Cisco Firepower Release Notes, Version 6.4.x

First Published: 2019-04-24

Last Modified: 2019-10-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 1

Welcome

This document contains release information for Version 6.4 of Cisco Firepower Threat Defense, Firepower Management Center, Firepower Device Manager, and Firepower Classic devices (Firepower 7000/8000 series, NGIPSv, ASA with FirePOWER Services).

For Cisco Defense Orchestrator (CDO) with FDM, also see What's New for Cisco Defense Orchestrator.

Release Dates

Sometimes we release updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. If you downloaded an earlier build, do not use it. For more information, see Resolved Bugs in New Builds, on page 61.

Table 1: Version 6.4 Dates

Version	Build	Date	Platforms
6.4.0.18	24	2024-04-24	All
6.4.0.17	26	2023-09-28	All
6.4.0.16	50	2022-11-21	All
6.4.0.15	26	2022-05-31	All
6.4.0.14	67	2022-02-18	All
6.4.0.13	57	2021-12-02	All
6.4.0.12	112	2021-05-12	All
6.4.0.11	11	2021-01-11	All
6.4.0.10	95	2020-10-21	All
6.4.0.9	62	2020-05-26	All

Version	Build	Date	Platforms
6.4.0.8	28	2020-01-29	All
6.4.0.7	53	2019-12-19	All
6.4.0.6	28	2019-10-16	No longer available.
6.4.0.5	23	2019-09-18	All
6.4.0.4	34	2019-08-21	All
6.4.0.3	29	2019-07-17	All
6.4.0.2	35	2019-07-03	FMC/FMCv FTD/FTDv, except Firepower 1000 series
	34	2019-06-27	—
		2019-06-26	Firepower 7000/8000 series ASA FirePOWER NGIPSv
6.4.0.1	17	2019-06-27	FMC 1600, 2600, 4600
		2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 with SM-40, SM-48, and SM-56 modules
		2019-05-15	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, and SM-44 modules ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Firepower 7000/8000 series NGIPSv

Version	Build	Date	Platforms
6.4.0	113	2020-03-03	FMC/FMCv
	102	2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 with SM-40, SM-48, and SM-56 modules
		2019-06-13	Firepower 1010, 1120, 1140
		2019-04-24	Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, and SM-44 modules ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Firepower 7000/8000 series NGIPSv

Sharing Data with Cisco

The following features share data with Cisco.

Cisco Success Network

Cisco Success Network sends usage information and statistics to Cisco, which are essential to provide you with technical support.

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.

Web Analytics

Web analytics provides non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.

You are enrolled by default but you can change your enrollment at any time after you complete initial setup. Note that ad blockers can block web analytics, so if you choose to remain enrolled, please disable ad blocking for the hostnames/IP addresses of your Cisco appliances.

For Assistance

Upgrade Guides

In management center deployments, the management center must run the same or newer version as its managed devices. Upgrade the management center first, then devices. Note that you always want to use the upgrade guide for the version of management center or device manager that you are *currently* running—not your target version.

Table 2: Upgrade Guides

Platform	Upgrade Guide	Link
Management center	Management center version you are *currently* running.	https://www.cisco.com/go/fmc-upgrade
Threat defense with management center	Management center version you are *currently* running.	https://www.cisco.com/go/ftd-fmc-upgrade
Threat defense with device manager	Threat defense version you are *currently* running.	https://www.cisco.com/go/ftd-fdm-upgrade
Threat defense with cloud-delivered Firewall Management Center	Cloud-delivered Firewall Management Center.	https://www.cisco.com/go/ftd-cdfmc-upgrade

Install Guides

If you cannot or do not want to upgrade, you can freshly install major and maintenance releases. This is also called *reimaging*. You cannot reimage to a patch. Install the appropriate major or maintenance release, then apply the patch. If you are reimaging to an earlier threat defense version on an FXOS device, perform a full reimage—even for devices where the operating system and software are bundled.

Table 3: Install Guides

Platform	Install Guide	Link
Management center hardware	Getting started guide for your management center hardware model.	https://www.cisco.com/go/fmc-install
Management center virtual	Getting started guide for the management center virtual.	https://www.cisco.com/go/fmcv-quick
Threat defense hardware	Getting started or reimage guide for your device model.	https://www.cisco.com/go/ftd-quick
Threat defense virtual	Getting started guide for your threat defense virtual version.	https://www.cisco.com/go/ftdv-quick

Platform	Install Guide	Link
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://www.cisco.com/go/firepower9300-config
FXOS for the Firepower 1000/2100 and Secure Firewall 3100	Troubleshooting guide, in the *Reimage Procedures* chapter.	Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense

More Online Resources

Cisco provides the following online resources to download documentation, software, and tools; to query bugs; and to open service requests. Use these resources to install and configure Cisco software and to troubleshoot and resolve technical issues.

- Documentation: http://www.cisco.com/go/threatdefense-64-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts

CHAPTER 2

System Requirements

This document includes the system requirements for Version 6.4.

FMC Platforms

The FMC provides a centralized firewall management console. For device compatibility with the FMC, see Device Management, on page 11. For general compatibility information, see the Cisco Secure Firewall Management Center Compatibility Guide.

FMC Hardware

Version 6.4 supports the following FMC hardware:

- Firepower Management Center 1600, 2600, 4600
- Firepower Management Center 1000, 2500, 4500
- Firepower Management Center 2000, 4000
- Firepower Management Center 750, 1500, 3500 (high availability not supported for FMC 750)

You should also keep the BIOS and RAID controller firmware up to date; see the Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes.

FMCv

Version 6.4 supports FMCv deployments in both public and private clouds.

With the FMCv, you can purchase a license to manage 2, 10, or 25 devices. Some versions and platforms support 300 devices. For full details on supported instances, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide.

Table 4: Version 6.4 FMCv Platforms

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			
Amazon Web Services (AWS)	YES	—	—
Microsoft Azure	YES	—	—
Private Cloud			
Kernel-based virtual machine (KVM)	YES	—	—
VMware vSphere/VMware ESXi 6.0 or 6.5	YES	—	—

Cloud-delivered Firewall Management Center

The Cisco cloud-delivered Firewall Management Center is delivered via the Cisco Defense Orchestrator (CDO) platform, which unites management across multiple Cisco security solutions. We take care of feature updates. Note that a customer-deployed management center is often referred to as *on-prem*, even for virtual platforms.

At the time this document was published, the cloud-delivered Firewall Management Center could manage devices running threat defense . For up-to-date compatibility information, see the Cisco Cloud-Delivered Firewall Management Center Release Notes.

Device Platforms

Firepower devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules. For details on device management methods, see Device Management, on page 11. For general compatibility information, see the Cisco Secure Firewall Threat Defense Compatibility Guide or the Cisco Firepower Classic Device Compatibility Guide.

FTD Hardware

Version 6.4 FTD hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 5: Version 6.4 FTD Hardware

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 1010, 1120, 1140	YES	—	YES	YES	—
Firepower 2110, 2120, 2130, 2140	YES	—	YES	YES	—

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 4110, 4120, 4140, 4150 Firepower 4115, 4125, 4145 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	YES	—	—	—	Requires FXOS 2.6.1.157 or later build. We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
ASA 5515-X ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X	YES	—	YES	YES	ASA 5508-X and 5516-X devices may require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ISA 3000	YES	—	YES	YES	May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

FTDv

Version 6.4 supports the following FTDv implementations. For information on supported instances, throughputs, and other hosting requirements, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.

Table 6: Version 6.4 FTDv Platforms

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
Public Cloud				
Amazon Web Services (AWS)	YES	—	—	—
Microsoft Azure	YES	—	—	—
Private Cloud				
Kernel-based virtual machine (KVM)	YES	—	YES	YES

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
VMware vSphere/VMware ESXi 6.0 or 6.5	YES	—	YES	YES

Firepower Classic: Firepower 7000/8000, ASA FirePOWER, NGIPSv

Firepower Classic devices run NGIPS software on the following platforms:

- Firepower 7000/8000 series hardware comes in a range of throughputs, scalability capabilities, and form factors.
- ASA devices can run NGIPS software as a separate application (the *ASA FirePOWER module*). Traffic is sent to the module after ASA firewall policies are applied. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues.
- NGIPSv runs the software in virtualized environments.

Table 7: Version 6.4 NGIPS Platforms

Device Platform	FMC Compatibility	ASDM Compatibility	Notes
Firepower 7010, 7020, 7030, 7050 Firepower 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140 Firepower 8250, 8260, 8270, 8290 Firepower 8350, 8360, 8370, 8390 AMP 7150, 8050, 8150 AMP 8350, 8360, 8370, 8390	YES	—	—
ASA 5508-X, 5516-X	YES	Requires ASDM 7.12(1).	Requires ASA 9.5(2) to 9.16(x). May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ASA 5515-X	YES	Requires ASDM 7.12(1).	Requires ASA 9.5(2) to 9.12(x).

Device Platform	FMC Compatibility	ASDM Compatibility	Notes
ASA 5525-X, 5545-X, 5555-X	YES	Requires ASDM 7.12(1).	Requires ASA 9.5(2) to 9.14(x).
ISA 3000	YES	Requires ASDM 7.12(1).	Requires ASA 9.5(2) to 9.16(x). May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
NGIPSv	YES	—	Requires VMware vSphere/VMware ESXi 6.0 or 6.5. For supported instances, throughputs, and other hosting requirements, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

Device Management

Depending on device model and version, we support the following management methods.

FMC

All devices support remote management with FMC, which must run the *same or newer* version as its managed devices. This means:

- You *can* manage older devices with a newer FMC, usually a few major versions back. However, we recommend you always update your entire deployment. New features and resolved issues often require the latest release on both the FMC and its managed devices.
- You *cannot* upgrade a device past the FMC. Even for maintenance (third-digit) releases, you must upgrade the FMC first.

Note that in most cases you can upgrade an older device directly to the FMC's major version. However, sometimes you can manage an older device that you cannot directly upgrade, even though the target version is supported on the device. For release-specific requirements, see Minimum Version to Upgrade, on page 32.

Table 8: FMC-Device Compatibility

FMC Version	Oldest Device Version You Can Manage
7.4	7.0
7.3	6.7
7.2	6.6
7.1	6.5

FMC Version	Oldest Device Version You Can Manage
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1
5.4.1	5.4.1 for ASA FirePOWER on the ASA-5506-X series, ASA5508-X, and ASA5516-X. 5.3.1 for ASA FirePOWER on the ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, and ASA-5585-X series. 5.3.0 for Firepower 7000/8000 series and legacy devices.

FDM

You can use FDM to locally manage a single FTD device.

Optionally, add Cisco Defense Orchestrator (CDO) to remotely manage multiple FTD devices, as an alternative to the FMC. Although some configurations still require FDM, CDO allows you to establish and maintain consistent security policies across your FTD deployment.

ASDM

You can use ASDM to locally manage a single ASA FirePOWER module, which is a separate application on an ASA device. Traffic is sent to the module after ASA firewall policies are applied. Newer versions of ASDM can manage newer ASA FirePOWER modules.

CHAPTER 3

Features

This document describes the new and deprecated features for Version 6.4.

For earlier releases, see Cisco Secure Firewall Management Center New Features by Release and Cisco Secure Firewall Device Manager New Features by Release.

Upgrade Impact

A feature has upgrade impact if upgrading and deploying can cause the system to process traffic or otherwise act differently without any other action on your part; this is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade; for example, if you must change a configuration.

Snort

Snort 3 is the default inspection engine for FTD starting in Version 6.7 (with FDM) and Version 7.0 (with FMC). Snort 3 features for FMC deployments also apply to FDM, even if they are not listed as new FDM features. However, keep in mind that the FMC may offer more configurable options than FDM.

Important If you are still using the Snort 2 inspection engine, switch to Snort 3 now for improved detection and performance. Snort 2 will be deprecated in a future release and will eventually prevent threat defense upgrade.

Intrusion Rules and Keywords

Upgrades can import and auto-enable new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. If a newer intrusion rule uses keywords that are not supported in your current version, that rule is not imported when you update the SRU/LSP. After you upgrade and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow.

For details on new keywords, see the Snort release notes: https://www.snort.org/downloads.

FlexConfig

Upgrades can add web interface or Smart CLI support for features that previously required FlexConfig. The upgrade does not convert FlexConfigs. After upgrade, configure the newly supported features in the web interface or Smart CLI. When you are satisfied with the new configuration, delete the deprecated FlexConfigs.

The feature descriptions below include information on deprecated FlexConfigs when appropriate. For a full list of deprecated FlexConfigs, see your configuration guide.

⚠

Caution Although you cannot newly assign or create FlexConfig objects using deprecated commands, in most cases existing FlexConfigs continue to work and you can still deploy. However, sometimes, using deprecated commands can cause deployment issues.

FMC Features in Version 6.4.x

Table 9: FMC Features in Version 6.4.x Patches

Feature	Details
Version 6.4.0.17 Smaller VDB for lower memory devices.	For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Minimum threat defense: Any Lower memory devices: ASA 5506-X series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Version restrictions: The ability to install a smaller VDB depends on the version of the FMC, not managed devices. If you upgrade the FMC from a supported version to an unsupported version, you cannot install VDB 363+ if your deployment includes even one lower memory device. For a list of affected releases, see CSCwd88641.
Version 6.4.0.10 Upgrades postpone scheduled tasks.	**Upgrade impact.** Upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for Firepower appliances *running* Version 6.4.0.10 or any later patch. It is not supported for upgrades *to* Version 6.4.0.10, or upgrades that skip Version 6.4.0.10. This feature is temporarily deprecated in Versions 6.5.0–6.6.1, but returns in Version 6.6.3.

Feature	Details
Version 6.4.0.9 Default HTTPS server certificates.	**Upgrade impact.** Upgrading an FMC or 7000/8000 series device from Version 6.4.0–6.4.0.8 to any later Version 6.4.0.x patch (or an FMC to Version 6.6.0+) renews the *default* HTTPS server certificate, which expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan. Your old certificate was set to expire depending on when it was generated, as follows: • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3 and earlier: 20 years Note that in Version 6.5.0–6.5.0.4, the lifespan-on-renew returns to 3 years, but this is again updated to 800 days with Version 6.5.0.5 and 6.6.0.
Version 6.4.0.4 New syslog fields.	These new syslog fields collectively identify a unique connection event: • Sensor UUID • First Packet Time • Connection Instance ID • Connection Counter These fields also appear in syslogs for intrusion, file, and malware events, allowing connection events to be associated with those events.
Version 6.4.0.2 Detection of rule conflicts in FTD NAT policies.	**Upgrade impact.** After you upgrade to Version 6.4.0.2 or later patch, you can no longer create FTD NAT policies with conflicting rules (often referred to as *duplicate* or *overlapping* rules). This fixes an issue where conflicting NAT rules were applied out-of-order. If you currently have conflicting NAT rules, you will be able to deploy post-upgrade. However, your NAT rules will continue to be applied out-of-order. Therefore, we recommend that after the upgrade, you inspect your FTD NAT policies by editing (no changes are needed) then attempting to resave. If you have rule conflicts, the system will prevent you from saving. Correct the issues, save, and then deploy.
Version 6.4.0.2 ISE Connection Status Monitor health module.	A new health module, the *ISE Connection Status Monitor*, monitors the status of the server connections between the Cisco Identity Services Engine (ISE) and the FMC.

Table 10: FMC Features in Version 6.4.0

Feature	Details
Platform	
FMC 1600, 2600, and 4600.	We introduced the FMC models FMC 1600, 2600, and 4600.

Feature	Details
FMCv for Azure.	We introduced FMCv for Microsoft Azure.
FTD on the Firepower 1010, 1120, and 1140.	We introduced the Firepower 1010, 1120, and 1140.
FTD on the Firepower 4115, 4125, and 4145.	We introduced the Firepower 4115, 4125, and 4145.
Firepower 9300 SM-40, SM-48, and SM-56 support.	We introduced three new security modules: SM-40, SM-48, and SM-56. With FXOS 2.6.1, you can mix different types of security modules in the same chassis.
ASA and FTD on the same Firepower 9300.	With FXOS 2.6.1, you can now deploy ASA and FTD logical devices on the same Firepower 9300.
Firepower Threat Defense: Device Management	
FTDv for VMware defaults to vmxnet3 interfaces.	FTDv for VMware now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. The vmxnet3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance. **Note** Version 6.6 ends support for e1000 interfaces. You will not be able to upgrade to Version 6.6+ until you switch to vmxnet3 or ixgbe interfaces. We recommend you do this now. For more information, refer to the instructions on adding and configuring VMware interfaces in the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide. Supported platforms: FTDv for VMware
Firepower Threat Defense: Routing	
Rotating (keychain) authentication for OSPFv2 routing.	You can now use rotating (keychain) authentication when configuring OSPFv2 routing. New/modified pages: • **Objects** > **Object Management** > **Key Chain** object • **Devices** > **Device Management** > edit device **>** **Routing** tab **>** **OSPF** settings **>** **Interface** tab > add/edit interface > **Authentication** option • **Devices** > **Device Management** **>** edit device **>** **Routing** tab **>** **OSPF** settings **>** **Area** tab **>** add/edit area **>** **Virtual Link** sub-tab **>** add/edit virtual link **>** **Authentication** option Supported platforms: FTD
Firepower Threat Defense: Encryption and VPN	

Feature	Details
RA VPN: Secondary authentication.	Secondary authentication, also called double authentication, adds an additional layer of security to RA VPN connections by using two different authentication servers. With secondary authentication enabled, AnyConnect VPN users must provide two sets of credentials to log in to the VPN gateway. RA VPN supports secondary authentication for the AAA Only and Client Certificate and AAA authentication methods. New/modified pages: **Devices** > **VPN** > **Remote Access >** add/edit configuration **> Connection Profile > AAA** area Supported platforms: FTD
Site-to-site VPN: Dynamic IP addresses for extranet endpoints.	You can now configure site to site VPNs to use a dynamic IP address for extranet endpoints. In hub-and-spoke deployments, you can use a hub as an extranet endpoint. New/modified pages: **Devices** > **VPN** > **Site To Site >** add/edit FTD VPN topology **> Endpoints** tab > add endpoint **> IP Address** option Supported platforms: FTD
Site-to-site VPN: Dynamic crypto maps for point-to-point topologies.	You can now use dynamic crypto maps in point-to-point as well as in hub-and-spoke VPN topologies. Dynamic crypto maps are still not supported for full mesh topologies. You specify the crypto map type when you configure a topology. Make sure you also specify a dynamic IP address for one of the peers in the topology. New/modified pages: **Devices** > **VPN** > **Site To Site >** add/edit FTD VPN topology **> IPsec** tab **> Crypto Map Type** option Supported platforms: FTD

Feature	Details
TLS crypto acceleration.	**Upgrade impact.** SSL hardware acceleration has been renamed *TLS crypto acceleration*. Depending on the device, TLS crypto acceleration might be performed in software or in hardware. The Version 6.4.0 upgrade process automatically enables acceleration on all eligible devices, even if you previously disabled the feature manually. In most cases you cannot configure this feature; it is automatically enabled and you cannot disable it. However, if you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can enable TLS crypto acceleration for *one* container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances. New FXOS CLI commands for the Firepower 4100/9300 chassis: • **show hwCrypto** • **config hwCrypto** New FTD CLI commands: • **show crypto accelerator status** (replaces **system support ssl-hw-status**) Removed FTD CLI commands: • **system support ssl-hw-accel** • **system support ssl-hw-status** Supported platforms: Firepower 2100 series, Firepower 4100/9300
Event Logging and Analysis	
Improvements to syslog messages for file and malware events.	Fully qualified file and malware event data can now be sent from managed devices via syslog. New/modified pages: **Policies** > **Access Control** > **Access Control >** add/edit policy **> Logging** tab **> File and Malware Settings** area Supported platforms: Any
Search intrusion events by CVE ID.	You can now search for intrusion events generated as a result of a particular CVE exploit. New/modified pages: **Analysis** > **Search** Supported platforms: FMC
IntrusionPolicy field is now included in syslog.	Intrusion event syslog messages now specify the intrusion policy that triggered the event. Supported platforms: Any

Feature	Details
Cisco SecureX integration.	Cisco SecureX is a cloud offering that helps you rapidly detect, investigate, and respond to threats. This feature lets you analyze incidents using data aggregated from multiple products, including Firepower Threat Defense. Note that the FMC web interface refers to this offering as *Cisco Threat Response (CTR)*. See the Cisco Secure Firewall Threat Defense and SecureX Integration Guide. New/modified pages: **System** > **Integration** > **Cloud Services** Supported platforms: FTD
Splunk integration.	Splunk users can use a new, separate Splunk app, Cisco Secure Firewall (f.k.a. Firepower) app for Splunk, to analyze events. Available functionality is affected by your Firepower version. See Cisco Secure Firewall App for Splunk User Guide. Supported platforms: FMC
Cisco Security Analytics and Logging (SaaS) integration.	You can send Firepower events to the Stealthwatch Cloud for storage, and optionally make your Firepower event data available for security analytics using Stealthwatch Cloud. Using Cisco Security Analytics and Logging (SaaS), also known as SAL (SaaS), your Firepower devices send events as syslog messages to a Security Events Connector (SEC) installed on a virtual machine on your network, and this SEC forwards the events to the Stealthwatch cloud for storage. You view and work with your events using the web-based Cisco Defense Orchestrator (CDO) portal. Depending on the license you purchase, you can also use the Stealthwatch portal to access that product's analytics features. See Cisco Secure Firewall Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide. Supported platforms: FTD with FMC
Administration and Troubleshooting	
New licensing capabilities for ISA 3000.	For ASA FirePOWER and FTD deployments, the ISA 3000 now supports URL Filtering and Malware licenses and their associated features. For FTD only, the ISA 3000 also now supports Specific License Reservation for approved customers. Supported platforms: ISA 3000
Scheduled remote backups of managed devices.	You can now use the FMC to schedule remote backups of certain managed devices. Previously, only Firepower 7000/8000 series devices supported scheduled backups, and you had to use the device's local GUI. New/modified pages: **System** > **Tools** > **Scheduling** > add/edit task > choose **Job Type: Backup** > choose a **Backup Type** Supported platforms: FTD physical platforms, FTDv for VMware, Firepower 7000/8000 series Exceptions: No support for FTD clustered devices or container instances

Feature	Details
Ability to disable Duplicate Address Detection (DAD) on management interfaces.	When you enable IPv6, you can disable DAD. You might want to disable DAD because using DAD opens up the possibility of denial of service attacks. If you disable this setting, you need check manually that this interface is not using an already-assigned address. New/modified pages: **System** > **Configuration** > **Management Interfaces** > **Interfaces** area **>** edit interface **> IPv6 DAD** check box Supported platforms: FMC, Firepower 7000/8000 series
Ability to disable ICMPv6 Echo Reply and Destination Unreachable messages on management interfaces.	When you enable IPv6, you can now disable ICMPv6 Echo Reply and Destination Unreachable messages. You might want to disable these packets to guard against potential denial of service attacks. Disabling Echo Reply packets means you cannot use IPv6 ping to the device management interfaces for testing purposes. New/modified pages: **System** > **Configuration** > **Management Interfaces** > **ICMPv6** New/modified commands: • **configure network ipv6 destination-unreachable** • **configure network ipv6 echo-reply** Supported platforms: FMC (web interface only), managed devices (CLI only)
Support for the Service-Type attribute for FTD users defined on the RADIUS server.	For RADIUS authentication of FTD CLI users, you used to have to predefine the usernames in the RADIUS external authentication object and manually make sure that the list matched usernames defined on the RADIUS server. You can now define CLI users on the RADIUS server using the Service-Type attribute and also define both Basic and Config user roles. To use this method, be sure to leave the shell access filter blank in the external authentication object. New/modified pages: **System** > **Users** > **External Authentication** tab **>** add/edit external authentication object **> Shell Access Filter** Supported platforms: FTD
View object use.	The object manager now allows you to see the policies, settings, and other objects where a network, port, VLAN, or URL object is used. New/modified pages: **Objects > Object Management >** choose object type **>** Find Usage (binoculars) icon Supported platforms: FMC

