deployed to FTD.
CSCwk22034	Snmpwalk displays incorrect interface speeds for values greater or equal than 10G
CSCwk22574	Remove SGT frames/packets to allow VTI decryption
CSCwk22759	Issue with Setting Certain Timezones (e.g. GMT+1) on Cisco ASA Firepower in Appliance Mode
CSCwk24176	FTD/ASA - VPN traffic flowing through the device may trigger tracebacks and reloads.
CSCwk26968	Backup feature does not save/restore DAP configuration in multiple context mode.
CSCwk27830	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwk30049	ASA/FTD May traceback & reload citing Thread Name 'lina' as the faulting thread.
CSCwk31371	NAT_HARDEN: CGNAT breaks when mapped ifc is configured as any
CSCwk32501	256/1550 block depletion process fover_thread
CSCwk35710	FTD/LINA may traceback and reload when "show capture" command is executed in EEM script
CSCwk36144	Update Fan RPM Thresholds for 42xx platforms
CSCwk36312	High cpu on "update block depletion" with secondary effects (Bgp flaps, traffic drops)
CSCwk37371	SGT INLINE-TAG added after upgrade to 7.4.x
CSCwk40335	Trigger Alert/Warning when the associated FQDN IDs of an IP address surpasses the set limit of 8

Identifier	Headline
CSCwk44165	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability
CSCwk45975	TLS1.3 Decryption configuration on SSL policy is affecting DND traffic.
CSCwk46737	ASA on HA: alloc_ch() alloc from chunk mem Failed message on one context in Standby device
CSCwk47035	CMI is disabled if pre-CMI nameif on diagnostic interface is MANAGEMENT
CSCwk48628	FTD/FxOS - Upgrade/erase configuration result in App-instance 'Operational State: Starting'
CSCwk52890	FTD / ASA High Memory Usage Due to HTTP-based Path Monitoring
CSCwk61157	FTD LINA Traceback and Reload dhcp_daemon Thread
CSCwk62381	ASA might traceback and reload due to ssh/client hitting a null pointer while using SCP.
CSCwk63011	Incorrect network module slot and status information in "show module" command output
CSCwk63586	App instance stuck in STOP_FAILED with error message
CSCwk63733	HA-monitored interfaces are going into "waiting" state and subsequently to "Failed"
CSCwk64643	Failover prompt shows state active while the firewall is in Negotiation
CSCwk70673	Certificate validation fails with trustpool when FIPS is enabled
CSCwk71227	FTD running on FPR 2k with LDAP skips backslash when updating ldap.conf
CSCwk71866	ASA: Site-to-Site VPN between contexts on the same device drops traffic due to 'ipsec-tun-down'
CSCwk75956	ASA/FTD may traceback and reload in Thread Name SSH
CSCwk76362	FTDv traceback in Thread name - PTHREAD
CSCwk78030	ASA/FTD: Memory Exhaustion due to Threat-Detection
CSCwk79288	Partition "/opt/cisco/config" gets full due to btmp file not getting logrotated
CSCwk82571	VPN Client Application version and OS is not displayed for the FTD Standby peer under User Activity
CSCwk88182	FTDv50 traceback during normal operation at PTHREAD-8141 spin_lock_fair_mode_enqueue
CSCwk88201	S2S VPN with 3rd party broken after upgrading FPR 9.20
CSCwk88225	Critical fault : [FSM:FAILED]: user configuration(FSM:sam:dme:AaaUserEpUpdateUserEp)