Feature	Details
Hit counts for access control and prefilter rules.	You can now access hit counts for access control and prefilter rules on your FTD devices. New/modified pages: • **Policies** > **Access Control** > **Access Control** **>** add/edit policy **> Analyze Hit Counts** • **Policies** > **Access Control** > **Prefilter** **>** add/edit policy **> Analyze Hit Counts** New commands: • **show rule hits** • **clear rule hits** • **cluster exec show rule hits** • **cluster exec clear rule hits** • **show cluster rule hits** Modified commands: **show failover** Supported platforms: FTD
URL Filtering health monitor improvements.	You can now configure time thresholds for URL Filtering Monitor alerts. New/modified pages: **System** > **Health** > **Policy** **>** add/edit policy **> URL Filtering Monitor** Supported platforms: Any
Connection-based troubleshooting.	Connection-based troubleshooting or debugging provides uniform debugging across modules to collect appropriate logs for a specific connection. It also supports level-based debugging up to 7 levels and enables uniform log collection mechanism for lina and Snort logs. New/modified commands: • **clear packet debugs** • **debug packet start** • **debug packet stop** • **show packet debugs** Supported platforms: FTD
New Cisco Success Network monitoring capabilities	Added the following Cisco Success Network monitoring capabilities: • CSPA (Cisco Security Packet Analyzer) query information • Contextual cross-launch instances enabled on the FMC • TLS/SSL inspection events • Snort restarts Supported platforms: FMC
Security and Hardening	

Feature	Details
Signed SRU, VDB, and GeoDB updates.	So Firepower can verify that you are using the correct update files, Version 6.4.0+ uses *signed* updates for intrusion rules (SRU), the vulnerability database (VDB), and the geolocation database (GeoDB). Earlier versions continue to use unsigned updates. Unless you manually download updates from Cosco—for example, in an air-gapped deployment—you should not notice any difference in functionality. If, however, you do manually download and install SRU, VDB, and GeoDB updates, make sure you download the correct package for your current version. Signed update files for Version 6.4.0+ begin with 'Cisco' instead of 'Sourcefire,' and terminate in .sh.REL.tar instead of .sh: • SRU: Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB: Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB: Cisco_GEODB_Update-*date-build*.sh.REL.tar Update files for Version 5.x through 6.3 still use the old naming scheme: • SRU: Sourcefire_Rule_Update-*date-build*-vrt.sh • VDB: Sourcefire_VDB_Fingerprint_Database-4.5.0-*version*.sh • GeoDB: Sourcefire_Geodb_Update-*date-build*.sh We will provide both signed and unsigned updates until the end-of-support for versions that require unsigned updates. Do not untar signed (.tar) packages. **Note** If you accidentally upload a signed update to an older FMC or ASA FirePOWER device, you must manually delete it. Leaving the package takes up disk space, and also may cause issues with future upgrades. Supported platforms: Any
SNMPv3 users can authenticate using a SHA-256 authorization algorithm.	SNMPv3 users can now authenticate using a SHA-256 algorithm. New/modified screen: **Devices** > **Platform Settings** > **SNMP** > **Users** > **Auth Algorithm Type** Supported platforms: Firepower Threat Defense
2048-bit certificate keys now required (security enhancement).	**Upgrade impact.** When making secure connections to external data sources, such as AMP for Endpoints or Cisco Threat Intelligence Detector (TID), the FMC now requires that the server certificate be generated with keys that are at least 2048 bits long. Certificates previously generated with 1024-bit keys will no longer work. Note that this security enhancement was introduced in Version 6.3.0.3. If you are upgrading from Version 6.1.0 through 6.3.0.2, you may be affected. If you cannot connect, regenerate the server certificate on your data source. If necessary, reconfigure the FMC connection to the data source. Supported platforms: FMC
Usability and Performance	

Feature	Details
Snort restart improvements.	Before Version 6.4.0, during Snort restarts, the system dropped encrypted connections that matched a 'Do not decrypt' SSL rule or default policy action. Now, routed/transparent traffic passes without inspection instead of dropping, as long as you did not disable large flow offload or Snort preserve-connection. Supported platforms: Firepower 4100/9300
Performance improvement for selected IPS traffic.	**Upgrade impact.** Egress optimization is a performance feature targeted for selected IPS traffic. It is enabled by default on all FTD platforms, and the Version 6.4.0 upgrade process enables egress optimization on eligible devices. New/modified commands: • **asp inspect-dp egress optimization** • **show asp inspect-dp egress optimization** • **clear asp inspect-dp egress optimization** • **show conn state egress_optimization** For more information, see the Cisco Secure Firewall Threat Defense Command Reference. To troubleshoot issues with egress optimization, contact Cisco TAC. **Note** To mitigate CSCvq34340, patching FTD device to Version 6.4.0.7+ turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled. We recommend you upgrade to Version 6.6+, where this issue is fixed. That will turn egress optimization back on, if you left the feature 'enabled.' If you remain at Version 6.4.0–6.4.0.6, you should manually disable egress optimization from the FTD CLI: **no asp inspect-dp egress-optimization**. For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature. Supported platforms: FTD
Faster SNMP event logging.	Performance improvements when sending intrusion and connection events to an external SNMP trap server. Supported platforms: Any
Faster deploy.	Improvements to appliance communications and deploy framework. Supported platforms: FTD
Faster upgrade.	Improvements to the event database. Supported platforms: Any
Firepower Management Center REST API	

Feature	Details
New REST API capabilities.	Added REST API objects to support Version 6.4.0 features: • cloudeventsconfigs: Manage SecureX integration. • ftddevicecluster: Manage chassis clustering. • hitcounts: Manage hit count statistics for access control and prefilter rules. • keychain: Manage key chain objects used for rotating authentication when configuring OSPFv2 routing. • loggingsettings: Manage logging settings for access control policies Supported platforms: FMC
API Explorer based on OAS.	Version 6.4.0 uses a new API Explorer, based on the OpenAPI Specification (OAS). As part of the OAS, you now use CodeGen to generate sample code. You can still access the legacy API Explorer if you prefer. Supported platforms: FMC
Deprecated Features	
Deprecated: SSL hardware acceleration FTD CLI commands.	As part of the TLS crypto acceleration feature, we removed the following FTD CLI commands: • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status**
Deprecated: Geolocation details.	In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on. The new country code package has the same file name as the old all-in-one package: Cisco_GEODB_Update-*date-build*. This allows deployments running Version 7.1 and earlier to continue to obtain GeoDB updates. If you manually download GeoDB updates—for example, in an air-gapped deployment—make sure you get the country code package and not the IP package. **Important** This split does not affect geolocation rules or traffic handling in any way—those rules rely only on the data in the country code package. However, because the country code package essentially replaces the all-in-one package, the contextual data is no longer updated and will grow stale. To obtain fresh data, upgrade or reimage the FMC to Version 7.2+ and update the GeoDB.

FDM Features in Version 6.4.x

Table 11: FDM Features in Version 6.4.x

Feature	Description
Firepower 1000 series device configuration.	You can configure Firepower Threat Defense on Firepower 1000 series devices using FDM. Note that you can configure and use the Power over Ethernet (PoE) ports as regular Ethernet ports, but you cannot enable or configure any PoE-related properties.
Hardware bypass for the ISA 3000.	You can now configure hardware bypass for the ISA 3000 on the **Device** > **Interfaces** page. In release 6.3, you needed to configure hardware bypass using FlexConfig. If you are using FlexConfig, please redo the configuring on the Interfaces page and remove the hardware bypass commands from FlexConfig. However, the portion of the FlexConfig devoted to disabling TCP sequence number randomization is still recommended.
Ability to reboot and shut down the system from the FDM CLI Console.	You can now issue the **reboot** and **shutdown** commands through the CLI Console in FDM. Previously, you needed to open a separate SSH session to the device to reboot or shut down the system. You must have Administrator privileges to use these commands.
External Authentication and Authorization using RADIUS for Firepower Threat Defense CLI Users.	You can use an external RADIUS server to authenticate and authorize users logging into the Firepower Threat Defense CLI. You can give external users config (administrator) or basic (read-only) access. We added the SSH configuration to the **AAA Configuration** tab on the **Device** > **System Settings** > **Management Access** page.
Support for network range objects and nested network group objects.	You can now create network objects that specify a range of IPv4 or IPv6 addresses, and network group objects that include other network groups (that is, nested groups). We modified the network object and network group object Add/Edit dialog boxes to include these features, and modified the various security policies to allow the use of these objects, contingent on whether address specifications of that type make sense within the context of the policy.
Full-text search options for objects and rules.	You can do a full-text search on objects and rules. By searching a policy or object list that has a large number of items, you can find all items that include your search string anywhere within the rule or object. We added a search box to all policies that have rules, and to all pages on the **Objects** list. In addition, you can use the **filter=fts~***search-string* option on GET calls for supported objects in the API to retrieve items based on a full-text search.
Obtaining a list of supported API versions for an FDM-managed Firepower Threat Defense device.	You can use the GET /api/versions (ApiVersions) method to get a list of the API versions that are supported on a device. You can use your API client to communicate and configure the device using commands and syntax valid for any of the supported versions.

Feature	Description
Hit counts for access control rules.	You can now view hit counts for access control rules. The hit counts indicate how often connections matched the rule. We updated the access control policy to include hit count information. In the Firepower Threat Defense API, we added the HitCounts resource and the **includeHitCounts** and **filter=fetchZeroHitCounts** options to the GET Access Policy Rules resource.
Site-to-Site VPN enhancements for dynamic addressing and certificate authentication.	You can now configure site-to-site VPN connections to use certificates instead of preshared keys to authenticate the peers. You can also configure connections where the remote peer has an unknown (dynamic) IP address. We added options to the Site-to-Site VPN wizard and the IKEv1 policy object.
Support for RADIUS servers and Change of Authorization in remote access VPN.	You can now use RADIUS servers for authenticating, authorizing, and accounting remote access VPN (RA VPN) users. You can also configure Change of Authentication (CoA), also known as dynamic authorization, to alter a user’s authorization after authentication when you use a Cisco ISE RADIUS server. We added attributes to the RADIUS server and server group objects, and made it possible to select a RADIUS server group within an RA VPN connection profile.
Multiple connection profiles and group policies for remote access VPN.	You can configure more than one connection profile, and create group policies to use with the profiles. We changed the **Device** > **Remote Access VPN** page to have separate pages for connection profiles and group policies, and updated the RA VPN Connection wizard to allow the selection of group policies. Some items that were previously configured in the wizard are now configured in the group policy.
Support for certificate-based, second authentication source, and two-factor authentication in remote access VPN.	You can use certificates for user authentication, and configure secondary authentication sources so that users must authenticate twice before establishing a connection. You can also configure two-factor authentication using RSA tokens or Duo passcodes as the second factor. We updated the RA VPN Connection wizard to support the configuration of these additional options.
Support for IP address pools with multiple address ranges, and DHCP address pools, for remote access VPN.	You can now configure address pools that have more than one address range by selecting multiple network objects that specify subnets. In addition, you can configure address pools in a DHCP server and use the server to provide addresses to RA VPN clients. If you use RADIUS for authorization, you can alternatively configure the address pools in the RADIUS server. We updated the RA VPN Connection wizard to support the configuration of these additional options. You can optionally configure the address pool in the group policy instead of the connection profile.

Feature	Description
Active Directory realm enhancements.	You can now include up to 10 redundant Active Directory (AD) servers in a single realm. You can also create multiple realms and delete realms that you no longer need. In addition, the limit for downloading users in a realm is increased to 50,000 from the 2,000 limit in previous releases. We updated the **Objects** > **Identity Sources** page to support multiple realms and servers. You can select the realm in the user criteria of access control and SSL decryption rules, to apply the rule to all users within the realm. You can also select the realm in identity rules and RA VPN connection profiles.
Redundancy support for ISE servers.	When you configure Cisco Identity Services Engine (ISE) as an identity source for passive authentication, you can now configure a secondary ISE server if you have an ISE high availability setup. We added an attribute for the secondary server to the ISE identity object.
File/malware events sent to external syslog servers.	You can now configure an external syslog server to receive file/malware events, which are generated by file policies configured on access control rules. File events use message ID 430004, malware events are 430005. We added the File/Malware syslog server options to the **Device** > **System Settings** > **Logging Settings** page.
Logging to the internal buffer and support for custom event log filters.	You can now configure the internal buffer as a destination for system logging. In addition, you can create event log filters to customize which messages are generated for the syslog server and internal buffer logging destinations. We added the Event Log Filter object to the **Objects** page, and the ability to use the object on the **Device** > **System Settings** > **Logging Settings** page. The internal buffer options were also added to the **Logging Settings** page.
Certificate for the FDM Web Server.	You can now configure the certificate that is used for HTTPS connections to the FDM configuration interface. By uploading a certificate your web browsers already trust, you can avoid the Untrusted Authority message you get when using the default internal certificate. We added the **Device** > **System Settings** > **Management Access** > **Management Web Server** page.
Cisco Threat Response support.	You can configure the system to send intrusion events to the Cisco Threat Response cloud-based application. You can use Cisco Threat Response to analyze intrusions. We added Cisco Threat Response to the **Device** > **System Settings** > **Cloud Services** page.

Feature	Description
Manually upload VDB, GeoDB, and SRU updates.	You can now manually retrieve update packages for VDB, Geolocation Database, and Intrusion Rules, and then upload them from your workstation to the FTD device using FDM. For example, if you have an air-gapped network, where FDM cannot retrieve updates from the Cisco Cloud, you can now get the update packages you need. We updated the **Device** > **Updates** page to allow you to select and upload a file from your workstation. Minimum FTD: 6.4.0.10. Version restrictions: This feature is not available in Version 6.5. Support returns in Version 6.6.
Smaller VDB for lower memory devices devices.	For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Minimum FTD: 6.4.0.17 Lower memory devices: ASA-5508-X, ASA-5515-X, ASA-5516-X, ASA-5525-X, ASA-5545-X Version restrictions: The smaller VDB is not supported in all versions. If you upgrade from a supported version to an unsupported version, you cannot install VDB 363+ on lower memory devices. For a list of affected releases, see CSCwd88641.
Universal Permanent License Reservation (PLR) mode.	If you have an air-gapped network, where there is no path to the internet, you cannot register directly with the Cisco Smart Software Manager (CSSM) for Smart Licensing. In this situation, you can now get authorization to use Universal Permanent License Reservation (PLR) mode, where you can apply a license that does not need direct communication with CSSM. If you have an air-gapped network, please contact your account representative and ask for authorization to use Universal PLR mode in your CSSM account, and to obtain the necessary licenses. We added the ability to switch to PLR mode, and to cancel and unregister a Universal PLR license, to the **Device** > **Smart License** page. In the FTD API, there are new resources for PLRAuthorizationCode, PLRCode, PLRReleaseCode, PLRRequestCode, and actions for PLRRequestCode, InstallPLRCode, and CancelReservation. Minimum FTD: 6.4.0.10. This feature is temporarily deprecated in Version 6.5 and returns in Version 6.6. If you are running Version 6.4.0.10 or later patch, we recommend you upgrade directly to Version 6.6+.

Feature	Description
Default HTTPS server certificates.	**Upgrade impact.** Patching may renew the device's current *default* HTTPS server certificate. Your certificate is set to expire depending on when it is generated, as follows: • 6.5.0.5+: 800 days • 6.5.0 to 6.5.0.4: 3 years • 6.4.0.9 and later patches: 800 days • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3: 20 years
New syslog fields.	These new syslog fields collectively identify a unique connection event: • Sensor UUID • First Packet Time • Connection Instance ID • Connection Counter These fields also appear in syslogs for intrusion, file, and malware events, allowing connection events to be associated with those events. Minimum FTD: 6.4.0.4
FTD REST API version 3 (v3).	The Firepower Threat Defense REST API for software version 6.4 has been incremented to version 3. You must replace v1/v2 in the API URLs with v3. The v3 API includes many new resources that cover all features added in software version 6.4. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, change the end of the FDM URL to **/#/api-explorer** after logging in.

CHAPTER 4

Upgrade Guidelines

This document provides critical and release-specific upgrade guidelines for Version 6.4.

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the appropriate upgrade or configuration guide: http://www.cisco.com/go/threatdefense-64-docs.

Table 12: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Backups	Back up configurations and events. Back up FXOS on the Firepower 4100/9300. Back up ASA for ASA FirePOWER.

Planning Phase	Includes
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade firmware on the Firepower 4100/9300. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA for ASA FirePOWER.
Final Checks	Check configurations. Check NTP synchronization. Deploy configurations. Run readiness checks. Check disk space. Check running tasks. Check deployment health and communications.

Minimum Version to Upgrade

Minimum Version to Upgrade

You can upgrade directly to Version 6.4 as follows.

Table 13: Minimum Version to Upgrade to Version 6.4

Platform	Minimum Version
FMC	6.1
FTD (except Firepower 4100/9300)	6.1 with FMC 6.2 with FDM FXOS 2.6.1.157 is required for the Firepower 4100/9300. In most cases, we recommend you use the latest FXOS build in each major version. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes, 2.6(1).
FTD for the Firepower 4100/9300	6.2
Firepower 7000/8000 series	6.1

Platform	Minimum Version
ASA with FirePOWER Services	6.1 with FMC 6.2 with ASDM See Device Platforms, on page 8 for ASA requirements for your model. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues. To help you decide, see the Cisco Secure Firewall ASA Release Notes.
NGIPSv	6.1

Minimum Version to Patch

Patches change the fourth digit *only*. You cannot upgrade directly to a patch from a previous major or maintenance release.

Upgrade Guidelines for Version 6.4

These checklists provide new and/or previously published upgrade guidelines that may apply to you.

Table 14: Upgrade Guidelines for FTD with FMC Version 6.4

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 32	Any	Any	Any
	Cisco Secure Firewall Management Center New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	Bugs, on page 57, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 43	Firepower 4100/9300	Any	Any
	Patches That Support Uninstall	Any	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Caution: Firepower 7000/8000 Series to Version 6.4.0.9–6.4.0.11, on page 36	Firepower 7000/8000 series	6.4.0 through 6.4.0.10	6.4.0.9 through 6.4.0.11
	EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic, on page 36	Firepower 1010	6.4.0 only	6.4.0.3 through 6.4.0.5
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 36	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4+
	Upgrade Failure: NGIPS Devices Previously at Version 6.2.3.12, on page 37	Firepower 7000/8000 series ASA FirePOWER NGIPSv	6.2.3 through 6.3.0.x	6.4.0 only
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 37	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0
	Renamed Upgrade and Installation Packages, on page 37	FMC Firepower 7000/8000 series NGIPSv	Any	6.3+
	Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 38	FMC Firepower 7000/8000 series NGIPSv	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 39	FTD	6.2.0 through 6.2.3.x	6.3+
	Security Intelligence Enables Application Identification, on page 39	FMC deployments	6.1.0 through 6.2.3.x	6.3+
	Update VDB after Upgrade to Enable CIP Detection, on page 40	Any	6.1.0 through 6.2.3.x	6.3+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 40	Any	6.1.0 through 6.2.3.x	6.3+

✓	Guideline	Platforms	Upgrading From	Directly To
	Remove Site IDs from Version 6.1.x Firepower Threat Defense Clusters Before Upgrade, on page 41	FTD clusters	6.1.0.x	6.2.3+
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 42	FMC	6.1.0.x	6.2+
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 42	FTD	6.1.0.x	6.2+

Table 15: Upgrade Guidelines for FTD with FDM Version 6.4

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 32	Any	Any	Any
	Cisco Secure Firewall Device Manager New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	Bugs, on page 57, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 43	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic, on page 36	Firepower 1010	6.4.0 only	6.4.0.3 through 6.4.0.5
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 36	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4+
	Update VDB after Upgrade to Enable CIP Detection, on page 40	Any	6.1.0 through 6.2.3.x	6.3+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 40	Any	6.1.0 through 6.2.3.x	6.3+

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Can Unregister FDM from CSSM, on page 41	Any	6.2.0 through 6.2.2.x	6.2.3+
	Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 41	Any	6.2.0 only	6.2.2+

Upgrade Caution: Firepower 7000/8000 Series to Version 6.4.0.9–6.4.0.11

Deployments: Firepower 7000/8000 series

Upgrading From: Version 6.4.0 through 6.4.0.10

Directly To: Version 6.4.0.9 through 6.4.0.11

Related Bug: CSCvw01028

If your Firepower 7000/8000 series device *ever* ran a version older than Version 6.4.0, do not upgrade to Version 6.4.0.9, 6.4.0.10, or 6.4.0.11. Otherwise, your device may become unresponsive and you will be forced to reimage. Instead, upgrade to Version 6.4.0.12+.

If you are already running one of the affected versions and you are vulnerable to this issue, you should contact Cisco TAC for a hotfix, then upgrade to Version 6.4.0.12 as soon as possible. You can also reimage and upgrade.

EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic

Deployments: Firepower 1010 with FTD

Affected Versions: Version 6.4.0 to 6.4.0.5

Related Bug: CSCvq81354

We *strongly* recommend you do not configure EtherChannels on Firepower 1010 devices running FTD Version 6.4.0 to Version 6.4.0.5. (Note that Versions 6.4.0.1 and 6.4.0.2 are not supported on this model.)

Due to an internal traffic hashing issue, some EtherChannels on Firepower 1010 devices may blackhole some egress traffic. The hashing is based on source/destination IP address so the behavior will be consistent for a given source/destination IP pair. That is, some traffic consistently works and some consistently fails.

This issue is fixed in Version 6.4.0.6 and Version 6.5.0.

TLS Crypto Acceleration Enabled/Cannot Disable

Deployments: Firepower 2100 series, Firepower 4100/9300 chassis

Upgrading from: Version 6.1.0 through 6.3.x

Directly to: Version 6.4.0+

SSL hardware acceleration has been renamed *TLS crypto acceleration*.

Depending on the device, TLS crypto acceleration might be performed in software or in hardware. The upgrade automatically enables acceleration on all eligible devices, even if you previously disabled the feature manually. In most cases you cannot configure this feature; it is automatically enabled and you cannot disable it.

Upgrading to Version 6.4.0: If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for *one* container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances.

Upgrading to Version 6.5.0+: If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for multiple container instances (up to 16) on a Firepower 4100/9300 chassis. New instances have this feature enabled by default. However, the upgrade does *not* enable acceleration on existing instances. Instead, use the **config hwCrypto enable** CLI command.

Upgrade Failure: NGIPS Devices Previously at Version 6.2.3.12

Deployments: 7000/8000 series, ASA FirePOWER, NGIPSv

Related bug: CSCvp42398

Upgrading from: Version 6.2.3 through 6.3.0.x

Directly to: Version 6.4.0 only

You cannot upgrade an NGIPS device to Version 6.4.0 if:

- The device previously ran Version 6.2.3.12, and then
- You uninstalled the Version 6.2.3.12 patch, or upgraded to Version 6.3.0.x.

  This also includes scenarios where you uninstalled the Version 6.2.3.12 patch *and then* upgraded to Version 6.3.0.x.

If this is your current situation, contact Cisco TAC.

Upgrade Failure: Insufficient Disk Space on Container Instances

Deployments: Firepower 4100/9300 with FTD

Upgrading from: Version 6.3.0 through 6.4.0.x

Directly to: Version 6.3.0.1 through Version 6.5.0

Most often during major upgrades — but possible while patching — FTD devices configured with container instances can fail in the precheck stage with an erroneous insufficient-disk-space warning.

If this happens to you, you can try to free up more disk space. If that does not work, contact Cisco TAC.

Renamed Upgrade and Installation Packages

Deployments: FMC, 7000/8000 series, NGIPSv

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3+

The naming scheme (that is, the first part of the name) for upgrade, patch, hotfix, and installation packages changed starting with Version 6.3.0, on select platforms.

Note This change causes issues with reimaging older *physical* appliances: DC750, 1500, 2000, 3500, and 4000, as well as 7000/8000 series devices and AMP models. If you are currently running Version 5.x and need to freshly install Version 6.3.0 or 6.4.0 on one of these appliances, rename the installation package to the "old" name after you download it from the Cisco Support & Download site.

Table 16: Naming Schemes: Upgrade, Patch, and Hotfix Packages

Platform	Naming Schemes
FMC	**New:** Cisco_Firepower_Mgmt_Center **Old:** Sourcefire_3D_Defense_Center_S3
Firepower 7000/8000 series	**New:** Cisco_Firepower_NGIPS_Appliance **Old:** Sourcefire_3D_Device_S3
NGIPSv	**New:** Cisco_Firepower_NGIPS_Virtual **Old:** Sourcefire_3D_Device_VMware **Old:** Sourcefire_3D_Device_Virtual64_VMware

Table 17: Naming Schemes: Installation Packages

Platform	Naming Schemes
FMC (physical)	**New:** Cisco_Firepower_Mgmt_Center **Old:** Sourcefire_Defense_Center_M4 **Old:** Sourcefire_Defense_Center_S3
FMCv: VMware	**New:** Cisco_Firepower_Mgmt_Center_Virtual_VMware **Old:** Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	**New:** Cisco_Firepower_Mgmt_Center_Virtual_KVM **Old:** Cisco_Firepower_Management_Center_Virtual
Firepower 7000/8000 series	**New:** Cisco_Firepower_NGIPS_Appliance **Old:** Sourcefire_3D_Device_S3
NGIPSv	**New:** Cisco_Firepower_NGIPSv_VMware **Old:** Cisco_Firepower_NGIPS_VMware

Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv

Deployments: FMC, 7000/8000 series devices, NGIPSv

Upgrading from: Version 6.1.0 through 6.1.0.6, Version 6.2.0 through 6.2.0.6, Version 6.2.1, Version 6.2.2 through 6.2.2.4, and Version 6.2.3 through 6.2.3.4

Directly to: Version 6.3.0+

You cannot run the readiness check on the listed models when upgrading from one of the listed Firepower versions. This occurs because the readiness check process is incompatible with newer upgrade packages.