Identifier	Headline
CSCwk89836	ASA/FTD may traceback and reload in Thread Name 'strlen'
CSCwk93762	Device traceback and reload thrice with Panic at spin_lock_fair_mode_enqueu and nlp_init().
CSCwk96912	FTD: Username missing in syslog message ID 302013 after upgrade to 7.4.1
CSCwm01544	Lina traceback and reload in data-path thread
CSCwm02801	Unstable HA causing depolyment failure
CSCwm03142	IPv6 Neighbor Discovery failure on shared interface in multi instance setup
CSCwm03287	FP4245 - NPU Accelerator changed speed of 100Gb interface to 10Mb
CSCwm04021	ASA|FTD Traceback & reload in process name lina
CSCwm04650	Increase memory usage leading to tracebacks in Lina.
CSCwm05520	Disable cluster syn cookie decoding when FTD cluster is deployed with inline-set
CSCwm05960	Generated Cryptochecksum changes without configuration change
CSCwm06393	Changes in port-channel membership or member status may cause periodic OSPF/EIGRP adjacency flaps
CSCwm07389	CGroups errors in ASA Syslog during every reboot
CSCwm07419	ldap.conf does not get generated using hostname
CSCwm08231	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Network Address Translation DNS Inspection Denial of Service Vulnerability
CSCwm08232	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Network Address Translation DNS Inspection Denial of Service Vulnerability
CSCwm08235	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software DHCP Denial of Service Vulnerability
CSCwm13199	SIP traffic is affected due to unexpected behavior with NAT untranslations.
CSCwm14509	Wrong drops seen with Invalid length for 23, 24 and 25 IE-Types during GTP inspection
CSCwm14561	ASA/FTD may traceback and reload in Thread Name 'fover_parse'
CSCwm14729	CSF 3100 series not rebooting after power outage, requiring manual power cycle
CSCwm28007	Browser redirects to blank page when the user clicks the WebVPN bookmark
CSCwm30731	The ASA's OSPF routing table is not properly synchronized with the neighbors
CSCwm33229	SAML Force re-authentication Is Not Enforcing User To re-enter Credentials Upon Retrying To Connect

Identifier	Headline
CSCwm33529	FXOS MTU Handling for Front Panel and Uplink Ports on Firepower devices require improvement
CSCwm33613	Default Group Policy is applied when receiving multiple Group Policies in SAML assertion attributes
CSCwm35035	SAML Auth Request by FTD Will Always Be Signed By Sha1 Irrelevant Of the Algorithm Configured
CSCwm35624	Long boot time seen with one AC rule having object-group and other plain ACL's
CSCwm35730	LINA may traceback in Thread Name: Datapath with NAT config
CSCwm35751	FPR3100: Interface may go to half duplex speed is hardcoded to 100mbps
CSCwm36631	FTD Secondary Unit got stuck in Bulk sync state.
CSCwm37455	ASA/FTD will allow local IP pool with invalid netmask
CSCwm42000	FTD/ASA may traceback and reload in DATAPATH thread
CSCwm42745	Dynamic Site-to-Site tunnels stuck in IN-NEG state When IKE_AUTH Is Missed
CSCwm49213	Show mod functionality needs to be fixed after change was reverted in CSCwk63011 due to regression
CSCwm49721	ASA Traceback and Reload due to MEMORY CORRUPTION WAS DETECTED
CSCwm49782	enhance sma 2nd cruz heartbeat logging
CSCwm50591	ASA/FTD: Inbound IPsec packets are dropped when IPsec offload is enabled with VTI and sub-interface
CSCwm50936	100GB interface flaps with Innolight QSFPs in both ends
CSCwm52931	ASA/FTD may traceback and reload in Thread Name "fover_parse"
CSCwm56864	show run access-list command returns warning
CSCwm60536	SQLNet traffic getting dropped intermittently in Clustering data unit.
CSCwm61282	ASA/FTD: RA VPN tunnel causing memory leak leading to traceback & Reload
CSCwm63868	FTD - Missing routes on BGP advertised-routes after FTD HA failover event
CSCwm64553	Incompatible members warning message after Po member interface flaps unable to rejoin Po
CSCwm68211	ASA traceback and reload on thread snmp_inspect
CSCwm70835	ASA traceback and reload due to stack overflow while using APCF file
CSCwm71265	ASA traceback and reload on thread DATAPATH when processing gtpv1 end marker msg for PDP

Identifier	Headline
CSCwm78351	Potential High CPU usage in Multi-Context Cluster setup with unconditional execution of capture code
CSCwm85228	ASA/FTD may traceback and reload in Thread Name "IKEv2 Daemon" while joining failover
CSCwm89523	'no capture /all' failed to disable capture completely in the backend, causing high datapath CPU
CSCwm90900	GTP inspection drops packet with error Reason:(IE-Type:CAUSE(2) IE is missing)
CSCwm90905	GTP inspection drops packet with error ERROR-DROP:MsgType:32
CSCwm91176	Cisco ASA/FTD Firepower 3100/4200 Series TLS 1.3 Cipher Denial of Service Vulnerability
CSCwm91406	FTD HA Standby Reloads Repeatedly After Upgrade to 7.4.2.1
CSCwm92397	LINA core observed pointing to "IP RIB Update" thread
CSCwm95070	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwm97054	ASA/FTD traceback and reload with high rate of SIP connections
CSCwm98278	TCP Conn not being flagged as Half-Closed after receiving the ACK for the FIN.
CSCwn01281	GTP inspection not allowing GTP data packets if session create response has cause type 18
CSCwn03446	When capture enabled on cluster interface, it always includes CCL IP along with the configured rule
CSCwn03835	ASA/FTD may traceback and reload in Thread Name 'SSH Ctxt Thread'
CSCwn13187	ASA upgrade failing from 9.20.2.21 to the target version 9.20.3.4
CSCwn13672	Bind ESP to VTI Tunnel Source Interface To Avoid Additional Route-Lookup Post Encryption
CSCwn14130	FTD cluster to traceback and reload after extended PAT is enabled
CSCwn14447	ASA/FTD may traceback and reload in Thread Name 'ldap_client_thread'
CSCwn15104	FTD reload with traceback on swapcontext function
CSCwn16320	Syslog servers below in FTD logging send hostname info as per emblem config for first syslog server
CSCwn17121	ASA/FTD may traceback and reload in Thread Name 'cli_xml_request_process'.
CSCwn19639	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Access Control Rules Bypass Vulnerability

Identifier	Headline
CSCwn19706	Admin users are prompted to change local password when authenticating to external server
CSCwn19739	HA would bring data interfaces up while moving from cold standby to failed state
CSCwn20024	ASA may traceback and reload in Thread Name 'ssh'
CSCwn20642	Discrepancy in VPN bytes with RA VPN user activity report
CSCwn21584	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Web Services Denial of Service Vulnerability
CSCwn22036	FTD: Management0/0 status went down, line protocol is up after upgrade
CSCwn22456	GTPv2 IE-type 157 (Signaling Priority Indication) is dropped with reason as unknown IE type
CSCwn24577	ASA booting process may freeze when including 'no pim' or 'no igmp' config
CSCwn26165	FTD/ASA May Traceback and Reload - During Deployment / Radius changes - Due to Radius Packets
CSCwn27819	Jumbo frame packets are being fragmented
CSCwn31240	Traceback and reload due to webvpn dtls flow offload enabled
CSCwn31588	FTD 7.6.0 instances going in split brain when assigned RP with CPU cores between 13-36 on MI- FP42xx
CSCwn34259	Monitored interfaces may go in waiting state after upgrade to 9.20.3.7
CSCwn34659	Firewall not initiating TCP request even after receiving the TC bit set in DNS response
CSCwn34707	Multiple Unicorn Admin Handler processes consume all the control plane CPU.
CSCwn39826	HA should prevent honouring failover requests while copy/config-sync/rollback is in progress
CSCwn40485	MI: Traffic fails to reach the Secondary FTD when enabled with data-sharing interface
CSCwn42949	Implementing forwarder flow on non-owner units handling distributed secondary flow connections
CSCwn44335	FXOS - Download command generates an extra "/" over HTTP and HTTPS GET requests
CSCwn46426	ASA 21xx: 'sh environment temperature' shows incorrect temperature values
CSCwn46855	LINA may observe random traceback with Netflow configured
CSCwo01557	ASA traceback and reload on DATAPATH thread due to memory corruption
CSCwo49928	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability

Cisco General Terms

The Cisco General Terms (including other related terms) governs the use of Cisco software. You can request a physical copy from Cisco Systems, Inc., P.O. Box 641387, San Jose, CA 95164-1387. Non-Cisco software purchased from Cisco is subject to applicable vendor license terms. See also: https://cisco.com/go/generalterms.

Related Documentation

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