Table 18: Patches with Readiness Checks for Version 6.3.0+

Readiness Check Not Supported	First Patch with Fix
6.1.0 through 6.1.0.6	6.1.0.7
6.2.0 through 6.2.0.6	6.2.0.7
6.2.1	None. Upgrade to Version 6.2.3.5+.
6.2.2 through 6.2.2.4	6.2.2.5
6.2.3 through 6.2.3.4	6.2.3.5

RA VPN Default Setting Change Can Block VPN Traffic

Deployments: Firepower Threat Defense configured for remote access VPN

Upgrading from: Version 6.2.x

Directly to: Version 6.3+

Version 6.3 changes the default setting for a hidden option, **sysopt connection permit-vpn**. Upgrading can cause your remote access VPN to stop passing traffic. If this happens, use either of these techniques:

- Create a FlexConfig object that configures the **sysopt connection permit-vpn** command. The new default for this command is **no sysopt connection permit-vpn**.

  This is the more secure method to allow traffic in the VPN, because external users cannot spoof IP addresses in the remote access VPN address pool. The downside is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic.

- Create access control rules to allow connections from the remote access VPN address pool.

  This method ensures that VPN traffic is inspected and advanced services can be applied to the connections. The downside is that it opens the possibility for external users to spoof IP addresses and thus gain access to your internal network.

Security Intelligence Enables Application Identification

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

In Version 6.3, Security Intelligence configurations enable application detection and identification. If you disabled discovery in your current deployment, the upgrade process may enable it again. Disabling discovery if you don't need it (for example, in an IPS-only deployment) can improve performance.

To disable discovery you must:

- Delete all rules from your network discovery policy.
- Use only simple network-based conditions to perform access control: zone, IP address, VLAN tag, and port. Do not perform any kind of application, user, URL, or geolocation control.
- **(NEW)** Disable network and URL-based Security Intelligence by deleting all whitelists and blacklists from your access control policy's Security Intelligence configuration, including the default Global lists.
- **(NEW)** Disable DNS-based Security Intelligence by deleting or disabling all rules in the associated DNS policy, including the default Global Whitelist for DNS and Global Blacklist for DNS rules.

Update VDB after Upgrade to Enable CIP Detection

Deployments: Any

Upgrading from: Version 6.1.0 through 6.2.3.x, with VDB 299+

Directly to: Version 6.3.0+

If you upgrade while using vulnerability database (VDB) 299 or later, an issue with the upgrade process prevents you from using CIP detection post-upgrade. This includes every VDB released from June 2018 to now, even the latest VDB.

Although we always recommend you update the vulnerability database (VDB) to the latest version after you upgrade, it is especially important in this case.

To check if you are affected by this issue, try to configure an access control rule with a CIP-based application condition. If you cannot find any CIP applications in the rule editor, manually update the VDB.

Invalid Intrusion Variable Sets Can Cause Deploy Failure

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0+

For network variables in an intrusion variable set, any IP addresses you *exclude* must be a subset of the IP addresses you *include*. This table shows you examples of valid and invalid configurations.

Valid	Invalid
Include: 10.0.0.0/8 Exclude: 10.1.0.0/16	Include: 10.1.0.0/16 Exclude: 172.16.0.0/12 Exclude: 10.0.0.0/8

Before Version 6.3.0, you could successfully save a network variable with this type of invalid configuration. Now, these configurations block deploy with the error: `Variable set has invalid excluded values`.

If this happens, identify and edit the incorrectly configured variable set, then redeploy. Note that you may have to edit network objects and groups referenced by your variable set.

Remove Site IDs from Version 6.1.x Firepower Threat Defense Clusters Before Upgrade

Deployments: Firepower Threat Defense clusters

Upgrading from: Version 6.1.x

Directly to: Version 6.2.3 through 6.4.0

Firepower Threat Defense Version 6.1.x clusters do not support inter-site clustering (you can configure inter-site features using FlexConfig starting in Version 6.2.0).

If you deployed or redeployed a Version 6.1.x cluster in FXOS 2.1.1, and you entered a value for the (unsupported) site ID, remove the site ID (set to `0`) on each unit in FXOS before you upgrade. Otherwise, the units cannot rejoin the cluster after the upgrade.

If you already upgraded, remove the site ID from each unit, then reestablish the cluster. To view or change the site ID, see the Cisco FXOS CLI Configuration Guide.

Upgrade Can Unregister FDM from CSSM

Deployments: FTD with FDM

Upgrading from: Version 6.2 through 6.2.2.x

Directly to: Version 6.2.3 through 6.4.0

Note Upgrades from 6.2.3 and 6.2.3.1 directly to 6.2.3.2 through 6.2.3.5 are also affected.

Upgrading FTD with FDM may unregister the device from the Cisco Smart Software Manager. After the upgrade completes, check your license status.

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 If the device is not registered, click **Register Device**.

Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0

Deployments: FTD with FDM, running on a lower-memory ASA 5500-X series device

Upgrading from: Version 6.2.0

Directly to: Version 6.2.2 through 6.4.0

If you are upgrading from Version 6.2.0, the upgrade may fail with an error of: `Uploaded file is not a valid system upgrade file`. This can occur even if you are using the correct file.

If this happens, you can try the following workarounds:

- Try again.
- Use the CLI to upgrade.

- Upgrade to 6.2.0.1 first.

Access Control Can Get Latency-Based Performance Settings from SRUs

Deployments: FMC

Upgrading from: 6.1.x

Directly to: 6.2.0+

New access control policies in Version 6.2.0+ *by default* get their latency-based performance settings from the latest intrusion rule update (SRU). This behavior is controlled by a new **Apply Settings From** option. To configure this option, edit or create an access control policy, click **Advanced**, and edit the Latency-Based Performance Settings.

When you upgrade to Version 6.2.0+, the new option is set according to your current (Version 6.1.x) configuration. If your current settings are:

- Default: The new option is set to **Installed Rule Update**. When you deploy after the upgrade, the system uses the latency-based performance settings from the latest SRU. It is possible that traffic handling could change, depending on what the latest SRU specifies.
- Custom: The new option is set to **Custom**. The system retains its current performance settings. There should be no behavior change due to this option.

We recommend you review your configurations before you upgrade. From the Version 6.1.x FMC web interface, view your policies' Latency-Based Performance Settings as described earlier, and see whether the **Revert to Defaults** button is dimmed. If the button is dimmed, you are using the default settings. If it is active, you have configured custom settings.

'Snort Fail Open' Replaces 'Failsafe' on FTD

Deployments: FTD with FMC

Upgrading from: Version 6.1.x

Directly to: Version 6.2+

In Version 6.2, the Snort Fail Open configuration replaces the Failsafe option on FMC-managed Firepower Threat Defense devices. While Failsafe allows you to drop traffic when Snort is busy, traffic automatically passes without inspection when Snort is down. Snort Fail Open allows you to drop this traffic.

When you upgrade an FTD device, its new Snort Fail Open setting depends on its old Failsafe setting, as follows. Although the new configuration should not change traffic handling, we still recommend that you consider whether to enable or disable Failsafe before you upgrade.

Table 19: Migrating Failsafe to Snort Fail Open

Version 6.1 Failsafe	Version 6.2 Snort Fail Open	Behavior
Disabled (default behavior)	**Busy**: Disabled **Down**: Enabled	New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down.

Version 6.1 Failsafe	Version 6.2 Snort Fail Open	Behavior
Enabled	**Busy**: Enabled **Down**: Enabled	New and existing connections pass without inspection when the Snort process is busy or down.

Note that Snort Fail Open requires Version 6.2 on the device. If you are managing a Version 6.1.x device, the FMC web interface displays the Failsafe option.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

For the Firepower 4100/9300, major FTD upgrades also require a chassis upgrade (FXOS and firmware). Maintenance release and patches rarely require this, but you may still want to upgrade to the latest build to take advantage of resolved issues.

Table 20: Upgrade Guidelines for the Firepower 4100/9300 Chassis

Guideline	Details
FXOS upgrades.	FXOS 2.6.1.157+ is required to run threat defense Version 6.4 on the Firepower 4100/9300. You can upgrade to any later FXOS version from as far back as FXOS 2.2.2. For critical and release-specific upgrade guidelines, new and deprecated features, and open and resolved bugs, see the Cisco Firepower 4100/9300 FXOS Release Notes.
Firmware upgrades.	FXOS 2.14.1+ upgrades include firmware. If you are upgrading to an earlier FXOS version, see the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
Time to upgrade.	Chassis upgrade can take up to 45 minutes and can affect traffic flow and inspection. For more information, see Traffic Flow and Inspection for Chassis Upgrades, on page 46.

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down during upgrade. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Uninstall a Patch

In FMC and ASDM deployments, you can uninstall most patches. If you need to return to an earlier major release, you must reimage. For guidelines, limitations, and procedures, see Uninstall a Patch in the FMC upgrade guide or Uninstall ASA FirePOWER Patches with ASDM, on page 44 in these release notes.

Uninstall ASA FirePOWER Patches with ASDM

Use the Linux shell (*expert mode*) to uninstall device patches. You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. If you disabled shell access, contact Cisco TAC to reverse the lockdown.

For ASA failover pairs and clusters, minimize disruption by uninstalling from one appliance at a time. Wait until the patch has fully uninstalled from one unit before you move on to the next.

Table 21: Uninstall Order for ASA with FirePOWER Services in ASA Failover Pairs/Clusters

Configuration	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	Always uninstall from the standby. **1.** Uninstall from the ASA FirePOWER module on the standby ASA device. **2.** Fail over. **3.** Uninstall from the ASA FirePOWER module on the new standby ASA device.
ASA active/active failover pair, with ASA FirePOWER	Make both failover groups active on the unit you are not uninstalling. **1.** Make both failover groups active on the primary ASA device. **2.** Uninstall from the ASA FirePOWER module on the secondary ASA device. **3.** Make both failover groups active on the secondary ASA device. **4.** Uninstall from the ASA FirePOWER module on the primary ASA device.
ASA cluster, with ASA FirePOWER	Disable clustering on each unit before you uninstall. Uninstall from one unit at a time, leaving the control unit for last. **1.** On a data unit, disable clustering. **2.** Uninstall from the ASA FirePOWER module on that unit. **3.** Reenable clustering. Wait for the unit to rejoin the cluster. **4.** Repeat for each data unit. **5.** On the control unit, disable clustering. Wait for a new control unit to take over. **6.** Uninstall from the ASA FirePOWER module on the former control unit. **7.** Reenable clustering.

⚠

Caution Do not make or deploy configuration changes during uninstall. Even if the system appears inactive, do not manually reboot, shut down, or restart an uninstall in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

Before you begin

- In ASA failover/cluster deployments, make sure you are uninstalling from the correct device.
- Make sure your deployment is healthy and successfully communicating.

Step 1 If the device's configurations are out of date, deploy now from ASDM.

Deploying before you uninstall reduces the chance of failure. Make sure the deployment and other essential tasks are completed. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

Step 2 Access the Firepower CLI on the ASA FirePOWER module. Log in as `admin` or another Firepower CLI user with configuration access.

You can either SSH to the module's management interface (hostname or IP address) or use the console. Note that the console port defaults to the ASA CLI and you must use the `session sfr` command to access the Firepower CLI.

Step 3 Use the `expert` command to access the Linux shell.

Step 4 Verify the uninstall package is in the upgrade directory.

```
ls /var/sf/updates
```

Patch uninstallers are named like upgrade packages, but have `Patch_Uninstaller` instead of `Patch` in the file name. When you patch a device, the uninstaller for that patch is automatically created in the upgrade directory. If the uninstaller is not there, contact Cisco TAC.

Step 5 Run the uninstall command, entering your password when prompted.

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

Caution The system does *not* ask you to confirm. Entering this command starts the uninstall, which includes a device reboot. Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. Make sure you are ready. Note that using the `--detach` option ensures the uninstall process is not killed if your SSH session times out, which can leave the device in an unstable state.

Step 6 Monitor the uninstall until you are logged out.

For a detached uninstall, use `tail` or `tailf` to display logs:

```
tail /ngfw/var/log/sf/update.status
```

Otherwise, monitor progress in the console or terminal.

Step 7 Verify uninstall success.

After the uninstall completes, confirm that the module has the correct software version. Choose **Configuration** > **ASA FirePOWER Configurations** > **Device Management** > **Device**.

Step 8 Redeploy configurations.

What to do next

In ASA failover/cluster deployments, repeat this procedure for each unit in your planned sequence.

Traffic Flow and Inspection

Device upgrades (software and operating system) affect traffic flow and inspection. Schedule maintenance windows when this will have the least impact.

Traffic Flow and Inspection for Chassis Upgrades

Upgrading FXOS reboots the chassis. For FXOS upgrades to Version 2.14.1+ that include firmware upgrades, the device reboots twice—once for FXOS and once for the firmware.

Even in high availability/clustered deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade one chassis at a time.

Table 22: Traffic Flow and Inspection: FXOS Upgrades

FTD Deployment	Traffic Behavior	Method
Standalone	Dropped.	—
High availability	Unaffected.	**Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby.
	Dropped until one peer is online.	Upgrade FXOS on the active peer before the standby is finished upgrading.
Inter-chassis cluster	Unaffected.	**Best Practice:** Upgrade one chassis at a time so at least one module is always online.
	Dropped until at least one module is online.	Upgrade chassis at the same time, so all modules are down at some point.
Intra-chassis cluster (Firepower 9300 only)	Passed without inspection.	Hardware bypass enabled: **Bypass: Standby** or **Bypass-Force**.
	Dropped until at least one module is online.	Hardware bypass disabled: **Bypass: Disabled**.
	Dropped until at least one module is online.	No hardware bypass module.

Traffic Flow and Inspection for FTD Upgrades with FMC

Software Upgrades for Standalone Devices

Devices operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

Table 23: Traffic Flow and Inspection: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped. For bridge group interfaces on the ISA 3000 only, you can use a FlexConfig policy to configure hardware bypass for power failure. This causes traffic to drop during software upgrades but pass without inspection while the device completes its post-upgrade reboot.
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force**	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby**	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled**	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability or clustered devices. For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.

For clusters, the data security module or modules upgrade first, then the control module. During the control security module upgrade, although traffic inspection and handling continues normally, the system stops logging events. Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the upgrade is completed. However, if the logging downtime is significant, the system may prune the oldest events before they can be logged.

Note Upgrading an inter-chassis cluster from Version 6.2.0, 6.2.0.1, or 6.2.0.2 causes a 2-3 second traffic interruption in traffic inspection when each module is removed from the cluster. Upgrading high availability or clustered devices from Version 6.0.1 through 6.2.2.x may have additional upgrade path requirements; see the upgrade path information in the planning chapter of the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Software Uninstall (Patches)

For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Table 24: Traffic Flow and Inspection: Deploying Configuration Changes

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled.	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled.	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled.	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Traffic Flow and Inspection for FTD Upgrades with FDM

Software Upgrades

Traffic is dropped while you upgrade. In a high availability deployment, you can minimize disruption by upgrading devices one at a time.

For the ISA 3000 only, if you configured hardware bypass for power failure, traffic is dropped during the upgrade but is passed without inspection while the device completes its post-upgrade reboot.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Traffic Flow and Inspection for ASA FirePOWER Upgrades

Software Upgrades

Your ASA service policies for redirecting traffic to the ASA FirePOWER module determine how the module handles traffic during software upgrade.

Table 25: Traffic Flow and Inspection: ASA FirePOWER Upgrades

Traffic Redirection Policy	Traffic Behavior
Fail open (**sfr fail-open**)	Passed without inspection
Fail closed (**sfr fail-close**)	Dropped
Monitor only (**sfr {fail-close}|{fail-open} monitor-only**)	Egress packet immediately, copy not inspected

Software Uninstall (Patches)

Interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In ASA failover/cluster deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection. Traffic behavior while the Snort process restarts is the same as when you upgrade ASA FirePOWER. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Traffic Flow and Inspection for NGIPSv Upgrades with FMC

Software Upgrades

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 26: Traffic Flow and Inspection: NGIPSv Upgrades

Interface Configuration	Traffic Behavior
Inline	Dropped.
Inline, tap mode	Egress packet immediately, copy not inspected.
Passive	Uninterrupted, not inspected.

Software Uninstall (Patches)

Interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection. Interface configurations determine whether traffic drops or passes without inspection during the interruption. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Table 27: Traffic Flow and Inspection: Deploying Configuration Changes

Interface Configuration	Traffic Behavior
Inline, **Failsafe** enabled or disabled	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
Inline, tap mode	Egress packet immediately, copy bypasses Snort
Passive	Uninterrupted, not inspected.

Time and Disk Space

Time to Upgrade

We recommend you track and record your own upgrade times so you can use them as future benchmarks. The following table lists some things that can affect upgrade time.

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, you can find troubleshooting information in the upgrade guide: https://www.cisco.com/go/ftd-upgrade. If you continue to have issues, contact Cisco TAC.

Table 28: Upgrade Time Considerations

Consideration	Details
Versions	Upgrade time usually increases if your upgrade skips versions.
Models	Upgrade time usually increases with lower-end models.
Virtual appliances	Upgrade time in virtual deployments is highly hardware dependent.
High availability and clustering	In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device.
Configurations	Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how they are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.
Components	You may need additional time to perform operating system or virtual hosting upgrades, upgrade package transfers, readiness checks, VDB and intrusion rule (SRU/LSP) updates, configuration deployment, and other related tasks.

Disk Space to Upgrade

To upgrade, the upgrade package must be on the appliance. For device upgrades with management center, you must also have enough space on the management center (in either /Volume or /var) for the device upgrade package. Or, you can use an internal server to store them. Readiness checks should indicate whether you have enough disk space to perform the upgrade. Without enough free disk space, the upgrade fails.

Table 29: Checking Disk Space

Platform	Command
Management center	Choose **System** (⚙) > **Monitoring** > **Statistics** and select the FMC. Under Disk Usage, expand the By Partition details.
Threat defense with management center	Choose **System** (⚙) > **Monitoring** > **Statistics** and select the device you want to check. Under Disk Usage, expand the By Partition details.
Threat defense with device manager	Use the **show disk** CLI command.

CHAPTER 5

Install the Software

If you cannot or do not want to upgrade to Version 6.4, you can freshly install major releases. This is also called *reimaging*. We do not provide installation packages for patches. To run a particular patch, install the appropriate major release, then apply the patch.

Installation Guidelines

These guidelines can prevent common reimage issues, but are not comprehensive. For detailed checklists and procedures, see the appropriate installation guide.

Reimaging Version 5.x Hardware to Version 6.3+

The renamed installation packages in Version 6.3+ cause issues with reimaging older hardware: FMC 750, 1500, 2000, 3500, and 4000, as well as 7000/8000 series devices and AMP models. If you are currently running Version 5.x and want to reimage to Version 6.4, rename the installation package to the "old" name after you download it.

After you reimage an FMC (Defense Center) from Version 5.x to a more recent version, it cannot manage its older devices. You should also reimage those devices, then re-add them to the FMC. Note that Series 2 devices are EOL and cannot run Firepower software past Version 5.4.0.x. You must replace them.

Backups

Before you reimage, we *strongly* recommend you back up to a secure remote location and verify transfer success. Reimaging returns most settings to factory defaults, including the system password. It deletes any backups left on the appliance.

Note If you want to reimage so that you don't have to upgrade, due to version restrictions you cannot use a backup to import your old configurations. You must recreate your configurations manually.

Appliance Access

If you do not have physical access to an appliance, reimaging to the current major or maintenance release lets you keep management network settings. This allows you to connect to the appliance after you reimage to perform the initial configuration. Note that if you delete network settings or if you reimage to an earlier release, you must have physical access to the appliance. You cannot use Lights-Out Management (LOM).

For devices, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC's management interface without traversing the device.

Unregistering from Smart Software Manager

Before you reimage any appliance or switch device management, you may need to unregister from the Cisco Smart Software Manager (CSSM). This is to avoid accruing orphan entitlements, which can prevent you from reregistering.

Unregistering removes an appliance from your virtual account, unregisters it from the cloud and cloud services, and releases associated licenses so they can be can be reassigned. When you unregister an appliance, it enters Enforcement mode. Its current configuration and policies continue to work as-is, but you cannot make or deploy any changes.

If you plan to restore from backup, do not unregister before you reimage and do not remove devices from the FMC. Instead, manually revert any licensing changes made since you took the backup. After the restore completes, reconfigure licensing. If you notice licensing conflicts or orphan entitlements, contact Cisco TAC.

Table 30: Scenarios for Unregistering from CSSM (Not Restoring from Backup)

Scenario	Action
Reimage the FMC.	Unregister manually.
Model migration for the FMC.	Unregister manually, before you shut down the source FMC.
Reimage FTD with FMC.	Unregister automatically, by removing the device from the FMC.
Reimage FTD with FDM.	Unregister manually.
Switch FTD from FMC to FDM.	Unregister automatically, by removing the device from the FMC.
Switch FTD from device manager to FMC.	Unregister manually.

Removing Devices from the FMC

In FMC deployments, if you plan to manually configure the reimaged appliance, remove devices from the FMC before you reimage either. If you plan to restore from backup, you do not need to do this.

Table 31: Scenarios for Removing Devices from the FMC (Not Restoring from Backup)

Scenario	Action
Reimage the FMC.	Remove all devices from management.

Scenario	Action
Reimage FTD.	Remove the one device from management.
Switch FTD from FMC to FDM.	Remove the one device from management.

Fully Reimaging FTD Hardware to Downgrade FXOS

For FTD hardware models that use the FXOS operating system, reimaging to an earlier software version may require a full reimage, regardless of whether FXOS is bundled with the software or upgraded separately.

Table 32: Scenarios for Full Reimages

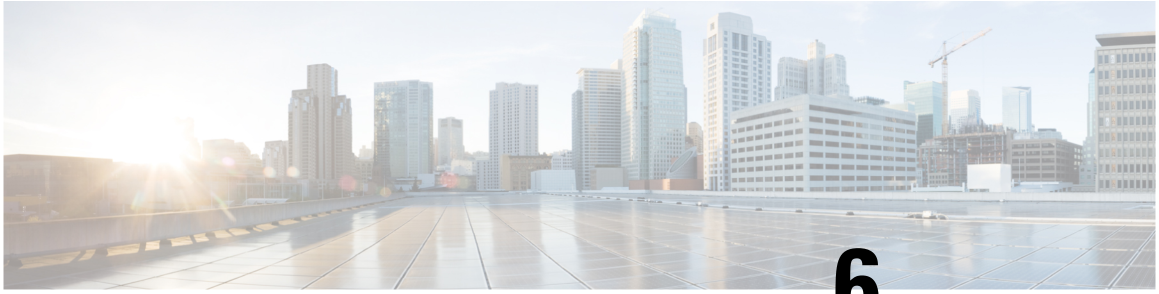
Model	Details
Firepower 1000 series Firepower 2100 series	If you use the **erase configuration** method to reimage, FXOS may not downgrade along with the software. This can cause failures, especially in high availability deployments. We recommend that you perform full reimages of these devices.
Firepower 4100/9300	Reverting FTD does not downgrade FXOS. For the Firepower 4100/9300, major FTD versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of FTD, you may be running a non-recommended version of FXOS (too new). Although newer versions of FXOS are backwards compatible with older FTD versions, we do perform enhanced testing for the recommended combinations. You cannot manually downgrade FXOS, so if you find yourself in this situation and you want to run a recommended combination, you will need a full reimage.

Installation Guides

Table 33: Installation Guides

Platform	Guide
FMC	
FMC 1600, 2600, 4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
FMC 1000, 2500, 4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMC 750, 1500, 2000, 3500, 4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
FMCv	Cisco Secure Firewall Management Center Virtual Getting Started Guide
FTD	

Platform	Guide
Firepower 1000/2100 series	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense
Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Configuration Guides: *Image Management* chapters Cisco Firepower 4100 Getting Started Guide Cisco Firepower 9300 Getting Started Guide
ASA 5500-X series	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide
ISA 3000	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide
FTDv	Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
ASA FirePOWER/NGIPSv	
Firepower 7000/8000 series	Cisco Firepower 7000 Series Getting Started Guide Cisco Firepower 8000 Series Getting Started Guide
ASA FirePOWER	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware



CHAPTER 6

Bugs

This document lists open and resolved bugs for threat defense and management center Version 6.4. For bugs in earlier releases, see the release notes for those versions. For cloud-delivered Firewall Management Center bugs, see the Cisco Cloud-Delivered Firewall Management Center Release Notes.

Important We do not list open bugs for patches.

Bug lists are auto-generated once and may not be subsequently updated. If updated, the 'table last updated' date does not mean that the list was fully accurate on that date—only that some change was made. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool.

Open Bugs

Open Bugs in Version 6.4.0

Table last updated: 2022-11-02

Table 34: Open Bugs in Version 6.4.0

Bug ID	Headline
CSCvo00852	Lina CPU is low and traffic gets lost for FTDv ESXi 12 core and FTDv KVM 12 core platforms
CSCvo03589	App agent heart beat can miss in MI scenario
CSCvo40478	FMC Dashboard is showing incorrect value as FMC latest product updates
CSCvo80725	vFTD 6.4 fails to establish OSPF adjacency due to "ERROR: ip_multicast_ctl failed to get channel"

Bug ID	Headline
CSCvp06568	NAP policy/SSL policy name name unknown in syslog on 6.3 FTD managed by 6.4 FMC
CSCvp19669	Users not showing correctly in FDM Events
CSCvp21403	Validation: Data Plane - Management Access does not handle RA-VPN port collission
CSCvp23703	first boot script S97compress-client-resources failed in FTD quietly.
CSCvp25570	Unable to create RAVPN Conn-Profile if group-policy attr and FQDN are edited in the same wizard flow
CSCvp29817	Fail to update login history when converting TempID to RealID. 1x log per ID, history lost
CSCvp30194	ASA SFR: seeing "Error importing SFO: Unable to load container" while trying to import ACP with IPS
CSCvp33797	User with sessions on FMC not properly updated after user info is downloaded from AD
CSCvp37229	few preprocessors won't be enabled if enable from 'My Changes' layer of Policy Layers
CSCvp45752	If a custom app is added in sub domain, snort doesn't restart on registered devices at older version
CSCvp47260	Generating troubleshooting files stopped in Japanese
CSCvp47535	Newly Added Application protocol are not able to view under Hosts
CSCvp48523	Access Policy doesn't reflect the modified user correctly
CSCvp48525	Unable to edit scheduled task on Task details
CSCvp48534	Unable to add categories in intrusion rule
CSCvp48545	Unable to Create Alerts with Japanese Name
CSCvp48565	VPN Troubleshooting logs setup takes abnormal time span
CSCvp56916	S2S VPN Wizard showing no pre-configured certificates available
CSCvp56951	FDM/FTDvirtual unable to support/deploy "ignore-ipsec-keyusage" flexconfig object
CSCvp57096	Upgrade to 6.4.0 may fail due to ids_event_msg_map table having NULL entries in the msg field
CSCvp59960	Network discovery not working with network groups containing literals - user or Cisco created.
CSCvq29993	6.4.0-102 2140 w/ SSL policy runs out of 1550 and 9472 blocks. doesn't recover
CSCvq33956	Optimizing memory allocation of deploy process(AQS subgroup) to allow huge policy deployments

Bug ID	Headline
CSCvq36298	Cannot change MTU size on ASAv/FTDv after upgrade
CSCvq78471	Removing a BVI and its DHCP pool simultaneiously causes policy deploy failures
CSCvr01675	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability
CSCvr35854	Apache HTTP Server URL Normalization Denial of Service Vulnerability
CSCvr35855	Apache HTTP Server mod_http2 Use-After-Free Denial of Service Vulnerab
CSCvr35856	Apache HTTP Server mod_auth_digest Race Condition Access Control Bypas
CSCvr57468	RunQuery not compatible with Java Development Kit 13
CSCvs05066	Snort file mempool corruption leads to performance degradation and process failure.
CSCvs24215	Firepower Device Manager (FDM) option to disable SSL rekey is not reflected on the config
CSCvs37065	Snort crash due to missing data in /ngfw/var/sf/fwcfg/interface_info.conf file
CSCvs50931	Policy deployment fails subsequent to SRU
CSCvs56923	SQL client not able to query FMC using external database access
CSCvs61881	Certificate mapping for AnyConnect on FTD no longer working.
CSCvs74586	Firepower FTD transparent does not decode non-ip packets
CSCvs82829	Calls fail once anyconnect configuration is added to the site to site VPN tunnel
CSCvs88186	Using same variable names between byte_extract and byte_math accross SIDs breaks snort validation
CSCvt01763	Application classification is not retried if a flow is marked brute force failed.
CSCvt03557	The time/timezone set on GUI is inconsistent on Virtual firepower management center
CSCvt06666	SFR httpsd process down after upgrade failure from 6.3.0.4 to 6.4
CSCvt16642	FMC not sending some audit messages to remote syslog server
CSCvt16723	log rotation for ngfw-onbox logs NOT happening at expected log size
CSCvt18051	RabbitMQ keeps crashing if dets file is corrupt
CSCvt20235	Firepower 4100 series all FTW interfaces link flap at the same time but occur rarely
CSCvt21986	Inconsistent allocation of cores for snort and lina between instances
CSCvt34894	Snort consumes memory causing block depletion
CSCvt35233	Excessive logging from the daq modules process_snort_verdict verdict blacklist
CSCvt35730	FDM deployment error if 2nd tunnel has overlapping crypto ACL

Bug ID	Headline
CSCvt37745	Traceback while secondary reverting from active to standby
CSCvt42955	SID 26932 false positive which triggers on QUIC traffic instead of NTP
CSCvt52607	Reduce SSL HW mode flow table memory usage to reduce the probability of Snort going in D state
CSCvt56923	FTD manual certificate enrollment fails with "&" (ampersand) in Organisation subject field
CSCvt62147	ASA traceback and reload on process name LINA
CSCvt63407	FP 2k running FTD 6.4.0.7 traceback and reload on process name LINA
CSCvt64696	AAA RADIUS server connection failure
CSCvt66136	6.4.0.9 upgrade from 6.4.0 with CC mode causes httpsd.conf to have an incorrect config
CSCvt66875	AppId caches proxy IP instead of tunneled IP for ultrasurf
CSCvt67832	FTD Traceback and Reload on Lina thread due to lock contention
CSCvt68131	FTD traceback and reload on thread "IKEv2 Mgd Timer Thread"
CSCvt70854	6.6.0-90: [Firepower 1010] Tomcat restarted during SRU update because of out of memory
CSCvt70866	sfipproxy may fail to bind listeners for secondary FMC
CSCvt72683	NAT policy configuration after NAT policy deployment on FP 8130 is not seen
CSCvt80126	ASA traceback and reload for the CLI "show asp table socket 18421590 det"
CSCvt80172	Supervisor software needs to be upgraded to address CVE-2017-11610
CSCvt86906	Stunnel 5.00 through 5.13, when using the redirect option, does not re
CSCvt87064	WebCore/platform/network/soup/SocketStreamHandleImplSoup.cpp in the li
CSCvu32449	FDM: AnyConnect "Validation failed due to duplicate name:"
CSCvu43355	FTD Lina traceback and reload in the QOS function
CSCvu44697	Firepower 4100/9300 - Fail-to-wire (FTW) EPM ports link flap during show tech collection
CSCvu46584	In GNOME glib-networking through 2.64.2, the implementation of GTlsCli
CSCvu53481	FTD upgrade fails due to HA config sync taking over 1h
CSCvu56286	FDM - New firewall session getting created after performing HA Failover for traffic in progress

Bug ID	Headline
CSCvu61711	FMC cannot add ACL rule with geolocation because "An internal error occurred."
CSCvu70529	Binary rules (SO rules) are not loaded when snort reloads
CSCvu85127	Unable to deploy if device with same UUID is trying to connect
CSCvv00254	When would have dropped events are generated some event data is invalid.

Resolved Bugs

Resolved Bugs in New Builds

Sometimes we release updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. If you downloaded an earlier build, do not use it.

You cannot upgrade from one build to another for the same software version. If you are already running an affected build, determine if an upgrade or hotfix would work instead. If not, contact Cisco TAC. See the Cisco Firepower Hotfix Release Notes for quicklinks to publicly available hotfixes.

Table 35: Version 6.4 New Builds

Version	New Build	Released	Packages	Platforms	Resolves
6.4.0.2	35	2019-07-03	Upgrade	FMC/FMCv FTD/FTDv, except Firepower 1000 series	CSCvq34224: Firepower Primary Detection Engine process terminated after Manager upgrade If you already upgraded to Version 6.4.0.2-34 and have FTD devices configured for high availability, apply Hotfix F. In FMC deployments, apply the hotfix to the FMC. In FDM deployments, apply the hotfix to both devices.
6.4.0	113	2020-03-03	Upgrade Reimage	FMC/FMCv	CSCvr95287: Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability If you are running an earlier build, apply the latest Version 6.4.0.x patch. If you cannot or do not want to patch, apply Hotfix T or Hotfix U.

Resolved Bugs in Version 6.4.0.18

Table last updated: 2024-04-24

Table 36: Resolved Bugs in Version 6.4.0.18

Bug ID	Headline
CSCvq48086	ASA concatenates syslog event to other syslog event while sending to the syslog server
CSCvv10948	FDM upgrade - There are no visible pending changes on UI -- but upgrade is not starting
CSCwa82736	FTD/ASA: Reordering of AnyConnect image fails with error Unable to remove/install image
CSCwc20635	Cisco Firepower Threat Defense ICMPv6 with Snort 2 Denial of Service Vulnerability
CSCwc40352	Lina Netflow sending permited events to Stealthwatch but they are block by snort afterwards
CSCwc78781	ASA/FTD may traceback and reload during ACL changes linked to PBR config
CSCwc91451	dvti hub core at ctm_sw_ipsec_cleanup_frags+394
CSCwd09231	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwd28037	No nameif during traffic causes the device traceback, lina core is generated.
CSCwe28912	FPR 4115- primary unit lost all HA config after ftd HA upgrade
CSCwe86923	In Apache MINA, a specifically crafted, malformed HTTP request may cause
CSCwe87134	ASA/FTD: Traceback and reload due to high rate of SCTP traffic
CSCwe93137	KP - multimode: ASA traceback observed during HA node break and rejoin.
CSCwf36419	ASA/FTD: Traceback and reload with Thread Name 'PTHREAD'
CSCwf47227	Remove Priority-queue command from FTD|| Priority-queue command causes silent egress packet drops
CSCwf60590	"show route all summary" executed on transparent mode FTD is causing CLISH to become Sluggish.
CSCwf63872	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
CSCwf64590	Units get kicked out of the cluster randomly due to HB miss | ASA 9.16.3.220
CSCwf69901	FTD: Traceback and reload during OSPF redistribution process execution
CSCwh04395	ASDM application randomly exits/terminates with an alert message on multi-context setup
CSCwh16301	Incorrect Hit count statistics on ASA Cluster only for Cluster-wide output

Bug ID	Headline
CSCwh19897	ASA/FTD Cluster: Reuse of TCP Randomized Sequence number on two different conns with same 5 tuple
CSCwh21474	ASA traceback when re-configuring access-list
CSCwh32118	ASDM management-sessions quota reached due to HTTP sessions stuck in CLOSE_WAIT
CSCwh41127	ASA/FTD: NAT64 error "overlaps with inside standby interface address" for Standalone ASA
CSCwh49244	"show aaa-server" command always shows the Average round trip time 0ms.
CSCwh49483	ASA/FTD may traceback and reload while running show inventory
CSCwh53745	ASA: unexpected logs for initiating inbound connection for DNS query response
CSCwh59199	ASA/FTD traceback and reload with IPSec VPN, possibly involving upgrade
CSCwh60604	ASA/FTD may traceback and reload in Thread Name 'lina' while processing DAP data
CSCwh65128	LINA show tech-support fails to generate as part of sf_troubleshoot.pl (Troubleshoot file)
CSCwh68482	FTD: Traceback and Reload in Process Name: lina
CSCwh69346	ASA: Traceback and reload when restore configuration using CLI
CSCwh77747	FPRM Audit logs not generated for user log in
CSCwh95175	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi02134	FTD sends multiple replicated NetFlow records for the same flow event
CSCwi31091	OSPF Redistribution route-map with prefix-list not working after upgrade
CSCwi40536	ASA/FTD: Traceback and reload when running show tech and under High Memory utilization condition
CSCwi46023	FTD drops double tagged BPDUs.
CSCwi59525	Multiple lina cores on 7.2.6 KP2110 managed by cdFMC
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability

Resolved Bugs in Version 6.4.0.17

Table last updated: 2024-05-22

Table 37: Resolved Bugs in Version 6.4.0.17

Bug ID	Headline
CSCvs74586	Firepower FTD transparent does not decode non-ip packets
CSCvt25221	FTD traceback in Thread Name cli_xml_server when deploying QoS policy
CSCvv24552	ASA/FTD: Traceback and Reload in Thread Name: Route Table Timestamp Update
CSCvx00655	ASA/SFR service card failure due to timeout getting CriticalStatus from PM
CSCvx09860	700-1158: 9 out of 150 VTI sessions down
CSCvy26511	Tune unmanaged disk alert thresholds for low end platforms
CSCvy30077	deploying anyconnect group-alias causes breaking HA and ungraceful failover
CSCvz00961	AnyConnect connection failure related to ASA truncated/corrupt config
CSCvz41551	FP2100: ASA/FTD with threat-detection statistics may traceback and reload in Thread Name 'lina'
CSCvz54471	ASA:Failed ASA in HA pair not recovering by itself, after an "HA state progression failed"
CSCvz70958	High Control Plane CPU due to dhcpp_add_ipl_stby
CSCwa04262	Cisco ASA Software SSL VPN Client-Side Request Smuggling Vulnerability via "/"URI
CSCwa72528	user-name from certificate feature does not work with SER option
CSCwa81427	External Authorization randomly fails on ASAv when using LDAP over SSL
CSCwb44848	ASA/FTD Traceback and reload in Process Name: lina
CSCwc03507	No-buffer drops on Internal Data interfaces despite little evidence of CPU hog
CSCwc64923	ASA/FTD may traceback and reload in Thread Name 'lina' ip routing ndbshr
CSCwc67687	ASA HA failover triggers HTTP server restart failure and ASDM outage
CSCwc68656	ASA CLI for TCP Maximum unprocessed segments
CSCwc74841	FMC RSS Feed broken because FeedBurner is no longer active - "Unable to parse feed"
CSCwc89796	ASA/FTD may traceback and reload in Thread Name 'appagent_async_client_receive_thread' hog detection
CSCwc95290	ESP rule missing in vpn-context may cause IPSec traffic drop

Bug ID	Headline
CSCwc99242	ISA3000 LACP channel member SFP port suspended after reload
CSCwd04210	ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT
CSCwd05772	Cisco FXOS Software Arbitrary File Write Vulnerability
CSCwd06005	ASA/FTD Cluster Traceback and Reload during node leave
CSCwd11855	ASA/FTD may traceback and reload in Thread Name 'ikev2_fo_event'
CSCwd19053	ASA/FTD may traceback with large number of network objects deployment using distribute-list
CSCwd22413	EIGRPv6 - Crashed with "mem_lock: Assertion mem_refcount' failed" on LINA.
CSCwd23188	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd25256	ASA/FTD Transactional Commit may result in mismatched rules and traffic loss
CSCwd26867	Device should not move to Active state once Reboot is triggered
CSCwd31181	Lina traceback and reload - VPN parent channel (SAL) has an invalid underlying channel
CSCwd33811	Cluster registration is failing because DATA_NODE isn't joining the cluster
CSCwd35726	Cisco FXOS Software Arbitrary File Write Vulnerability
CSCwd38774	ASA: Traceback and reload due to clientless webvpn session closure
CSCwd38775	ASA/FTD may traceback and reload in Thread lina
CSCwd38805	Syslog 106016 is not rate-limited by default
CSCwd39468	ASA/FTD Traceback and reload when configuring ISAKMP captures on device
CSCwd40260	Serviceability Enhancement - Unable to parse payload are silently drop by ASA/FTD
CSCwd41083	ASA traceback and reload due to DNS inspection
CSCwd48633	ASA - traceback and reload when Webvpn Portal is used
CSCwd49018	After establishing multicontext HA ,SNMP no longer outputs interface information.
CSCwd50218	ASA restore is not applying vlan configuration
CSCwd53135	ASA/FTD: Object Group Search Syslog for flows exceeding threshold
CSCwd56254	"show tech-support" generation does not include "show inventory" when run on FTD
CSCwd56296	FTD Lina traceback and reload in Thread Name 'IP Init Thread'
CSCwd56774	Misleading drop reason in "show asp drop"
CSCwd56995	Clientless Accessing Web Contents using application/octet-stream vs text/plain

Bug ID	Headline
CSCwd61016	ASA: Standby may get stuck in "Sync Config" status upon reboot when there is EEM is configured
CSCwd63580	FPR2100: Increase in failover convergence time with ASA in Appliance mode
CSCwd63961	AC clients fail to match DAP rules due to attribute value too large
CSCwd69454	Port-channel interfaces of secondary unit are in waiting status after reload
CSCwd74116	S2S Tunnels do not come up due to DH computation failure caused by DSID Leak
CSCwd78624	ASA configured with HA may traceback and reload with multiple input/output error messages
CSCwd82235	LINA Traceback on FPR-1010 under Thread Name: update_cpu_usage
CSCwd83141	CCL/CLU filters are not working correctly
CSCwd84868	Observing some devcmd failures and checkheaps traceback when flow offload is not used.
CSCwd85927	Traceback and reload when webvpn users match DAP access-list with 36k elements
CSCwd88641	Deployment changes to push VDB package based on Device model and snort engine
CSCwd89095	Stratix5950 and ISA3000 LACP channel member SFP port suspended after reload
CSCwd91421	ASA/FTD may traceback and reload in logging_cfg processing
CSCwd93376	Clientless VPN users are unable to download large files through the WebVPN portal
CSCwd94096	Anyconnect users unable to connect when ASA using different authentication and authorization server
CSCwd95436	Primary ASA traceback upon rebooting the secondary
CSCwd95908	ASA/FTD traceback and reload, Thread Name: rtcli async executor process
CSCwd96755	ASA is unexpected reload when doing backup
CSCwd97020	ASA/FTD: External IDP SAML authentication fails with Bad Request message
CSCwe03529	FTD traceback and reload while deploying PAT POOL
CSCwe05913	FTD traceback/reloads - Icmp error packet processing involves snp_nat_xlate_identity
CSCwe07722	Cluster data unit drops non-VPN traffic with ASP reason "VPN reclassify failure
CSCwe14174	FTD - 'show memory top-usage' providing improper value for memory allocation
CSCwe18974	ASA/FTD may traceback and reload in Thread Name: CTM Daemon
CSCwe20043	256-byte memory block gets depleted on start if jumbo frame is enabled with FTD on ASA5516

Bug ID	Headline
CSCwe21187	ASA/FTD may drop multicast packets due to no-mcast-intrf ASP drop reason until UDP timeout expires
CSCwe21280	Multicast connection built or teardown syslog messages may not always be generated
CSCwe29529	FTD MI does not adjust PVID on vlans attached to BVI
CSCwe29583	ASA/FTD may traceback and reload in Thread Name 'None' at lua_getinfo
CSCwe29850	ASA/FTD Show chunkstat top command implementation
CSCwe36176	ASA/FTD: High failover delay with large number of (sub)interfaces and http server enabled
CSCwe38029	Multiple traceback seen on standby unit.
CSCwe40463	Stale IKEv2 SA formed during simultaneous IKE SA handling when missing delete from the peer
CSCwe42061	Deleting a BVI in FTD interfaces is causing packet drops in other BVIs
CSCwe44311	FP2100:Update LINA asa.log files to avoid recursive messages-&lt;date&gt;.1.gz rotated filenames
CSCwe44672	Syslog ASA-6-611101 is generated twice for a single ssh connection
CSCwe45779	ASA/FTD drops traffic to BVI if floating conn is not default value due to no valid adjacency
CSCwe51286	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe59737	ASA/FTD reboots due to traceback pointing to watchdog timeout on p3_tree_lookup
CSCwe61928	PIM register packets are not sent to RP after a reload if FTD uses a default gateway to reach the RP
CSCwe61969	ASA Multicontext 'management-only' interface attribute not synced during creation
CSCwe63067	ASA/FTD may traceback and reload in Thread Name 'lina' due to due to tcp intercept stat
CSCwe63232	ASA/FTD: Ensure flow-offload states within cluster are the same
CSCwe64404	ASA/FTD may traceback and reload
CSCwe64563	The command "neighbor x.x.x.x ha-mode graceful-restart" removed when deleting any created context
CSCwe65634	ASA - Standby device may traceback and reload during synchronization of ACL DAP
CSCwe66132	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe67751	Last fragment from SIP IPv6 packets has MF equal to 1, flagging that more packets are expected

Bug ID	Headline
CSCwe67816	ASA / FTD Traceback and reload when removing isakmp capture
CSCwe74328	AnyConnect - mobile devices are not able to connect when hostscan is enabled
CSCwe78977	ASA/FTD may traceback and reload in Thread Name 'pix_flash_config_thread'
CSCwe79072	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe80278	Dynamic interface NAT rules cause SSH/ICMP to fail with nat-no-xlate-to-pat-pool in ASA cluster
CSCwe85432	ASA/FTD traceback and reload on thread DATAPATH-14-11344 when SIP inspection is enabled
CSCwe86225	ASA/FTD traceback and reload due citing thread name: cli_xml_server in tm_job_add
CSCwe89030	Serial number attribute from the subject DN of certificate should be taken as the username
CSCwe90720	ASA Traceback and reload in parse thread due ha_msg corruption
CSCwe92905	ngfwManager process continuously restarting leading to ZMQ Out of Memory traceback
CSCwe93489	Threat-detection does not recognize exception objects with a prefix in IPv6
CSCwe93532	ASA/FTD may traceback and reload in Thread Name 'lina'.
CSCwe95757	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwf04831	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwf06818	Cisco Firepower Threat Defense Software Encrypted Archive File Policy Bypass Vulnerability
CSCwf10910	FTD : Traceback in ZMQ running 7.3.0
CSCwf14126	ASA Traceback and reload citing process name 'lina'
CSCwf14811	TCP normalizer needs stats that show actions like packet drops
CSCwf17042	ASDM replaces custom policy-map with default map on class inspect options at backup restore.
CSCwf20338	ASA may traceback and reload in Thread Name 'DHCPv6 Relay'
CSCwf22005	ASA Packet-tracer displays the first ACL rule always, though matches the right ACL
CSCwf23564	Unable to establish BGP when using MD5 authentication over GRE TUNNEL and FTD as passthrough device
CSCwf26534	ASA/FTD: Connection information in SIP-SDP header remains untranslated with destination static Any
CSCwf33574	ASA access-list entries have the same hash after upgrade

Bug ID	Headline
CSCwf33904	[IMS_7_4_0] - Virtual FDM Upgrade fails: HA configStatus='OUT_OF_SYNC after UpgradeOnStandby
CSCwf42144	ASA/FTD may traceback and reload citing process name "lina"
CSCwf44537	99.20.1.16 lina crash on nat_remove_policy_from_np
CSCwf49573	ASA/FTD: Traceback and reload when issuing 'show memory webvpn all objects'
CSCwf54418	Reduce time taken to clear stale IKEv2 SAs formed after Duplicate Detection
CSCwf78321	ASA: Checkheaps traceback and reload due to Clientless WebVPN
CSCwf95147	OSPFv3 Traffic is Centralized in Transparent Mode
CSCwh13821	ASA/FTD may traceback and reload in when changing capture buffer size
CSCwh23100	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
CSCwh23567	PAC Key file missing on standby on reload

Resolved Bugs in Version 6.4.0.16

Table last updated: 2022-11-21

Table 38: Resolved Bugs in Version 6.4.0.16

Bug ID	Headline
CSCvs27235	nat-no-xlate-to-pat-pool drops when master leaves cluster and after rebalance
CSCvu84127	Firepower may reboot for no apparent reason
CSCvu87906	Backup file keep growing in 6.6.0-90 (Unified Event Files are Incorrectly Included In Backup)
CSCvu96069	HA during failover active having traffic with high CPU the system may reload unexpected
CSCvv52349	No utility to handle XFS corruption on 2100/1000 series Firepower devices
CSCvv97527	asa config timeout command breaks snort's DAQ configuration
CSCvw29647	FTD: NAS-IP-Address:0.0.0.0 in Radius Request packet as network interface for aaa-server not defined
CSCvw52083	FXOS logrotate does not rotate properly all the log files
CSCvw72260	ASA upgrade failed with: "CSP directory does not exist - STOP_FAILED Application_Not_Found"
CSCvw82067	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic

Bug ID	Headline
CSCvw94160	CIAM: openssl CVE-2020-1971
CSCvw98315	FXOS reporting old FTD version after FTD upgrade to 6.7.0
CSCvx89827	Not able to set Bangkok time zone in FPR 2110
CSCvy50598	BGP table not removing connected route when interface goes down
CSCvy65178	Need dedicated Rx rings for to the box BGP traffic on Firepower platform
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
CSCvy90162	Traceback watchdog bark at Unicorn Proxy Thread from scaled AC-SSL-SAML Auth TVM profile
CSCvy95520	Cisco Firepower Management Center and Firepower Threat Defense Software SSH DoS Vulnerability
CSCvy96895	ASA disconnects the VTY session using of Active IP address and Standby MAC address after failed over
CSCvz05767	FP-1010 HA link goes down or New hosts unable to connect to the device
CSCvz15755	FTD - Port-channel not coming up after upgrade and may generate core file
CSCvz55140	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 117, seq 17)
CSCvz60142	ASA/FTD stops serving SSL connections
CSCvz61689	Port-channel member interfaces are lost and status is down after software upgrade
CSCvz71596	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
CSCvz75988	Inconsistent logging timestamp with RFC5424 enabled
CSCvz78816	ASA disconnects the ssh, https session using of Active IP address and Standby MAC address after FO
CSCvz83432	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 121, seq 18)
CSCvz85683	Wrong syslog message format for 414004
CSCvz85913	ASN.1 strings are represented internally within OpenSSL as an ASN1_STR for CISCO-SSL-1.0.2
CSCwa04395	User Agent session processing crashes SFDataCorrelator on 6.6.5 standalone sensors
CSCwa05385	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 19)

Bug ID	Headline
CSCwa20758	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20)
CSCwa32286	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 125, seq 21)
CSCwa41936	Cisco FTD Bleichenbacher Attack Vulnerability
CSCwa46905	WM 1010 speed/duplex setting is not getting effect and causes unstable interface
CSCwa50145	FPR8000 sensor UI login creates shell user with basic privileges
CSCwa55562	Different CG-NAT port-block allocated for same source IP causing per-host PAT port block exhaustion
CSCwa67884	Conditional flow-offload debugging produces no output
CSCwa75966	ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped
CSCwa76564	ASDM session/quota count mismatch in ASA when multiple context switch before and after failover
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwa90615	WR8 and LTS18 commit id update in CCM layer (seq 24)
CSCwa91070	Cgroup triggering oom-k for backup process
CSCwb01983	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb01990	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb01995	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02006	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02026	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
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
CSCwb08644	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
CSCwb13294	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 25)
CSCwb15795	Audit message not generated by: no logging enable from ASAv9.12
CSCwb17963	Unable to identify dynamic rate liming mechanism & not following msg limit per/sec at syslog server.
CSCwb24039	ASA traceback and reload on routing

Bug ID	Headline
CSCwb26212	ASA drops existing anyconnect sessions and stop accepting new ayconnect sessions
CSCwb28849	ASA/FTD: Mitigation of OpenSSL vulnerability CVE-2022-0778
CSCwb41361	WR8, LTS18 and LTS21 commit id update in CCM layer (seq 26)
CSCwb41854	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwb46949	LTS18 commit id update in CCM layer (seq 27)
CSCwb51707	ASA Traceback and reload in process name: lina
CSCwb52401	Cisco Firepower Threat Defense Software Privilege Escalation Vulnerability
CSCwb53172	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
CSCwb53328	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url
CSCwb53694	Cisco Firepower Management Center Software XML External Entity Injection Vulnerability
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
CSCwb61901	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb61908	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb65447	FTD: AAB cores are not complete and not decoding
CSCwb65718	FMC is stuck on loading SI objects page
CSCwb66761	Cisco Firepower Threat Defense Software Generic Routing Encapsulation DoS Vulnerability
CSCwb67040	FP4112|4115 Traceback & reload on Thread Name: netfs_thread_init
CSCwb68642	ASA traceback in Thread Name: SXP CORE
CSCwb71460	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
CSCwb74571	PBR not working on ASA routed mode with zone-members
CSCwb74938	ASA traceback and reload with error "assertion "0" failed: file "timer_services.c", line 165"
CSCwb78971	Fatal error: Upgrade Failed: Invalid password: A blank or masked password is not allowed

Bug ID	Headline
CSCwb79812	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
CSCwb80192	WR6, WR8 commit id update in CCM layer(Seq 30)
CSCwb80559	FTD offloads SGT tagged packets although it should not
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
CSCwb83388	ASA HA Active/standby tracebacks seen approximately every two months.
CSCwb86118	TPK ASA: Device might get stuck on ftp copy to disk
CSCwb87498	Lina traceback and reload during EIGRP route update processing.
CSCwb87950	Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability
CSCwb88587	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb89963	ASA Traceback & reload in thread name: Datapath
CSCwb90074	ASA: Multiple Context Mixed Mode SFR Redirection Validation
CSCwb92709	We can't monitor the interface via "snmpwalk" once interface is removed from context.
CSCwb92937	Error 403: Forbidden when expanding in view group objects
CSCwb93914	Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability
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.
CSCwb97251	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCwc02133	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwc02488	ASA/FTD may traceback and reload in Thread Name 'None'
CSCwc02700	Fragmented packets are dropped when unit leaves cluster
CSCwc03069	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
CSCwc08676	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 32)
CSCwc09414	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwc10037	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwc10792	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete

Bug ID	Headline
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
CSCwc23695	ASA/FTD can not parse UPN from SAN field of user's certificate
CSCwc25207	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 33)
CSCwc26648	ASA/FTD Traceback and Reload in Thread name Lina or Datatath
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
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
CSCwc40413	Memory leak in rulesd0, rulesd1, rulesd2, rulesd3 on IPS 8350
CSCwc41590	Upgrade fail & App Instance fail to start with err "CSP_OP_ERROR. CSP signature verification error."
CSCwc41661	FTD Multiple log files with zero byte size.
CSCwc44289	FTD - Traceback and reload when performing IPv4 &lt;&gt; 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
CSCwc46569	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 34)
CSCwc49095	ASA/FTD 2100 platform traceback and reload when fragments are coalesced and sent to PDTS
CSCwc50887	FTD - Traceback and reload on NAT IPv4&lt;&gt;IPv6 for UDP flow redirected over CCL link
CSCwc51326	FXOS-based Firepower platform showing 'no buffer' drops despite high values for RX ring watermarks

Bug ID	Headline
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
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
CSCwc60907	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 35)
CSCwc61912	ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6
CSCwc64565	ASA Traceback and reload in aaa_shim_thread
CSCwc66757	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwc72284	TACACS Accounting includes an incorrect IPv6 address of the client
CSCwc73224	Call home configuration on standby device is lost after reload
CSCwc74103	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-11-32591'
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
CSCwc90091	ASA 9.12(4)47 with &lt;user-statistics&gt;, will affects the "policy-server xxxx global" visibility.
CSCwc93166	Using write standby in a user context leaves secondary firewall license status in an invalid state
CSCwc94501	ASA/FTD tracebacks due to ctm_n5 resets
CSCwc96805	traceback and reload due to tcp intercept stat in thread unicorn
CSCwd00386	ASA/FTD may traceback and reload when clearing the configration due to "snp_clear_acl_log_flow_all"
CSCwd11303	ASA might generate traceback in ikev2 process and reload

Resolved Bugs in Version 6.4.0.15

Table last updated: 2022-05-11

Table 39: Resolved Bugs in Version 6.4.0.15

Bug ID	Headline
CSCvx10555	A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker
CSCvt85766	FPR2k: FCM Syslog Remote Destinations tab disappeared after upgrading
CSCwa53489	Lina Traceback and Reload Due to invalid memory access while accessing Hash Table
CSCvw94160	CIAM: openssl CVE-2020-1971
CSCvx06920	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 103, seq 5)
CSCvz89327	OSPFv2 flow missing cluster centralized "c" flag
CSCwa26535	IPv6 PMTU discovery does not work for RA VPN Cllient with tunneled route
CSCvz92016	Cisco ASA and FTD Software Web Services Interface Privilege Escalation Vulnerability
CSCvz05541	ASA55XX: Expansion module interfaces not coming up after a software upgrade
CSCvz15755	FTD - Port-channel not coming up after upgrade and may generate core file
CSCvx24245	ASA Traceback and reload in occam_group_free
CSCvw37340	Vulnerability in the MySQL Server product of Oracle MySQL (component:
CSCvx98807	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 109, seq 9)
CSCvx16700	FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC"
CSCwa40223	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCvx47550	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 105, seq 6)
CSCvw43510	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP ...
CSCvz89126	ASDM session/quota count mismatch in ASA when multiple context switchover is done from ASDM
CSCvy66530	lrzsz before version 0.12.21~rc can leak information to the receiving
CSCvy66531	There's a flaw in libxml2's xmllint in versions before 2.9.11. An atta
CSCvt25917	FTD CLI - Fail to display the disabled local user and cannot enable back
CSCwa19443	Flow Offload - Compare state values remains in error state for longer periods
CSCvz82562	ASA/FTD: site-to-site VPN - traffic incorrectly fragmented

Bug ID	Headline
CSCvz68336	SSL decryption not working due to single connection on multiple in-line pairs
CSCwa05385	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 19)
CSCvx37833	Diskmanager improperly pruning connection events leads to corrupt files
CSCwa73172	ASA reload and traceback in Thread Name: PIX Garbage Collector
CSCvz41761	FMC Does not allow to create an EIGRP authentication secret key using the $ character
CSCvz92932	ASA show tech execution causing spike on CPU and impacting to IKEv2 sessions
CSCvx73164	Lasso SAML Implementation Vulnerability Affecting Cisco Products: June 2021
CSCvz76966	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DNS DoS
CSCvy02448	Time sync do not work correctly for ASA on FPFPR2100 series platform
CSCwa15291	A crafted request uri-path can cause mod_proxy to forward the request to an origin server...
CSCwa79494	Traffic keep failing on Hub when IPSec tunnel from Spoke flaps
CSCwa87315	ASA/FTD may traceback and reload in Thread Name 'IP Address Assign'
CSCvx47628	In OpenLDAP through 2.4.57 and 2.5.x through 2.5.1alpha, an assertion
CSCwa04134	The in-memory certificate cache in strongSwan before 5.9.4 has a remot
CSCvy89658	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 114, seq 13)
CSCvw43529	Integer overflow in the DHCP client (udhcpc) in BusyBox before 1.25. ...
CSCvw62288	ASA: 256 byte block depletion when syslog rate is high
CSCvy60285	The mq_notify function in the GNU C Library (aka glibc) through 2.33 has a use-after-free
CSCvy60574	Port dcosAG leak fix CSCvx14602 to KP/WM
CSCvw72260	ASA upgrade failed with: "CSP directory does not exist - STOP_FAILED Application_Not_Found"
CSCvw90923	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 101, seq 4)
CSCvz95108	FTD Deployment failure post upgrade due to major version change on device
CSCvy96698	Resolve spurious status actions checking speed values twice in FXOS portmgr
CSCvu84127	Firepower may reboot for no apparent reason
CSCvx54585	nfm-burnin.sh fails: Incorrect Expanded Geryon base and media CPLD

Bug ID	Headline
CSCwa28822	FTD moving UI management from FDM to FMC causes traffic to fail
CSCvw98315	FXOS reporting old FTD version after FTD upgrade to 6.7.0
CSCwb18252	FTD/ASA: Traceback on BFD function causing unexpected reboot
CSCwa26038	ICMP inspection causes packet drops that are not logged appropriately
CSCvv21602	cfprApSmMonitorTable is missing in the FP2K MIB
CSCwa44950	ASA/FTD - Memory leak observed when VPN is deployed
CSCvw48829	Timezone in "show clock" is different from which in "show run clock"
CSCvz08387	ASP drop capture output may display incorrect drop reason
CSCvx41045	High CPU utilization in sfmbservice in FMC
CSCvw98603	Multiple vulnerabilities in SQlite
CSCwa41834	ASA/FTD traceback and reload due to pix_startup_thread
CSCvx47634	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and
CSCvy30016	SSL decryption policy may cause performance degradation in Snort
CSCvx47636	A flaw was discovered in ldap_X509dn2bv in OpenLDAP before 2.4.57 lead
CSCvu41615	Cisco FTD Software Snort Out of Memory Denial of Service Vulnerability
CSCvw43537	The recv_and_process_client_pkt function in networking/ntpd.c in bus ...
CSCvz51157	In librt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/s
CSCvz30558	Cisco Firepower Management Center Cross-site Scripting Vulnerability
CSCvz36933	Sensor SNMP process may restart when policy deploy
CSCvy60295	A flaw was found in OpenLDAP. openLDAPÃ¢ETMs slapd server trigger an assertion failure.
CSCvy60294	There's a flaw in libxml2 in versions before 2.9.11. An attacker who i
CSCvy60292	There is a flaw in the xml entity encoding functionality of libxml2 in
CSCvz05687	Fragmented Certificate request failed for DND flow
CSCwa30114	"Error:NAT unable to reserve ports" when using a range of ports in an object service
CSCwa74900	Traceback and reload after enabling debug webvpn cifs 255
CSCvy64145	WR6 and WR8 commit id update in CCM layer(sprint 113, seq 12)
CSCvu75930	Service module not returning error to supervisor when SMA resources are depleted

Bug ID	Headline
CSCvz76746	While implementing management tunnel a user can use open connect to bypass anyconnect.
CSCwa96759	Lina may traceback and reload on tcpmod_proxy_handle_mixed_mode
CSCvw97256	Need handling of rmu read failure to ignore link state update when link state API read fails
CSCvz55140	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 117, seq 17)
CSCvs42388	Gratuitous logging of string: "Memory stats information for preprocessor is NULL"
CSCvz05767	FP-1010 HA link goes down or New hosts unable to connect to the device
CSCvy10789	FTD 2110 ascii characters are disallowed in LDAP password
CSCwa58686	ASA/FTD Change in OGS compilation behavior causing boot loop
CSCvz71064	Deleting The Context From ASA taking Almost 2 Minutes with ikev2 tunnel
CSCvz46333	FTD policy deployment failure due to internal socket connection loss
CSCwa56975	DHCP Offer not seen on control plane
CSCvs84242	FMC Deployment Failure when removing Auto NAT and correlated network object
CSCvz32623	An integer overflow in util-linux through 2.37.1 can potentially cause
CSCvy04430	Management Sessions fail to connect after several weeks
CSCvy95329	Incorrect Access rule matching because of ac rule entry missing
CSCvw43541	inftrees.c in zlib 1.2.8 might allow context-dependent attackers to ...
CSCvy04343	ASA in PLR mode,"license smart reservation" is failing.
CSCvw43544	The crc32_big function in crc32.c in zlib 1.2.8 might allow context- ...
CSCvz24238	CiscoÂ Firepower Management Center Cross-site Scripting Vulnerability
CSCwa06960	ASA Traceback and Reload due to CTM daemon during internal health test
CSCvx66329	FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh
CSCvy95520	Incorporate fail2ban into IMS to prevent SSH DOS attack
CSCwa65389	ASA traceback and reload in Unicorn Admin Handler when change interface configuration via ASDM
CSCwa32286	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 125, seq 21)
CSCvx95884	High CPU and massive "no buffer" drops during HA bulk sync and during normal conn sync

Bug ID	Headline
CSCvr39217	Fxos Snmp-user is not persistent after reboot
CSCwb01700	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA
CSCwa08262	AnyConnect users with mapped group-policies take attributes from default GP under the tunnel-group
CSCvw93159	Firepower 2100: ASA/FTD generates message "Local disk 2 missing on server 1/1"
CSCvy03045	Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed
CSCvx89827	Not able to set Bangkok time zone in FPR 2110
CSCvx91317	A remote code execution issue was discovered in MariaDB 10.2 before 10
CSCvz85913	ASN.1 strings are represented internally within OpenSSL as an ASN1_STR for CISCO-SSL-1.0.2
CSCvz65181	Cisco Firepower Threat Defense Software Security Intelligence DNS Feed Bypass Vulnerabilit
CSCvv17599	Multiple vulnerabilities in cpe:2.3:o:linux:linux_kernel:4.14.187:
CSCvw16165	Firepower 1010 Series stops passing traffic when a member of the port-channel is down
CSCvw52083	FXOS logrotate does not rotate properly all the log files
CSCvz33468	ASA/FTD - NAT stops translating source addresses after changes to object-groups in manual NAT Rule
CSCvy60305	A flaw was found in ImageMagick in versions before 7.0.11. has a potential cipher leak
CSCvv52349	No utility to handle XFS corruption on 2100/1000 series Firepower devices
CSCvw09745	NFE ports are down after upgrade to 6.4.0.10-86 before reapplying AC policy
CSCvw43555	A heap-based buffer overflow exists in Info-Zip UnZip version &lt;= 6.0 ...
CSCwa85043	Traceback: ASA/FTD may traceback and reload in Thread Name 'Logger'
CSCvw43559	BusyBox project BusyBox wget version prior to commit 8e2174e9bd836e5 ...
CSCvy08798	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 110, seq 10)
CSCvx10520	curl 7.20.0 through 7.70.0 is vulnerable to improper restriction of na
CSCwa13873	ASA Failover Split Brain caused by delay on state transition after "failover active" command run
CSCvy60284	A flaw was found in OpenLDAP in versions before 2.4.56. This flaw allo

Bug ID	Headline
CSCvx67468	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 107, seq 7)
CSCvv55066	FPR1010: Internal-Data0/0 and data interfaces are flapping during SMB file transfer
CSCwa56449	ASA traceback in HTTP cli EXEC code
CSCvx33904	Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation
CSCwa85138	Multiple issues with transactional commit diagnostics
CSCvx97053	Unable to configure ipv6 address/prefix to same interface and network in different context
CSCvz25066	fs/seq_file.c in the Linux kernel 3.16 through 5.13.x before 5.13.4 do
CSCwa33898	Cisco Adaptive Security Appliance Software Clientless SSL VPN Heap Overflow Vulnerability
CSCvz25064	The wordexp function in the GNU C Library (aka glibc) through 2.33 may
CSCwa68660	FTP inspection stops working properly after upgrading the ASA to 9.12.4.x
CSCvy98027	Application interface down whereas physical interface Up on FXOS
CSCvp69087	core_svc_sam_dme found after upgrade
CSCwa36535	Standby unit failed to join failover due to large config size.
CSCvx13835	Multiple vulnerabilities in bind
CSCvz73146	FTD - Traceback in Thread Name: DATAPATH
CSCvz61767	Policy deployment with SNMPv2 or SNMPv1 configuration fails
CSCvt64238	FXOS pktmgr Rx Drops counter keeps increasing in LACP Port-Channel
CSCvy41763	Cisco Firepower Threat Defense Software XML Injection Vulnerability
CSCwa87597	ASA/FTD Failover: Joining Standby reboots when receiving configuration replication from Active mate
CSCvx49720	BIND servers are vulnerable if they are running an affected version an
CSCvs68576	Deploy failure when deleting auto nat rule due to double negate
CSCvy60333	ImageMagick before 7.0.8-50 has a "use of uninitialized value" vulnerability
CSCwb01919	FP2140 ASA 9.16.2 HA units traceback and reload at lua_getinfo (getfuncname)
CSCvr38379	Upgraded FTD will not reimage to base FTD version with the use of 'auto-install' feature in FPR2100
CSCvx10514	An issue was discovered in p11-kit 0.21.1 through 0.23.21. Multiple in

Bug ID	Headline
CSCvw43489	The NEEDBITS macro in the inflate_dynamic function in inflate.c for ...
CSCvr33586	FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded
CSCvx10519	curl 7.62.0 through 7.70.0 is vulnerable to an information disclosure
CSCwa94894	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-4-9608'
CSCvz09106	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
CSCwa55878	FTD Service Module Failure: False alarm of "ND may have gone down"
CSCwa11079	Pre allocate sub context for DRBG health test
CSCvz44645	FTD may traceback and reload in Thread Name 'lina'
CSCwa77083	Host information is missing when Security Zones are configured in Network Discovery rules
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
CSCvx26927	TLS site not loading when it has segmented and retransmitted CH
CSCvz91218	Statelink hello messages dropped on Standby unit due to interface ring drops on high rate traffic
CSCwa20758	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20)
CSCwa40719	Traceback: Secondary firewall reloading in Threadname: fover_parse
CSCvy35948	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 111, seq 11)
CSCwa67882	Offloaded GRE tunnels may be silently un-offloaded and punted back to CPU
CSCvy60322	In BIND 9.0.0 -&gt; 9.11.29, 9.12.0 -&gt; 9.16.13, and versions BIND 9.9.3-S
CSCvy60320	A race condition in Linux kernel SCTP sockets (net/sctp/socket.c) befo
CSCvy12991	Chassis local date and time may drift back to midnight Jan 1 2015 after reboot
CSCvy60326	Integer overflow in the htmldoc 1.9.11 and before may allow attackers
CSCvv24647	FTD 2100 - SNMP: incorrect values returned for Ethernet statistics polling
CSCvx49717	An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before
CSCvw13348	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 98, seq 2)
CSCwa97784	ASA: Jumbo sized packets are not fragmented over the L2TP tunnel
CSCvx78968	ASA/FTD Traceback and reload on Thread Name: IKEv2 Daemon with VTIs configured

Bug ID	Headline
CSCwa29810	ASA Certificate enrollment via Local CA server is not possible
CSCwa60574	ASA traceback and reload on snp_ha_trans_alloc_msg_muxbuf_space function
CSCwa14485	Cisco Firepower Threat Defense Software Denial of Service Vulnerability
CSCvw43546	In the add_match function in libbb/lineedit.c in BusyBox through 1.2 ...
CSCwa61361	ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR
CSCvy24921	SNMPv3 - SNMP EngineID changes after every configuration change
CSCvx47642	An integer underflow was discovered in OpenLDAP before 2.4.57 leading
CSCvx47643	A flaw was discovered in OpenLDAP before 2.4.57 leading to a slapd cra
CSCvx47644	A flaw was discovered in OpenLDAP before 2.4.57 leading to an assertio
CSCvz30582	Cisco Firepower Management Center Cross-site Scripting Vulnerability
CSCvy18166	AAB snort core due to high volume traffic logging
CSCvv95277	FPR2100 High disk usage in partition /opt/cisco/platform/logs due to growth of httpd log files
CSCwa18858	ASA drops non DNS traffic with reason "label length 164 bytes exceeds protocol limit of 63 bytes"
CSCvw02334	ipv6 route table (data and management) in a multi-context environment.
CSCvx91341	An issue was discovered in GNOME GLib before 2.66.8. When g_file_repla
CSCwa40237	Cisco Firepower Management Center File Upload Security Bypass Vulnerability
CSCvv79459	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 94, seq 1)
CSCvz86256	Primary ASA should send GARP as soon as split-brain is detected and peer becomes cold standby
CSCwb07981	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
CSCvt67167	Data Unit traceback and reload without traffic at Thread Name :"logger"
CSCvx49716	An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before
CSCvw43508	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZ ...
CSCwb25809	Single Pass - Traceback due to stale ifc
CSCwa31373	duplicate ACP rules are generated on FMC 6.6.5 after rule copy.
CSCwa11088	Access rule-ordering gets automatically changed while trying to edit it before page refresh/load

Bug ID	Headline
CSCvq39187	KP: Host key verification is getting failed while ssh to host
CSCvz83432	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 121, seq 18)
CSCvw43610	In IJG JPEG (aka libjpeg) before 9d, jpeg_mem_available() in jmemnob ...
CSCvz81342	Diskmanager not pruning AMP File Capture files
CSCwa57115	New access-list are not taking effect after removing non-existance ACL with objects.

Resolved Bugs in Version 6.4.0.14

Table last updated: 2022-02-17

Table 40: Resolved Bugs in Version 6.4.0.14

Bug ID	Headline
CSCwa46963	Security: CVE-2021-44228 -> Log4j 2 Vulnerability
CSCwa70008	Expired certs cause Security Intel. and malware file preclassification signature updates to fail
CSCwa88571	Unable to register FMC with the Smart Portal

Resolved Bugs in Version 6.4.0.13

Table last updated: 2021-12-02

Table 41: Resolved Bugs in Version 6.4.0.13

Bug ID	Headline
CSCum03297	ENH: ASA should save the timestamp of the MAXHOG in 'show proc cpu-hog'
CSCvg66052	2 CPU Cores continuously spike on firepower appliances
CSCvi58484	Cluster: ping sourced from FTD/ASA to external IPs may if reply lands on different cluster unit
CSCvm76755	DP-CP arp-in and adj-absent queues need to be separated
CSCvp16933	Cisco Firepower Threat Defense Software Shell Access Vulnerability
CSCvp69936	ASA : Traceback on tcp_intercept Thread name : Threat detection
CSCvq39187	KP: Host key verification is getting failed while ssh to host
CSCvq43454	ENH : Support a tolerance time for the "NotValidBefore" timestamp, while using SAML auth

Bug ID	Headline
CSCvq54299	After restart of both A/S units, not all context configs may be loaded when using SL on 2100
CSCvr11958	AWS FTD: Deployment failure with ERROR: failed to set interface to promiscuous mode
CSCvr33586	FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded
CSCvr38379	Upgraded FTD will not reimage to base FTD version with the use of 'auto-install' feature in FPR2100
CSCvr39217	Fxos Snmp-user is not persistent after reboot
CSCvs27336	Traceback on ASA by Smart Call Home process
CSCvs47365	Event rate seen on FMC slows down or stops coming from devices using FXOS 2.9.1 update
CSCvt10944	ctm crashed while sending emix traffic over VTI tunnel
CSCvt15348	ASA show processes cpu-usage output is misleading on multi-core platforms
CSCvt25917	FTD CLI - Fail to display the disabled local user and cannot enable back
CSCvt31292	FTD device might not send events to SSE
CSCvt64238	FXOS pktmgr Rx Drops counter keeps increasing in LACP Port-Channel
CSCvt85766	FPR2k: FCM Syslog Remote Destinations tab disappeared after upgrading
CSCvu36302	%ASA-3-737403 is used incorrectly when vpn-addr-assign local reuse-delay is configured
CSCvu97242	FTD 2100: Corefile and crashinfo might both be truncated and incomplete in the event of a crash
CSCvv07917	ASA learning a new route removes asp route table created by floating static
CSCvv20780	Policy deploy fails with "Failed to hold the deployment transaction" error
CSCvv24647	FTD 2100 - SNMP: incorrect values returned for Ethernet statistics polling
CSCvv43190	Crypto engine errors when GRE header protocol field doesn't match protocol field in inner ip header
CSCvv48594	Memory leak: due to snp_tcp_intercept_stat_top_n_integrate() in threat detection
CSCvv48942	Snmpwalk showing traffic counter as 0 for failover interface
CSCvv55248	Syslogs generated for ACL transaction commit are not in consistent format & not available some times
CSCvv62499	FMC: Remove_peers.pl script should work when FTD is member of a cluster

Bug ID	Headline
CSCvv71097	traceback: ASA reloaded snp_fdb_destroy_fh_callback+104
CSCvv79459	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 94, seq 1)
CSCvv84172	Dangling ref in Clustered table and EO upon failed registration
CSCvv85029	ASA5555 traceback and reload on Thread Name: ace_work
CSCvv89715	Fastpath rules for Firepower 8000 series stack disappear randomly from the FMC
CSCvw03628	ASA will not import CA certificate with name constraint of RFC822Name set as empty
CSCvw06298	ASA duplicate MAC addresses in Shared Interfaces of different Contexts causing traffic impact
CSCvw13348	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 98, seq 2)
CSCvw16165	Firepower 1010 Series stops passing traffic when a member of the port-channel is down
CSCvw18614	ASA/FTD traceback in the LINA process
CSCvw48829	Timezone in "show clock" is different from which in "show run clock"
CSCvw62526	ASA traceback and reload on engineering ASA build - 9.12.3.237
CSCvw68593	A flaw in the way reply ICMP packets are limited in the Linux kernel f
CSCvw71405	FPR1120 running ASA traceback and reload in crypto process.
CSCvw90923	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 101, seq 4)
CSCvw93159	Firepower 2100: ASA/FTD generates message "Local disk 2 missing on server 1/1"
CSCvw93276	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCvw97256	Need handling of rmu read failure to ignore link state update when link state API read fails
CSCvx04003	Lack of throttling of ARP miss indications to CP leads to oversubscription
CSCvx06920	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 103, seq 5)
CSCvx14031	IPv4 DACL stuck on Active device when DACL removed after CoA for IKEv2 Session, traffic not impacted
CSCvx16134	100% cpu-usage for some processes seen in "show processes cpu-usage" though using multicore
CSCvx23833	IKEv2 rekey - Invalid SPI for ESP packet using new SPI received right after Create_Child_SA response
CSCvx24537	SAML: SAML Authentication may fail if we have 2 or more IDP certs with same Subject Name

Bug ID	Headline
CSCvx25719	X-Frame-Options header is not set in webvpn response pages
CSCvx29814	IP address in DHCP GIADDR field is reversed after sending DHCP DECLINE to DHCP server
CSCvx33904	Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation
CSCvx34237	ASA reload with FIPS failure
CSCvx42081	FPR4150 ASA Standby Ready unit Loops to failed and remove config to install it again
CSCvx43150	On the FMC, process of registration of member device post RMA is not successful
CSCvx45976	ASA/FTD Watchdog forced traceback and reload in Threadname: vnet-proxy (rip: socks_proxy_datarelay)
CSCvx47230	X-Frame-Options header support for older versions of IE and windows platforms
CSCvx47550	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 105, seq 6)
CSCvx49715	Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may
CSCvx50980	ASA CP CPU wrong calculation leads to high percentage (100% CP CPU)
CSCvx54235	ASP capture dispatch-queue-limit shows no packets
CSCvx57417	Smart Tunnel Code signing certifcate renewal
CSCvx64478	Unwanted console output during SAML transactions
CSCvx65745	FPR2100: enable kernel panic on octeon for UE events to trigger crash
CSCvx66329	FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh
CSCvx67468	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 107, seq 7)
CSCvx68355	ASA - unable to import CA certificate when countryName is encoded as UTF8
CSCvx71571	ASA: "ERROR: Unable to delete entries from Hash Table" with CSM
CSCvx75963	ASA traceback while taking captures
CSCvx77768	Traceback and reload due to Umbrella
CSCvx80830	VPN conn fails from same user if Radius server sends a dACL and vpn-simultaneous-logins is set to 1
CSCvx86621	ASA(lina) clock (always shows Jan 2010) does not sync properly with fxos
CSCvx87709	FPR 2100 running ASA in HA. Traceback and reload on watchdog during failover

Bug ID	Headline
CSCvx95255	Supportive change in ASA to differentiate, new ASDM connections from existing ASDM context switch
CSCvx95884	High CPU and massive "no buffer" drops during HA bulk sync and during normal conn sync
CSCvx97632	ASA traceback and reload when copying files with long destination filenames using cluster command
CSCvx98807	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 109, seq 9)
CSCvy01752	Traceback on FPR 4115 in Thread - Lic HA Cluster
CSCvy02448	Time sync do not work correctly for ASA on FPFPR2100 series platform
CSCvy02703	ASA/FTD tracebacks due to CTM message handler
CSCvy03006	improve debugging capability for uauth
CSCvy03045	Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed
CSCvy03907	Creation/Edit of Access Control Policy fails with error 'Rule Name Already Exists'
CSCvy04869	AnyConnect certificate authentication fails if user certificate has 8192 bits key size
CSCvy07491	ASA traceback when re-configuring access-list
CSCvy08798	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 110, seq 10)
CSCvy08908	Port-forwarding application blocked by Java
CSCvy10583	ASA Traceback and Reload in Thread Name: DATAPATH
CSCvy10789	FTD 2110 ascii characters are disallowed in LDAP password
CSCvy12782	FTD/ASA: PATed traffic impacted when configured on ixgbe-vf SRIOV interfaces in HA
CSCvy14721	ssl traffic dropped by FTD while CH packet has a destination port no greater than source port
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
CSCvy18366	LINA Crash from pdts_pd_segment.c:1941 on FPR1k & ISA3k
CSCvy21334	Active tries to send CoA update to Standby in case of "No Switchover"

Bug ID	Headline
CSCvy23349	FTD unnecessarily ACKing TCP flows on inline-pair deployment
CSCvy25849	ASA fails to process the OCSP response when the string 'OK' is missing in the HTTP response
CSCvy31424	QP FTD application fails to start due to outdated affinity.conf following FXOS/FTD upgrade
CSCvy33105	Ambiguous command error is shown for 'show route bgp' or 'show route isis' if DNS lookup is enabled
CSCvy33676	UN-NAT created on FTD once a prior dynamic xlate is created
CSCvy35737	FTD traceback and reload during anyconnect package verification
CSCvy35948	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 111, seq 11)
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
CSCvy46026	"Unable to load container (UUID)" when try to open a device under Devices > Device management
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
CSCvy49732	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCvy50011	ASA traceback in IKE Daemon process and reload
CSCvy51814	Firepower flow-offload stops offloading all existing and new flows
CSCvy52074	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
CSCvy53461	RSA keys & Certs get removed post reload on WS-SVC-ASA-SM1-K7 with ASA code 9.12.x
CSCvy55356	CPU hogs less than 10 msec are produced contrary to documentation
CSCvy57905	VTI tunnel interface stays down post reload on KP/WM platform in HA
CSCvy60574	Port dcosAG leak fix CSCvx14602 to KP/WM
CSCvy61008	Time out of sync between Lina and FXOS
CSCvy64145	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 113, seq 12)

Bug ID	Headline
CSCvy64492	ASAv adding non-identity L2 entries for own addresses on MAC table and dropping HA hellos
CSCvy64911	Debugs for: SNMP MIB value for crasLocalAddress is not showing the IP address
CSCvy67756	Firepower Services HTTPS traffic stops working when matching Do not decrypt rule in SSL policy
CSCvy69189	FTD HA stuck in bulk state due to stuck vpnfol_sync/Bulk-sync keytab
CSCvy72846	ASA accounting reports incorrect Acct-Session-Time
CSCvy74781	The standby device is sending the keep alive messages for ssl traffic after the failover
CSCvy80202	Intrusion Event Performance Graphs load blank on 4100 despite of fix of CSCvm48451
CSCvy89658	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 114, seq 13)
CSCvy91668	PAT pool exhaustion with stickiness traffic could lead to new connection drop.
CSCvy92990	FTD traceback and reload related to SSL after upgrade to 7.0
CSCvy96625	Revert 'fix' introduced by CSCvr33428 and CSCvy39659
CSCvy96698	Resolve spurious status actions checking speed values twice in FXOS portmgr
CSCvy98027	Application interface down whereas physical interface Up on FXOS
CSCvy98458	FP21xx -traceback "Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header"
CSCvz00383	FTD lina traceback and reload in thread Name Checkheaps
CSCvz00699	Traceback in webvpn and reload experienced periodically after ASA upgrade
CSCvz05189	FTD reload with Lina traceback during xlate replication in Cluster
CSCvz07614	ASA: Orphaned SSH session not allowing us to delete a policy-map from CLI
CSCvz15529	ASA traceback and reload thread name: Datapath
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
CSCvz25434	ASA/FTD blackholes traffic due to 1550 block depletion when BVI is configured as DHCP client
CSCvz27714	Interface flapping on 8350 sensor during policy deployments

Bug ID	Headline
CSCvz29233	ASA: ARP entries from custom context not removed when an interface flap occurs on system context
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
CSCvz38361	BGP packets dropped for non directly connected neighbors
CSCvz39565	ASA/FTD Traceback and Reload during bulk VPN session connect
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
CSCvz48407	Traceback and reload in Thread Name: DATAPATH-15-18621
CSCvz53142	ASA does not use the interface specified in the name-server command to reach IPv6 DNS servers
CSCvz57710	conf t is converted to disk0:/t under context-config mode
CSCvz58710	ASA traceback due to SCTP traffic.
CSCvz60901	ASA: IPv6 Neighbor reachability issues
CSCvz60970	ASA Traceback in Thread Name: DATAPATH-4-23199 in enic_put / FREEB when sending LU to statelink
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"
CSCvz69571	ASA log shows wrong value of the transferred data after the anyconnect session terminated.
CSCvz73709	ASA/FTD Standby unit fails to join HA
CSCvz77744	OSPFv3: FTD Wrong "Forwarding address" added in ospfv3 database
CSCvz81934	Revert 'fix' introduced by CSCvx95884
CSCvz84850	ASA/FTD traceback and reload caused by "timer services" function
CSCvz87824	ASASM traceback and reload on "snp_svcmod_heart_beat_timeout_cb" function

Resolved Bugs in Version 6.4.0.12

Table last updated: 2021-05-13

Table 42: Resolved Bugs in Version 6.4.0.12

Bug ID	Headline
CSCtx83747	Syslog 718055 contains wrongly formatted MAC address
CSCui74211	Expired DHCP-Client leases not purged on ASA-standby unit
CSCuj60109	ENH: SFP transceivers attached to ASA-IC-6GE-SFP-A are not shown by CLI
CSCuj99176	Make ASA-SSM cplane keepalives more tolerable to communication delays
CSCun74870	ASA IKEv2: NO-PROPOSAL-CHOSEN sent instead of TS_UNSUPPORTED
CSCuq47482	ENH: ASA show tech should include "show module x detail"
CSCut44164	ASA: Add additional crypto stats to "show tech"
CSCuu60064	ENH: ASAv show tech should include "show vm"
CSCuu84198	DHCPRelay debugs should highlight invalid parameters from DHCP server
CSCuw51499	TCM doesn't work for ACE addition/removal, ACL object/object-group edits
CSCuy53106	ASA OS incorrectly calculates certificate expiry date in Syslog 717054
CSCvb92169	ASA should provide better fragment-related logs and ASP drop reasons
CSCvc40724	Invalid group URL causes improperly formatted message back to AnyConnect
CSCvf88062	CTM: Nitrox S/G lengths need to be validated
CSCvg59385	ASA scansafe connector takes too long to failover to secondary CWS Tower
CSCvg69380	ASA - rare cp processing corruption causes console lock
CSCvg73237	ENH: Configure CAC as an absolute value as well instead of just percentage of total VPN capacity.
CSCvh30209	Traceback in mfib_idb_get when toggling multicast on/off repeatedly
CSCvh85504	"Backlog Status" health module false negative alerts
CSCvi07901	CISCO-REMOTE-ACCESS-MONITOR-MIB crasIPSecNumSessions is zero on ASA for IKEv2 AnyConnect
CSCvi85020	Order of SSH configuration generates "SSH version 1 is not secure." error messages at boot
CSCvk51778	"show inventory" (or) "show environment" on ASA 5515/5525/5545/5555 shows up Driver/ioctl error logs

Bug ID	Headline
CSCvm15088	ENH: Add PSU details in "show environment" for ASA5525
CSCvm78605	ASA Failover: 'show interface tunnel' shows tunnel source as standby IP address
CSCvm82290	ASA core blocks depleted when host unreachable in IRB/TFW configuration
CSCvm98585	CPU hog from idfw module observed in 5525 FTD
CSCvn12453	Implement debug menu command to show RX ring number a flow is hashed to
CSCvn16864	ENH: Missing Content-Security-Policy Header in ASA HTTP WebVPN portal
CSCvn16877	ENH: Missing X-Content-Type-Options Header in ASA HTTP WebVPN portal
CSCvn16887	ENH: Missing X-XSS-Protection Header in ASA HTTP WebVPN portal
CSCvn64647	ASA traceback and reload due to tcp_retrans_timeout internal thread handling
CSCvn82441	[SXP] Issue with establishing SXP connection between ASA on FPR-2110 and switches
CSCvn93683	ASA: cluster exec show commands not show all output
CSCvn95731	ASA traceback and reload on Thread Name SSH
CSCvo11623	ASAv/Azure: Smart Licensing does not use hostname from custom template for registration
CSCvo12504	ASA: Failover fsm gets stuck in a multicontext in case of module difference.
CSCvo33227	BusyBox udhcp Components Out-of-Bounds Read Information Disclosure Vul
CSCvo33896	snmpd(): insufficient memory to handle queries
CSCvo34210	ASA running 9.6.4.20 Traceback in threadname Unicorn Proxy Thread
CSCvo58030	Failover mac address configured on interface does not allow to delete subinterface
CSCvo64516	ASA fails command authorization if tcp syslog is down.
CSCvo68887	Timestamp in Crash File name says UTC but is local timezone
CSCvo78772	ENH: ASA WebVPN should send "Cache-Control: no-store" instead of "Cache-Control: no-cache"
CSCvo81249	ASA may cause high-rate of DNS queries between ASA (acting as a DNS client) and a server
CSCvo86485	incorrect HTML <base> tag handling by Grammar Based Parser
CSCvo87430	FTD : Can't deploy ISAKMP VPNs containing question marks
CSCvo99076	ENH: IKEv2 quick connection preempt for static IP assigned to client by AAA

Bug ID	Headline
CSCvp09083	ASA working as DHCP server drops DHCP renewal request packet sent by DHCP clients
CSCvp10079	DB switch role failed on FMC HA switch
CSCvp13352	ASA continues to do TCP keepalives for Client side connections even after vpn session times out
CSCvp16618	URL inside HTML base tag is not rewritten after it is handled by GBP
CSCvp23530	OSPF neighbor command not replicated to standy after write standby or reload
CSCvp29554	Traceback and reload due to a watchdog timeout when accessingfilesystem (webvpn related)
CSCvp29803	Apache HTTP Server Modules Scripts Arbitrary Code Execution Vulnerab ...
CSCvp31311	There should be enough PKI handles for the max sessions on a given platform
CSCvp38774	WebVPN rewriter not loading website correctly
CSCvp42484	IS-IS hello packet length not updated to correct mtu when mtu modified
CSCvp42722	ASA does not generate logging message 611103 for any syslog destination (buffer, trap, etc)
CSCvp52437	ASA | Saving configuration, give message "Platform does not support appliance mode configuration."
CSCvp56719	Cisco FMC and FTD Software sftunnel Pass the Hash Vulnerability
CSCvp57417	Upon downgrade of an ASAv, the firewall may traceback and reload
CSCvp67033	ASA: Cannot distinguish name aliases for IPv6 and displays a "incomplete command" error message
CSCvp69229	OpenSSL 0-byte Record Padding Oracle Information Disclosure Vulnerabil
CSCvp71766	Radius authentication fails when sourced from BVI across a VPN tunnel
CSCvp71879	limit-resource CLI for ssh/telnet has no effect if quota-CLI is not configured
CSCvp72624	SNMP Limit for OID 1.3.6.1.2.1.4.35 (ipNetToPhysicalTable)
CSCvp73394	Failover ASA IKEv2 VTI: Secondary ASA sends standby IP as the traffic selector
CSCvp75965	primary FPR2110 crash after customer configure syslog setting on FMC
CSCvp76904	With dhcp-network-scope configured incorrectly, DHCP debugs on ASA show wrong gateway and netmask.
CSCvp77226	ASA traceback and reload on sysopt traffic detailed in multicontext mode
CSCvp78171	ASA in cluster fail to synchronise IPv6 ND table with peer units.

Bug ID	Headline
CSCvp91905	ASA will add the newly configured IPv6 Address to the current link-local address
CSCvp94478	ASA scp quite slow
CSCvp96658	Inconsistency in timezone for show logging in newer versions
CSCvq00560	ASA silently drops packets which violate ESP Authentication data field size (ICV)
CSCvq15976	ASA Memory Leak - snp_svc_insert_dtls_session
CSCvq17551	Syslog 711004 not consistently triggering event manager event
CSCvq22358	Disabling anti-replay for one context it disables it for other contexts as well
CSCvq27016	FMC shows 'Unable to fetch failover history..' for FTD HA.
CSCvq37913	VPN-sessiondb does not replicate to standby ASA
CSCvq47743	AnyConnect and Management Sessions fail to connect after several weeks
CSCvq49124	ASA on FP1010 Traceback in http_exec_cli thread
CSCvq49718	Observed Traceback in ASA with dns debugs enabled while resolving FQDN Entries
CSCvq50944	OSPFv3 neighborship is flapping every ~30 minutes
CSCvq54620	FPR4110 crashes after using 'vpn-sessions logoff all'
CSCvq54624	DTLS AnyConnect tunnel doesn't resume due to cache miss
CSCvq55426	Adding an ipv6 default route causes CLI to hang for 50 seconds
CSCvq58729	2140: crypto accelerator status show SOFTWARE mode by default
CSCvq65864	Traceback in HTTP Cli Exec with rest-api agent enabled
CSCvq70536	FTD: Deployment failure when breaking HA and graceful-restart is present on config
CSCvq73595	ASA webvpn unable to extract username from cert UPN if username is longer than 32 chars
CSCvq76706	Ability to clear message logged statistics in output of "show logging"
CSCvq78126	V route is missing even after setting the reverse route in Crypto map config in HA-IKEv2
CSCvq79042	FQDN ACL entries incomplete due to DNS response from server is large and truncated
CSCvq81410	ASA::Unable to execute any ASA command via http using safari browser.
CSCvq81692	ASA: After changing admin-context, call-home does not use new admin context setting
CSCvq83060	SNMP: Cannot get failover link information from oid in multiple mode

Bug ID	Headline
CSCvq84444	Configuring static routes causes "Route Session" rerr counter to increment on standby ASA
CSCvq87625	ENH: Addition of 'show run all sysopt' to 'show tech' output
CSCvq92240	Memory leak observed while running AnyConnect ssl vpn tests
CSCvq93640	WRL6 and WRL8 commit id update in CCM layer (sprint 67)
CSCvq93836	ENH: Addition of 'show logging setting' to 'show tech' output
CSCvq98396	ASA: crypto session handles leak on the standby unit
CSCvq99107	Hot swap of SFP is not taking effect on the ASA
CSCvr03705	We need to have default route with AD and tunneled at the same time for the same next hub.
CSCvr04203	Memory leak observed while running AnyConnect ssl vpn tests
CSCvr09399	Dynamic flow-offload can't be disabled
CSCvr12018	ASA: VPN traffic fails to take the tunnel route when the default route is learnt over BGP.
CSCvr15503	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA
CSCvr20486	FTD 1010 Passive interfaces does not receive unicast packets
CSCvr20757	Block leak on ASA while running Cisco Umbrella DNS inspection
CSCvr20876	low memory causes kernel to invoke - oom and reload device - modified rlimit for KP
CSCvr23580	Can't delete 2 or more than two IP address-pool
CSCvr23986	Cisco ASA & FTD devices may reload under conditions of low memory and frequent complete MIB walks
CSCvr33428	FMC generates Connection Events from a SYN flood attack
CSCvr35872	ASA traceback Thread Name: DATAPATH with PBR configured
CSCvr37486	established rules in asp table are not un-installed on config removal
CSCvr37502	libexpat Improper Parsing Denial of Service Vulnerability
CSCvr39516	lina segfault/reload caused by malloc failure in modexp-octeon
CSCvr50509	Some 3DES related configurations are lost after booted
CSCvr50630	ASA Traceback: SCTP bulk sync and HA synchronization
CSCvr50718	ASA | Incorrect handling of ICMP-TYPE objects for ICMP6 rules

Bug ID	Headline
CSCvr51426	ASA is not sending the mask in the accounting packets
CSCvr55518	Missing clean up on rule creation failure.
CSCvr57605	ASA after reload had license context count greater than platform limits
CSCvr58411	RRI on static HUB/SPOKE config is not working on HUB when a new static SPOKE is added or deleted
CSCvr60195	ASA/FTD may traceback and reload when repeatedly adding/removing multicast commands
CSCvr68146	Unable to auto-rejoin FTD cluster
CSCvr68872	Secondary unit exceed platform context count limit in split brain scenario when failover link down
CSCvr72648	BIGNUM leak in ec_bits()
CSCvr80164	WR6 and WR8 commit id update in CCM layer(sprint 72)
CSCvr83372	I/O error occurred while writing; fd='28', error='Resource temporarily unavailable (11)'
CSCvr86077	ASA Traceback/pagefault in Datapath due to re_multi_match_ascii
CSCvr90079	HSTS config option not updated on show run all
CSCvr90462	Improve ipv6 duplicate address detection to avoid disabling ipv6 in case of transient active-active
CSCvr92311	Standby ASA logging %ASA-4-720022: (VPN-Secondary) Cannot find trust point __tmpCiscoM1Root__
CSCvr98924	ASA traceback and reload due to routing subsystem
CSCvr99642	ASA traceback and reload multiple times with trace "webvpn_periodic_signal"
CSCvs02954	ASA OSPF: Prefix removed from the RIB when topology changes, then added back when another SPF is run
CSCvs04179	ASA - 9.8.4.12 traceback and reload in ssh or fover_rx Thread
CSCvs05262	Decrement TTL display wrong result
CSCvs13204	ASAv failover traffic on SR-IOV interfaces might be dropped due to interface-down
CSCvs16073	snmp poll failure with host and host-group configured
CSCvs27264	mroute entries on ASA not getting refreshed.
CSCvs28213	ASA Traceback in Thread Name SSH with assertion slib_malloc.c

Bug ID	Headline
CSCvs29779	ASA may traceback and reload while waitinPC g for "DATAPATH-12-1899" process to finish.
CSCvs31159	Incorrect empty location handling inside CSCOGet_location wrapper
CSCvs31443	ASA reporting negative memory values on "%ASA-5-321001: Resource 'memory' limit'" message
CSCvs31470	OSPF Hello causing 9K block depletion, control point CPU 100% and cluster unstable.
CSCvs32907	Addition of debug counters for STRAP implementation.
CSCvs33102	ASA/FTD may traceback and reload in Thread Name 'EIGRP-IPv4'
CSCvs33852	After upgrade to version 9.6.4.34 is not possible to add an access-group
CSCvs38785	Inconsistent timestamp format in syslog
CSCvs39589	ASA doesn't honor SSH Timeout When Data Channel is not Negotiated
CSCvs40230	ICMP not working and failed with inspect-icmp-seq-num-not-matched
CSCvs43154	Secondary ASA is unable to join the failover due to aggressive warning messages.
CSCvs45111	WR6 and WR8 commit id update in CCM layer(sprint 75)
CSCvs45548	reactivation-mode timed causing untimely reactivation of failed server
CSCvs47283	Traffic may match an access-list incorrectly with object-group-search enabled
CSCvs48437	ASA cannot send syslog to two UDP ports at same time
CSCvs52108	ASA Traceback Due to Umbrella Inspection
CSCvs52169	ASA sends malformed RADIUS message when device-id from AnyConnect is too long
CSCvs55603	ICMP Reply Dropped when matched by ACL
CSCvs56802	Cisco Firepower 2100 Series SSL/TLS Inspection Denial of Service Vulnerability
CSCvs59487	Observed crash in KP device while upgrading to 99.14.1.64 image.
CSCvs59558	Failover mac address getting removed on the reload of the Primary active unit
CSCvs59966	false reported value for OID "cipSecGlobalActiveTunnels" - same as ASDM
CSCvs60254	libxml2 xmlParseBalancedChunkMemoryRecover Memory Leak Vulnerability
CSCvs63484	SAML tokens are not removed from hash table
CSCvs70260	IKEv2 vpn-filter drops traffic with implicit deny after volume based rekey collision
CSCvs71698	Management default route conflicts with default data routing

Bug ID	Headline
CSCvs71969	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability
CSCvs72378	ASDM session being abruptly terminated when switching between different contexts
CSCvs72450	FXOS - Recover hwclock of service module from corruption due to simultaneous write collision
CSCvs73663	ASA Traceback on IPsec message handler Thread
CSCvs73754	ASA/FTD: Block 256 size depletion caused by ARP of BVI not assigned to any physical interface
CSCvs76605	Wrong Module version listed for FXOS 2.6(1.174)
CSCvs77818	Traceback: spin_lock_fair_mode_enqueue: Lock (np_conn_shrlock_t) is held for a long time
CSCvs82726	Placeholder to address CSCvs31470 in Multi-Context Mode
CSCvs84542	ASA traceback with thread: idfw_proc
CSCvs85196	ASA SIP connections drop after several consecutive failovers: pinhole timeout/closed by inspection
CSCvs87795	ASA: backup context failed to "ERROR: No such file or directory"
CSCvs88413	Port-channel bundling is failing after upgrade to 9.8 version
CSCvs90100	ASA/FTD may traceback and reload in Thread Name 'License Thread'
CSCvs94486	CSCvs59487 requires additional fix for resolution
CSCvs97863	Reduce number of fsync calls during close in flash file system
CSCvs97908	Invalid scp session terminates other active http, scp sessions
CSCvt00255	Upgrade kernel to cpe:2.3:o:linux:linux_kernel:4.14.187:
CSCvt01282	WR6 and WR8 commit id update in CCM layer(sprint 79)
CSCvt05862	IPv6 DNS server resolution fails when the server is reachable over the management interface.
CSCvt06606	Flow offload not working with combination of FTD 6.2(3.10) and FXOS 2.6(1.169)
CSCvt06841	Incorrect access-list hitcount seen when configuring it with a capture on ASA
CSCvt08492	Events are not generated on FDM after FXOS upgrade
CSCvt11302	On FPR devices when FIPS is enabled cannot create webtype ACLs
CSCvt11547	Cisco Firepower Device Manager Software Filesystem Space Exhaustion Denial of Service Vuln

Bug ID	Headline
CSCvt11661	DOC - Clarify the meaning of mp-svc-flow-control under show asp drop
CSCvt11742	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCvt12463	ASA: Traceback in thread Unicorn Admin Handler
CSCvt13301	Default Syslog using non-standard port does not work for Intrusion events
CSCvt13822	ASA: VTI rejecting IPSec tunnel due to no matching crypto map entry
CSCvt15056	SFR managed by ASDM: System policy does not apply.
CSCvt17912	stress, pushing platform limits causing segfault/reload in lina_free_exec_st
CSCvt18199	IPv6 Nat rejected with error "overlaps with inside standby interface address" for Standalone ASA
CSCvt22356	Health-check monitor-interface debounce-time in ASA Cluster resets to 9000ms after ASA reboot
CSCvt23643	VPN failover recovery is taking approx. 30 seconds for data to resume
CSCvt25225	ASA: Active unit HA traceback and reload during Config Sync state during OSPF sync
CSCvt26031	ASAv Unable to register smart licensing with IPv6
CSCvt26530	FTD failed over due to 'Inspection engine in other unit has failed due to snort failure'
CSCvt27585	Observed traceback on 2100 while performing Failover Switch from Standby.
CSCvt30731	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 80)
CSCvt35945	Encryption-3DES-AES should not be required when enabling ssh version 2 on 9.8 train
CSCvt36542	Multi-context ASA/LINA on FPR not sending DHCP release message
CSCvt38279	Erase disk0 on ISA3000 causes file system not supported
CSCvt39977	Invalid packet data when PSNG_TCP_PORTSCAN [122:1:1] rule alerts.
CSCvt41357	"no logging permit-hostdown" does not block connections when syslog host is inaccessible
CSCvt43136	Multiple Cisco Products Snort TCP Fast Open File Policy Bypass Vulnerability
CSCvt43967	Pad packets received from RA tunnel which are less than or equal 46 bytes in length with zeros
CSCvt46289	ASA LDAPS connection fails on Firepower 1000 Series
CSCvt48601	Cisco Firepower Manament Center Software Stored Cross-Site Scripting Vulnerability

Bug ID	Headline
CSCvt50528	Warning Message for default settings with Installation of Certificates in ASA/FTD - CLI
CSCvt51349	Fragmented packets forwarded to fragment owner are not visible on data interface captures
CSCvt51987	Traffic outage due to 80 size block exhaustion on the ASA FPR9300 SM56
CSCvt53640	ASA5585 may traceback and reload after upgrading SFR from 6.4.0 to 6.4.0.x
CSCvt54182	LINA cores are generated when FTD is configured to do SSL decryption.
CSCvt63027	Cisco Firepower Management Center XML Entity Expansion Vulnerability
CSCvt63484	ASA High CPU with igb_saleen_io_sfp_mod_poll_thre process
CSCvt64035	remote acess mib - SNMP 64 bit only reporting 4Gb before wrapping around
CSCvt64952	"Show crypto accelerator load-balance detail" has missing and undefined output
CSCvt65982	Route Fallback doesn't happen on Slave unit, upon RRI route removal.
CSCvt68294	Adjust Firepower 4120 Maximum VPN Session Limit to 20,000
CSCvt70664	ASA: acct-session-time accounting attribute missing from Radius Acct-Requests for AnyConnect
CSCvt71529	ASA traceback and reload during SSL handshake
CSCvt72683	NAT policy configuration after NAT policy deployment on FP 8130 is not seen
CSCvt73407	TACACS Fallback authorization fails for Username enable_15 on ASA device.
CSCvt75760	Traceback/Page-fault in Clientless WebVPN due to HTTP cleanup
CSCvt80126	ASA traceback and reload for the CLI "show asp table socket 18421590 det"
CSCvt80134	WebVPN rewriter fails to parse data from SAP Netweaver.
CSCvt80172	Supervisor software needs to be upgraded to address CVE-2017-11610
CSCvt83133	Unable to access anyconnect webvpn portal from google chrome using group-url
CSCvt90330	ASA traceback and reload with thread name coa_task
CSCvt91521	Crypto accelerator bias setting should be included in show tech
CSCvt92647	Connectivity over the state link configured with IPv6 addresses is lost after upgrading the ASA
CSCvt98599	IKEv2 Call Admission Statistics "Active SAs" counter out of sync with the real number of sessions
CSCvt99020	Cisco Firepower Manament Center Software Stored Cross-Site Scripting Vulnerability

Bug ID	Headline
CSCvt99137	With huge FTP traffic in cluster, the SEC_FLOW messages are in a retransmit loop
CSCvu00112	tsd0 not reset when ssh quota limit is hit in ci_cons_shell
CSCvu03107	AnyConnect statistics is doubled in both %ASA-4-113019 and RADIUS accounting
CSCvu03562	Device loses ssh connectivity when username and password is entered
CSCvu03675	FPR2100: ASA console may hang & become unresponsive in low memory conditions
CSCvu05180	aaa-server configuration missing on the FTD after a Remote Access VPN policy deployment
CSCvu06767	Lina cores on multi-instance causing a boot loop on both logical-devices
CSCvu07602	FPR-41x5: 'clear crypto accelerator load-balance' will cause a traceback and reload
CSCvu07880	ASA on QP platforms display wrong coredump filesystem space (50 GB)
CSCvu12039	Cluster data unit might fail to synchronize SCTP configuration from the control unit after bootup
CSCvu12045	Deployment fails for NGIPS with error "System (/etc/rc.d/init.d/netif-speed eth0) Failed"
CSCvu12248	ASA-FPWR 1010 traceback and reload when users connect using AnyConnect VPN
CSCvu16423	ASA 9.12(2) - Multiple tracebacks due to Unicorn Proxy Thread
CSCvu17924	FTD failover units traceback and reload on DATAPATH
CSCvu17965	ASA generated a traceback and reloaded when changing the port value of a manual nat rule
CSCvu20007	Config_XML_Response from LINA is not in the correct format,Lina reporting as No memory available.
CSCvu20666	Few FPR 2100 series External Authentication RADIUS not taking configuration
CSCvu26296	ASA interface ACL dropping snmp control-plane traffic from ASA
CSCvu26561	WebVPN SSO Gives Unexpected Results when Integrated with Kerberos
CSCvu29184	Cisco Firepower Threat Defense Software Command File Overwrite Vulnerability
CSCvu29395	Traceback observed while performing master role change with active IGMP joins
CSCvu29660	Block exhaustion snapshot not created when available blocks goes to zero
CSCvu32698	ASA Crashes in SNMP while joining the cluster when key config-key password-encryption" is present
CSCvu33992	traceback: ASA reloaded lina_sigcrash+1394

Bug ID	Headline
CSCvu34413	SSH keys lost in ASA after reload
CSCvu40213	ASA traceback in Thread Name kerberos_recv
CSCvu40324	ASA traceback and reload with Flow lookup calling traceback
CSCvu40398	ASAv reload due to FIPS SELF-TEST FAILURE after enabling FIPS
CSCvu43924	GIADDR of DHCP Discover packet is changed to the ip address of dhcp-network-scope
CSCvu45748	ASA traceback in threadname 'ppp_timer_thread'
CSCvu45822	ASA experienced a traceback and reloaded
CSCvu48886	FTD deployment failure when removing non-default "crypto ikev2 limit max-in-negotiation-sa"
CSCvu49625	[PKI] Standard Based IKEv2 Certificate Auth session does second userfromcert lookup unnecessarily
CSCvu55469	FTD - Connection idle timeout doesn't reset
CSCvu55843	ASA traceback after TACACS authorized user made configuration changes
CSCvu61704	ASA high CPU with intel_82576_check_link_thread impacting on overall unit performance
CSCvu65688	IKEv2 CAC "Active SAs" counter out of sync with the real number of sessions despite CSCvt98599
CSCvu68529	Embryonic connections limit does not work consistently
CSCvu70931	Cluster / aaa-server key missing after "no key config-key" is entered
CSCvu72094	ASA traceback and reload on thread name DATAPATH
CSCvu73207	DSCP values not preserved in DTLS packets towards AnyConnect users
CSCvu77095	ASA unable to delete ACEs with remarks and display error "Specified remark does not exist"
CSCvu78721	Cannot change (modify) interface speed after upgrade
CSCvu89110	ASA: Block new conns even when the "logging permit-hostdown" is set & TCP syslog is down
CSCvu90727	Native VPN client with EAP-TLS authentication fails to connect to ASA
CSCvu91097	Cisco Firepower Management Center Software Policy Vulnerability
CSCvu91792	SNMP IfInDiscards OIDs for Internal-Data 0/0 and 0/1 may return incorrect values
CSCvu98222	FTD Lina engine may traceback in datapath after enabling SSL decryption policy

Bug ID	Headline
CSCvv04584	Multicast traffic is being dropped with the resson no-mcast-intrf
CSCvv07721	FirePOWER: System>Users>User Roles Pages is blank on Firepower 7000 and Firepower 8000 series
CSCvv07864	Multicast EIGRP traffic not seen on internal FTD interface
CSCvv08244	Firepower module may block trusted HTTPS connections matching 'Do not decrypt' SSL decryption rule
CSCvv08684	Cluster site-specific MAC addresses not rewritten by flow-offload
CSCvv09396	Stale VPN routes for L2TP, after the session was terminated
CSCvv10778	Traceback in threadname DATAPATH (5585) or Lina (2100) after upgrade to 9.12.4
CSCvv12127	Series 3 policy deploy can fail when adding a large number of IPV4 source and destination AC rules.
CSCvv12857	ASA gets frozen after crypto engine failure
CSCvv15572	ASA traceback observed when "config-url" is entered while creating new context
CSCvv16082	stress/low memory: assert: mh->mh_mem_pool > MEMPOOL_UNDEFINED && mh->mh_mem_pool < MEMPOOL_MAX_TYPE
CSCvv19230	ASAv Anyconnect users unexpectedly disconnect with reason: Idle Timeout
CSCvv20450	FMC 6.4 to 6.7 upgrade fails "Error running script 500_rpms/110_generate_dbaccess.sh"
CSCvv23370	Observed traceback in FPR2130 while running webVPN, SNMP related traffic.
CSCvv25394	After upgrade ASA swapped names for disks, disk0 became disk1 and vice versa.
CSCvv25839	reCAPTCHA is not working when SSl decryption is enable.
CSCvv28997	ASA Traceback and reload on thread name Crypto CA
CSCvv29687	Rate-limit syslogs 780001/780002 by default on ASA
CSCvv30172	Intermittently after reboot, ADI can't join KCD
CSCvv31334	Lina traceback and reload seen on trying to switch peer on KP HA with 6.6.1-63
CSCvv31629	Intermittently embedded ping reply over GRE drops on FTD cluster if traffic passes asymmetrically.
CSCvv32333	ASA still doesn't allow to poll internal-data0/0 counters via SNMP in multiple mode
CSCvv32425	ASA traceback when running show asp table classify domain permit
CSCvv34003	snmpwalk for OID 1.3.6.1.2.1.47.1.1.1.1.5 on ISA 3000 returning value of 0 for .16 and .17

Bug ID	Headline
CSCvv34140	ASA IKEv2 VTI - Failed to request SPI from CTM as responder
CSCvv36518	ASA: Extended downtime after reload after CSCuw51499 fix
CSCvv36725	ASA logging rate-limit 1 5 message ... limits to 1 message in 10 seconds instead of 5
CSCvv37629	Malformed SIP packets leads to 4k block hold-up till SIP conn timeout causing probable traffic issue
CSCvv40223	Error parsing flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.cdb, when trying to modify/read the user-db
CSCvv41453	Removing static ipv6 route from management-only route table affects data traffic
CSCvv43484	ASA stops processing RIP packets after system upgrade
CSCvv44270	ASAv5 reloads without traceback.
CSCvv48942	Snmpwalk showing traffic counter as 0 for failover interface
CSCvv49698	ASA Anyconnect url-redirect not working for ipv6
CSCvv49800	ASA/FTD: HA switchover doesn't happen with graceful reboot of firepower chassis
CSCvv50338	Traceback Cluster unit on snpi_nat_xlate_destroy+2508
CSCvv53696	ASA/FTD traceback and reload during AAA or CoA task of Anyconnect user
CSCvv56644	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv57590	ASA: ACL compilation takes more time on standby
CSCvv57842	WebSSL clientless user accounts being locked out on 1st bad password
CSCvv58332	ASA/FTD is reading BGP MP_REACH_NLRI attribute's next-hop bytes in reverse order
CSCvv58605	ASA traceback and reload in thread:Crypto CA,mem corruption by unvirtualized pki global table in MTX
CSCvv59036	Static routes deleted from the FMC without user deleting it.
CSCvv59676	Snort2: Implement aggressive pruning for certificate cache for TLS to free up memory
CSCvv62305	ASA traceback and reload in fover_parse when attempting to join the failover pair.
CSCvv63412	ASA dropping all traffic with reason "No route to host" when tmatch compilation is ongoing
CSCvv65184	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv66005	ASA traceback and reload on inspect esmtp

Bug ID	Headline
CSCvv66920	Inner flow: U-turn GRE flows trigger incorrect connection flow creation
CSCvv67500	ASA 9.12 random traceback and reload in DATAPATH
CSCvv70984	ASA traceback while modifying the bookmark SSL Ciphers configuration
CSCvv72466	OSPF network commands go missing in the startup-config after upgrading the ASA
CSCvv73017	Traceback due to fover and ssh thread
CSCvv79897	Block "sensor restart" command for FTD units to prevent Lina crash and system reboot event
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
CSCvv87496	ASA cluster members 2048 block depletion due to "VPN packet redirect on peer"
CSCvv88017	ASA: EasyVPN HW Client triggers duplicate phase 2 rekey causing disconnections across the tunnel
CSCvv90181	No deployment failure reason in transcript if 'show running-config' is running during deployment
CSCvv90720	ASA/FTD: Mac address-table flap seen on connected switch after a HA switchover
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
CSCvw01028	7K/8K devices experience unresponsiveness if upgraded to 6.4.0.[9,10,11] from release prior to 6.4.0
CSCvw05393	Certificate validation syslog is not generated on OCSP revocation check
CSCvw06195	ASA traceback cp_midpath_process_thread
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
CSCvw19272	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability
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

Bug ID	Headline
CSCvw23199	ASA/FTD Traceback and reload in Thread Name: Logger
CSCvw24164	heartbeat false positives
CSCvw24556	TCP File transfer (Big File) not properly closed when Flow offload is enabled
CSCvw24700	FPR2100 ASA running 9.12.4.7 fails to boot with ERROR: FIPS Self-Test failure, fipsPostGFSboxKat
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.
CSCvw28894	SFDataCorrelator slow startup and vuln remap due to duplicate entries in vuln tables
CSCvw31254	User with shell set to /bin/false on 8350 sensor causes deployment failure
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
CSCvw33987	ASAv/2100 Smart License failure post upgrade
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
CSCvw41728	Unable to configure syslog via CLI on FTD
CSCvw42999	9.10.1.11 ASA on FPR2110 traceback and reloads randomly
CSCvw43486	ASA/FTD Traceback and reload during PBR configuration change
CSCvw43534	A Null pointer dereference vulnerability exists in Mozilla Network S ...
CSCvw43543	The inflateMark function in inflate.c in zlib 1.2.8 might allow cont ...
CSCvw43586	A vulnerability was found in gnutls versions from 3.5.8 before 3.6.7 ...
CSCvw43615	An issue was discovered in GnuTLS before 3.6.15. A server can trigge ...
CSCvw44122	ASA: "class-default" class-map redirecting non-DNS traffic to DNS inspection engine
CSCvw46702	FTD Cluster secondary units fail to join cluster due to application configuration sync timeout
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
CSCvw49531	Applications are being misclassified after VDB upgrade.

Bug ID	Headline
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
CSCvw52098	Upgrade to 6.4.0.11 fails at 800_post/901_reapply_sensor_policy.pl on standby 2120
CSCvw52609	Cisco ASA and FTD Software Web Services Buffer Overflow Denial of Service Vulnerability
CSCvw53255	FTD/ASA HA: Standby Unit FXOS is still able to forward traffic even after failover due to traceback
CSCvw53427	ASA Fails to process HTTP POST with SAML assertion containing multiple query parameters
CSCvw53796	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerability
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
CSCvw54802	Revocation check fails to move to none after ocsp check fails due to server being unavailable
CSCvw58414	Name of anyconnect custom attribute of type dynamic-split-exclude-domains is changed after reload
CSCvw58865	sftunnel TLS handshake should not include NewSessionTicket
CSCvw59035	Connection issues to directly connected IP from FTD BVI address
CSCvw60177	Standby/Secondary cluster unit might crash in Thread Name: fover_parse and "cluster config sync"
CSCvw62526	ASA traceback and reload on engineering ASA build - 9.12.3.237
CSCvw62820	memcached 1.5.6 or higher update
CSCvw63862	ASA: Random L2TP users cannot access resources due to stale ACL filter entries
CSCvw71766	ASA traceback and reload in Thread: Ikev2 Daemon
CSCvw74495	Application detection fails for FTP service when an unsuccessful login is encountered.
CSCvw74940	ASA traceback in IKE Daemon and reload
CSCvw79208	Incorrect URL normalization when "http://" substring is at a latter stage in the input string
CSCvw79294	sftunnel logging huge number of logs to messages file

Bug ID	Headline
CSCvw81322	FTD running multi-instance mode gets snort GID 3 rules disabled after SRU install and deploy
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
CSCvw84339	Managed device backup fails, for FTD, if hostname exceeds 30 characters
CSCvw85377	URL is not updated in the access policy URL filtering rule
CSCvw87788	ASA traceback and reload webvpn thread
CSCvw89365	ASA/FTD may traceback and reload during certificate changes.
CSCvw93272	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCvw93282	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCvw93513	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCvw95301	ASA traceback and reload with Thread name: ssh when capture was removed
CSCvw96295	Unable to add Route Tracking to static route in FMC 6.4.0.10
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
CSCvx01381	FMC GUI year drop-down list for Manual Time set up only listing until 2020
CSCvx02869	Traceback in Thread Name: Lic TMR
CSCvx03764	Offload rewrite data needs to be fixed for identity nat traffic and clustering environment
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
CSCvx05956	High snort cpu usage while copying navl attribute
CSCvx08734	ASA: default IPv6/IPv4 route tunneled does not work
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

Bug ID	Headline
CSCvx15040	DHCP Proxy Offer is getting drop on the ASA/FTD
CSCvx16202	self referenced object pushed from FMC results in lina crash with error - loop in grp hierarchy
CSCvx17664	ASA may traceback and reload in Thread Name 'webvpn_task'
CSCvx17785	Crash seen consistently by adding/removing acl & entering into route-map command
CSCvx20352	Snort PDTS buffer corruption during upgrade or heavy traffic load
CSCvx26286	IPV6 address was marked as duplicate on both units and ipv6 Traffic was stopped after the failover.
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
CSCvx30314	ASA 9.15.1.7 traceback and reload in ssl midpath
CSCvx41171	Concurrent modification of ACL configuration breaks output of "show running-config" completely
CSCvx42197	ASA EIGRP route stuck after neighbour disconnected
CSCvx44401	FTD/ASA traceback in Thread Name : Unicorn Proxy Thread
CSCvx48490	SSL Decrypted https flow EOF events showing 'Initiator/Responder' Packets as 0
CSCvx50366	Traceback in Thread Name: fover_health_monitoring_thread
CSCvx51860	Failed lookups due to license check when the sensor URL lookup is enabled in 6.4.0.x
CSCvx52122	ASA traceback and reload in SNMP Notify Thread while deleting transparent context
CSCvx59120	COA Received before data tunnel comes up results in tear down of parent session
CSCvx71434	ASA/FTD Traceback and reload in Thread Name: pix_startup_thread due to asa_run_ttyS0 script
CSCvx74035	ASA traceback and reload after run "clear configure all" with multiple ACLs and objects configured
CSCvy09252	Syncd exits repeatedly on secondary FMC in 6.4.0.12-97 FMC-HA pair

Resolved Bugs in Version 6.4.0.11

Table last updated: 2021-01-11

Table 43: Resolved Bugs in Version 6.4.0.11

Bug ID	Headline
CSCvv59788	Lina traceback on 21xx following upgrade from 6.4.0.8 to 6.4.0.9
CSCvw42241	CRL command missing on FP1k

Resolved Bugs in Version 6.4.0.10

Table last updated: 2020-12-08

Table 44: Resolved Bugs in Version 6.4.0.10

Bug ID	Headline
CSCuw95798	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerabilities
CSCuz24872	Original Client IP does not populate for dropped events when inline normalization enabled
CSCvh19161	ASA/FTD traceback and reload in Thread Name: SXP CORE
CSCvi46896	FeedDownloader should not update status to Downloading after download is complete
CSCvj93609	ASA traceback on spin_lock_release_actual
CSCvm69545	Multiple Cisco Products SNORT HTTP Detection Engine File Policy Bypass Vulnerability
CSCvn27043	Hostscan: LastSuccessfulInstallParams can not be detected by Hostscan
CSCvn78076	Firepower:Misleading stats w.r.t "Memory Usage" being displayed under System->Monitoring->Statistics
CSCvo26597	CLI Banner not seen on FTD
CSCvo59683	Large number of stale Objects in EOAttributes table results in high CPU/backup failure
CSCvp45786	Not able to upload the STIX or Flat File Manually under Threat Intelligence Director
CSCvp56719	Cisco FMC and FTD Software sftunnel Pass the Hash Vulnerability
CSCvp56744	Cisco FMC and FTD Software Directory Traversal Vulnerability
CSCvp76950	FTD Traceback and Reload on Lina thread for thread_logger
CSCvp99327	FMC UI Unresponsive After Attempt To Register Smart License With Smart Satellite
CSCvq04619	FTD ftd_sftunnel core is generated after upgrading from 6.4.0

Bug ID	Headline
CSCvq11282	Cisco Firepower Management Center Software Denial of Service Vulnerability
CSCvq20707	Snort rendering block verdict for rules with action of alert.
CSCvq43920	Cisco Firepower Threat Defense Software Hidden Commands Vulnerability
CSCvq46587	After failover, Active unit tcp sessions are not removed when timeout reached
CSCvq53902	Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities
CSCvq63653	FTD may crash when processing fragmented packets
CSCvq95694	Memory leak SSL_ALLOC [ERROR] ssl_alloc.c:113:ssl_alloc_destroy()
CSCvr27584	Estreamer process queries wrong database for rna_policy_rules table and causes excessive logging
CSCvr46901	Analysis Connection Events doesn't show and report all the events in UI
CSCvr49229	FMC high CPU utilization in sfmbservice
CSCvr51955	Estreamer should terminate a connection when not receiving ACKs for a long time
CSCvr53058	Cisco Firepower Threat Defense Software TCP Intercept Bypass Vulnerability
CSCvr55741	FMC shows policies out of date after successful deploy
CSCvr57051	Policy deployment failed with error "Can't use an undefined value as a HASH reference "
CSCvr63851	SSH via External Auth to NGIPS succeeds then closes immediately
CSCvr66798	DNS Application Detector sometimes fails to detect DNS traffic
CSCvr76029	FTD-HA: after restoring FTD-HA backup file, snort process will be down
CSCvr76044	FTD Snort Rule Profiling does not work consistently - log folder is missing
CSCvr79974	Configuration might not replicated if packet loss on the failover Link
CSCvr86016	FMC connections to v3.sds.cisco.com are bypassing proxy
CSCvr94406	Cannot download TAXII feeds in Intelligence Sources v6.2.3 -> v6.4.0.4 on either HTTP or HTTPS
CSCvr99222	NTP configuration is not synchronized to LINA on Multi Instance
CSCvs01422	Lina traceback when changing device mode of FTD
CSCvs05066	Snort file mempool corruption leads to performance degradation and process failure.
CSCvs09533	FP2100: Traceback and reload when processing traffic through more than two inline sets

Bug ID	Headline
CSCvs10748	Cisco ASA Software and FTD Software Web Services Denial of Service Vulnerability
CSCvs21705	admin user is not authorized to access the device routing configuration inside the domain.
CSCvs24215	Firepower Device Manager (FDM) option to disable SSL rekey is not reflected on the config
CSCvs28290	Cisco Firepower Threat Defense Software SSL Input Validation Denial of Service Vulnerabili
CSCvs39253	Firepower 7000 & 8000 cannot sent emails on version 6.4
CSCvs41883	Deployment fails after upgrading to 6.4.0.x if ND policy refs are missing
CSCvs49104	Network Discovery Policy rules are ignored if it uses network groups
CSCvs50137	Same Security Zone used in ACP rule is Not pushed to NGFW rules
CSCvs50931	Policy deployment fails subsequent to SRU
CSCvs56802	Cisco Firepower 2100 Series SSL/TLS Inspection Denial of Service Vulnerability
CSCvs56888	Cisco Firepower Threat Defense Software TCP Flood Denial of Service Vulnerability
CSCvs64510	Deployment failure with message (Can't call method "binip" on unblessed reference)
CSCvs71766	Cisco Firepower Management Center Software Open Redirect Vulnerability
CSCvs74452	SFDatacorrelator and Snort process cores repeatedly while loading malware seed file
CSCvs74586	Firepower FTD transparent does not decode non-ip packets
CSCvs77334	FTD failover due to error "Inspection engine in other unit has failed due to snort and disk failure"
CSCvs82829	Calls fail once anyconnect configuration is added to the site to site VPN tunnel
CSCvs87168	SNORT Fatal Error due to out of range interface ID
CSCvs91270	Inspect Interruption - Error in deployment page.
CSCvt00113	ASA/FTD traceback and reload due to memory leak in SNMP community string
CSCvt01763	Application classification is not retried if a flow is marked brute force failed.
CSCvt02409	Cisco Firepower Threat Defense Software Inline Pair/Passive Mode DoS Vulnerability
CSCvt03598	Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability
CSCvt03794	Policy deployment failure after SRU update on FTD with passive zone
CSCvt04377	When vlan encapsulation is exceeded decoding errors are depleting disk space.

Bug ID	Headline
CSCvt04535	Allow 30-seconds of NFE microengine missing heartbeat faults before engaging error recovery
CSCvt04560	SCTP heartbeats failing across the firewall in Cluster deploymnet.
CSCvt09940	Cisco Firepower 4110 ICMP Flood Denial of Service Vulnerability
CSCvt13445	Cisco ASA and FTD Software FTP Inspection Bypass Vulnerability
CSCvt16642	FMC not sending some audit messages to remote syslog server
CSCvt18028	Cisco ASA and FTD WebVPN CRLF Injection Vulnerability
CSCvt20709	Wrong direction in SSL-injected RESET causes it to exit through wrong interface, causing MAC flap
CSCvt24328	FTD: Traceback and reload related to lina_host_file_open_raw function
CSCvt26067	Active FTP fails when secondary interface is used on FTD
CSCvt28182	sctp-state-bypass is not getting invoked for inline FTD
CSCvt35053	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerabilities
CSCvt35233	Excessive logging from the daq modules process_snort_verdict verdict blacklist
CSCvt35897	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS Vuln
CSCvt39135	snort instances CPU spikes to >90% at low non-SSL traffic with SSL policy applied
CSCvt39349	Registration of device should be allowed as long as deploy status = DEPLOYED or FAILED
CSCvt41333	Dynamic RRI route is not destroyed when IKEv2 tunnel goes down
CSCvt45863	Crypto ring stalls when the length in the ip header doesn't match the packet length
CSCvt48941	FTD Standby unit does not join HA due to "HA state progression failed due to APP SYNC timeout"
CSCvt50263	FMC Unable to fetch VPN troubleshooting logs from WM Model devices
CSCvt50946	Stuck uauth entry rejects AnyConnect user connections despite fix of CSCvi42008
CSCvt52782	ASA traceback Thread name - webvpn_task
CSCvt54267	Cisco Firepower Management Center Software Denial of Service Vulnerability
CSCvt59015	KP IOQ driver. Add defensive parameter and state checks.
CSCvt59253	ASA 9.13.1.7 traceback and reload while processing hostscan data (process name LINA)

Bug ID	Headline
CSCvt60190	Cisco ASA and FTD Web Services File Upload Denial of Service Vulnerability
CSCvt61370	Events may stop coming from a device due to a communication deadlock
CSCvt63556	Local User Password not updating in 6.4.0.9
CSCvt64270	ASA is sending failover interface check control packets with a wrong destination mac address
CSCvt64642	FMC -Deployment Failure- Anyconnect - "Certificate Map" using "DC (Domain Component)" to match cert.
CSCvt66136	6.4.0.9 upgrade from 6.4.0 with CC mode causes httpsd.conf to have an incorrect config
CSCvt66351	NetFlow reporting impossibly large flow bytes
CSCvt66875	AppId caches proxy IP instead of tunneled IP for ultrasurf
CSCvt68131	FTD traceback and reload on thread "IKEv2 Mgd Timer Thread"
CSCvt70322	Cisco ASA Software and FTD Software Web Services Denial of Service Vulnerability
CSCvt73806	FTD traceback and reload on FP2120 LINA Active Box. VPN
CSCvt73808	Handling for longer header length messages going from DAQ to Oct driver
CSCvt75241	Redistribution of VPN advertised static routes fail after reloading the FTD on FPR2100
CSCvt78068	Time sync do not work correctly for FTD on FP1000/1100 series platform
CSCvt79777	duplicate ip addresses in sfipproxy.conf
CSCvt81628	False positives for ultrasurf
CSCvt83121	Cisco ASA and FTD Software OSPFv2 Link-Local Signaling Denial of Service Vulnerability
CSCvt86188	SNMP traps can't be generated via diagnostic interface
CSCvt93142	ASA should allow null sequence encoding in certificates for client authentication.
CSCvt95517	Certificate mapping for AnyConnect on FTD stops working.
CSCvu01039	Traceback: Modifying FTD inline-set tap-mode configuration with active traffic
CSCvu08013	DTLS v1.2 and AES-GCM cipher when used drops a particular size packet frequently.
CSCvu08422	Cisco Firepower Threat Defense Software Multi-Instance Container Escape Vulnerability
CSCvu12684	HKT - Failover time increases with upgrade to 9.8.4.15
CSCvu15801	Cisco ASA and FTD Software SIP Denial of Service Vulnerability

Bug ID	Headline
CSCvu25030	FTD 6.4.0.8 traceback & reload on thread name : CP processing
CSCvu30134	High unmanaged disk usage on /ngfw due to logrotate and missing /var/spool/cron/root directory.
CSCvu38795	FTD firewall unit cannot join the cluster after a traceback due to invalid interface GOID entry
CSCvu42434	ASA: High CPU due to stuck running SSH sessions / Unable to SSH to ASA
CSCvu43355	FTD Lina traceback in datapath due to double free
CSCvu44910	Cisco ASA Software and FTD Software Web Services Cross-Site Scripting Vulnerability
CSCvu46685	Cisco ASA and FTD Software SSL/TLS Session Denial of Service Vulnerability
CSCvu47925	Cisco ASA and FTD IP Fragment Memory Leak Vulnerability
CSCvu48285	ASA configured with TACACS REST API: /cli api fail with "Command authorization failed" message
CSCvu53258	FMC pushes certificate map incorrectly to lina
CSCvu57834	syslog-ng process utilizing 100% CPU
CSCvu59817	Cisco ASA and FTD Software SSL VPN Direct Memory Access Denial of Service Vulnerability
CSCvu60923	Editing the IP in a Radius Server Group object results in unintended values for the IP address
CSCvu63458	FPR2100: Show crash output on show tech does not display outputs from most recent tracebacks
CSCvu66119	URL rules are incorrectly promoted on series 3 resulting in traffic matching the wrong rule.
CSCvu70529	Binary rules (SO rules) are not loaded when snort reloads
CSCvu72658	AnyConnect Connected Client IPs Not Advertised into OSPF Intermittently
CSCvu75581	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvu75594	FTD: Traceback and reload when changing capture buffer options on a already applied capture
CSCvu75615	Cisco ASA Software and FTD Software WebVPN Portal Access Rule Bypass Vulnerability
CSCvu80370	Cisco Firepower Threat Defense Software SNMP Denial of Service Vulnerability
CSCvu82743	Encoded Rule Plugin SID: value, GID: 3 not registered properly. Disabling this rule

Bug ID	Headline
CSCvu83178	Dynamic routing protocols summary route not being replicated to standby
CSCvu83309	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvu91105	High unmanaged disk usage on /ngfw due to large process_stdout.log file
CSCvu98197	HTTPS connections matching 'Do not decrypt' SSL decryption rule may be blocked
CSCvv09944	Lina Traceback during FTD deployment when WCCP config is being pushed
CSCvv13835	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvv13993	Cisco Firepower 1000 Series Bleichenbacher Attack Vulnerability
CSCvv16245	Cisco Firepower Management Center Software Common Access Card Authentication Bypass Vuln
CSCvv33712	Cisco ASA Software Web-Based Management Interface Reflected Cross-Site Scripting Vulnerabi
CSCvv40916	3 min delay caused by AbstractBaseDeploymentValidationHandler.validatePreApply during deploy.
CSCvv44051	Cluster unit traceback on snp_cluster_forward_and_free_packet due to GRE/IPiniP passenger flows
CSCvv50107	FTD Traceback and reload while trying to switch peer on HA
CSCvv52591	DMA memory leak in ctm_hw_malloc_from_pool causing management and VPN connections to fail
CSCvv58604	Reset not sent when traffic matches AC-policy configured with block/reset and SSL inspection
CSCvv70096	Snort 2: Memory Leak in SSL Decrypt & Resign Processing
CSCvv77910	FQDN rules do not work on 1k platforms
CSCvv98534	Failed upgrade does not create audit messages in syslog
CSCvw48033	Changes to SNMPv3 authentication & privacy passwords in SNMP alerts not taking immediate effect

Resolved Bugs in Version 6.4.0.9

Table last updated: 2020-08-18

Table 45: Resolved Bugs in Version 6.4.0.9

Bug ID	Headline
CSCvi34123	ENHancement: Cannot add DNS lists that contain _ at the beginning of the list.

Bug ID	Headline
CSCvj00997	"show open-network-ports" not showing the proper infomration on FP4100 Series
CSCvm77115	Lina Traceback due to invalid TSC values
CSCvo31790	Cisco Firepower Threat Defense Software Management Interface DoS Vulnerability
CSCvo76866	Traceback on 2100 - watchdog
CSCvo80853	Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability
CSCvp57643	FTD/ASA - Cluster/HA - Master/Active unit does not update all the route changes to Slaves/Standby
CSCvp63814	FTD - Inner Flow: Carrier id flow lookup enhancement
CSCvp90847	Refresh Root CAs that SSL uses for resigning in FTD/FMC
CSCvp93468	Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability
CSCvp99930	deployment failure with sftunnel exception while primary active.
CSCvq09357	Unrestricted File Upload in FMC -Backup Management - Upload Backup
CSCvq10500	captures of both CLISH and LINA doesn't work with IPv6 address
CSCvq24258	Increase number of worker for mojo-server on large appliances
CSCvq35440	Upgrade Enhancements to STRAP verification for anyconnect - Cisco VPN session replay vulnerability
CSCvq38889	slib memory manager : mempool mutex vs spinlock selection
CSCvq39344	Firepower managed devices may stop responding to SNMPv3 GET/WALK requests
CSCvq61601	OpenSSL vulnerability CVE-2019-1559 on FTD
CSCvq71351	FMC:Page stuck when editing inline sets
CSCvq79913	ICMP error packets being dropped for Null pdts_info
CSCvq89361	Cisco Firepower 1000 Series SSL/TLS Denial of Service Vulnerability
CSCvq89794	FDM - user downloads not working with LDAPS
CSCvq93572	Unable to add user on FTD using external authentication
CSCvq93669	Cisco Firepower Threat Defense Software SSL/TLS URL Category Bypass Vulnerability
CSCvq96495	Console connection for FPR2100 is disconnected randomly about 20 minutes.
CSCvr07460	ASA traceback and reload related to crypto PKI operation
CSCvr09468	ASA traceback and reload for the CLI "Show nat pool"

Bug ID	Headline
CSCvr13278	PPPoE session not coming up after reload.
CSCvr17735	SFDataCorrelator high CPU during SI update
CSCvr19922	Cluster: BGP route may go in out of sync in some scenarios
CSCvr20449	Policy deployment is reported as successful on the FMC but it is actually failed
CSCvr20893	FTD in HA pair crashes in ids_event_proce process after policy deployment
CSCvr21803	Mac address flap on switch with wrong packet injected on ingress FTD interface
CSCvr30694	FMC : FMC detect HA Sync Failed
CSCvr33586	FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded
CSCvr35125	Packet loss over failover link triggers Split-Brain
CSCvr39556	Segfault in libclamav.so (in the context of SFDataCorrelator)
CSCvr42344	Traceback on snp_policy_based_route_lookup when deleting a rule from access-list configured for PBR
CSCvr49833	Cisco Firepower 2100 Series Security Appliances ARP Denial of Service Vulnerability
CSCvr51998	ASA Static route disappearing from asp table after learning default route via BGP
CSCvr54250	Many user_ip_map files even though no realm is configured
CSCvr54980	FPR2100: Power doesn't turn off after turned off the power button on back of chassis
CSCvr56031	FTD/LINA Traceback and reload observed in thread name: cli_xml_server
CSCvr72665	FMC upgrading to 6.3/6.4 shouldn't remove existing deprecated flexconfig
CSCvr73115	Initial FTD Deploy After Policy Import causes Unused Objects which bloat policy size
CSCvr78166	Deployment failed on FTD with reason "failed to retrieve running configuration"
CSCvr79008	Session processing delay from FMC wastefully querying all Directory Servers normalizing bad username
CSCvr86213	CD is required to ignore Cluster-Msg-Delivery-Confirmation in Cluster Node Release Lina State
CSCvr90768	FTD: Deployment through slow links may fail
CSCvr90965	FTDv Deployment in Azure causes unrecoverable traceback state due to no dns domain-lookup any"
CSCvr92168	Cisco ASA and Cisco FTD Software OSPF Packets Processing Memory Leak Vulnerability

Bug ID	Headline
CSCvr92327	ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'
CSCvr92617	NPE in SecurityIntelligenceEoConvertor causes Lucene indexing failure
CSCvr93978	ASA traceback and reload on Thread DATAPATH-0-2064
CSCvr96527	FMC existing rule error while adding new rule
CSCvs00023	port manager crashes with "shutdown" command from clish CLI
CSCvs01422	Lina traceback when changing device mode of FTD
CSCvs03023	Clustering module needs to skip the hardware clock update to avoid the timeout error and clock jump
CSCvs04067	Not able to access FMC devices with Chrome on Mac after upgrade to Catalina.
CSCvs06043	TunnelClient for CSM_CCMservice on ngfwManager not reading ACK sent from CSM_CCM service on FMC
CSCvs07668	FTD traceback and reload on thread DATAPATH-1-15076 when SIP inspection is enabled
CSCvs07982	ASA TRACEBACK: sctpProcessNextSegment - SCTP_INIIT_CHUNK
CSCvs10443	6.5 CloudEvent code writes config files in a way that 6.4 code does not understand
CSCvs10526	Throttle SSE Attempts on FTDs
CSCvs12288	Snort unexpectedly exits with SSL policy enabled and debug_policy_all
CSCvs15276	ERROR: entry for ::/0 exists when configuring ipv6 icmp
CSCvs15972	Network Performance Degradation when SSL policy is enabled
CSCvs19968	Fix consoled from getting stuck and causing HA FTD policy deployment errors.
CSCvs22503	eStreamer repeatedly exits after "Failed to deserialize policy event"
CSCvs23750	6.4.0.4 FMC WebUI cannot create a Series-3 stack (Cannot select primary device)
CSCvs25607	addition of netmap_num to constraints causes performance degradation
CSCvs28094	Receiving error 403 when editing User Preferences on FP8000 sensors
CSCvs28580	Traceback when processing SSL traffic under heavy load
CSCvs29405	Snort handles traffic as Tagged, when CMD field does not exist in Frame
CSCvs32303	SNMP polling fails on Standby FMC as the snmpd process is in Waiting state
CSCvs33416	Upgrade kernel to cpe:2.3:o:linux:linux_kernel:4.14.158:
CSCvs34844	pm process becomes randomly deadlocked when communicating with hardware.

Bug ID	Headline
CSCvs34854	FMC generates referred interfaces cli delta after access-list cli delta
CSCvs37013	Prevent octeon_init from getting stuck and causing HA FTD policy deployment errors.
CSCvs39388	FTD not sending system syslog messages in CC mode
CSCvs40531	AnyConnect 4.8 is not working on the FPR1000 series
CSCvs45111	WR6 and WR8 commit id update in CCM layer(sprint 75)
CSCvs47201	GET ALL for devicerecords we get "isPartOfContainer": false for devices part of HA and cluster
CSCvs47252	ASA traceback and reload when running command "clear capture /"
CSCvs50459	Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability
CSCvs50952	Upgrade of 6.4.0.4-34 to 6.4.0.6 is deleting Static Route
CSCvs59056	ASA/FTD Tunneled Static Routes are Ignored by Suboptimal Lookup if Float-Conn is Enabled
CSCvs61392	On firepower devices, hardware rules are not updated after successful policy deployment
CSCvs79023	ASA/FTD Traceback in Thread Name: DATAPATH due to DNS inspection
CSCvs80157	ASA Traceback Thread Name: IKE Daemon
CSCvs80536	FP41xx incorrect interface applied in ASA capture
CSCvs91389	FTD Traceback Lina process
CSCvs91869	FPR-1000 Series Random Number Generation Error
CSCvs98634	catalina.<date>.log files can consume all disk space in their partition
CSCvt01397	Deployment is marked as success although LINA config was not pushed
CSCvt10097	logs about SF_Egress_Zone/SF_Ingress_Zone is empty even though security zones have interfaces
CSCvt15163	Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability
CSCvt21041	FTD Traceback in thread 'ctm_ipsec_display_msg'
CSCvt33785	IPSec SAs are not being created for random VPN peers
CSCvt46830	FPR2100 'show crypto accelerator statistics' counters do not track symmetric crypto
CSCvt79988	Policy deployment failure due to snmp configuration after upgrading FMC to 6.6
CSCvt93177	Disable Full Proxy to Light Weight Proxy by Default. (FP2LWP) on FTD Devices

Resolved Bugs in Version 6.4.0.8

Table last updated: 2020-05-26

Table 46: Resolved Bugs in Version 6.4.0.8

Bug ID	Headline
CSCul34972	DHCP Client Proxy doesn't disable after FO units are flipped
CSCva36446	ASA Stops Accepting Anyconnect Sessions/Terminates Connections Right After Successful SSL handshake
CSCvd33448	fireamp.pl using 100% Cpu after restore backup.
CSCvh75756	Duplicate preprocessor keyword: ssl
CSCvk55766	Try to assign devices to platform settings policy list of devices randomly disappear under policy
CSCvm85823	Not able to ssh, ssh_exec: open(pager) error on console
CSCvo74833	High unmanaged disk space on Firepower devices due to untracked files
CSCvp04134	Traceback in HTTP Cli Exec when upgrading to 9.12.1
CSCvp06526	Manage the sfhassd thread CPU affinity to match the Snort CPU affinity
CSCvp39970	/var/opt/CSCOpx/MDC/tomcat/log/stdout.logs writing excessive log messages which may fill the disk
CSCvp70833	ASA/FTD: Twice nat Rule with same service displaying error "ERROR: NAT unable to reserve ports"
CSCvp81083	ASA/Lina Traceback related to TLS/VPN
CSCvq10239	With SSL HW acceleration enabled, FTD TCP Proxy tears down the connection after 3 retransmissions
CSCvq14954	Slave unit having mgmt-only can't join to cluster
CSCvq29969	Firepower Recommendations rule count changes even when not regenerated
CSCvq34160	traceback and reload when establishing ASDM connection to fp1000 series platform
CSCvq43453	Overrides cannot be added for port object if it is used in variable sets in sub domains
CSCvq45105	ENH: Add "Management-access" to FDM flex-config CLI and a CLI-console API issue via SSE/CDO
CSCvq46587	After failover, Active unit tcp sessions are not removed when timeout reached
CSCvq50587	ASA/FTD may traceback and reload in Thread Name 'BGP Router'
CSCvq51284	FPR 2100, low block 9472 causes packet loss through the device.

Bug ID	Headline
CSCvq56257	Cached malware disposition does not always expire as expected
CSCvq67271	Retrieving an specfic rule by ID of a child Access Policy returns a 404 : Not Found status.
CSCvq73534	Cisco ASA Software Kerberos Authentication Bypass Vulnerability
CSCvq73599	Cisco VPN session replay vulnerability : STRAP fix on ASA for SSL(OpenSSL 1.0.2) and SCEP proxy
CSCvq75634	Management interface configuration leads to immediate traceback and reload
CSCvq76198	Traffic interruptions for FreeBSD systems
CSCvq83019	Long processing time to insert policy deploy task if many application filter object used in ACPolicy
CSCvq87797	Multiple context 5585 ASA, transparent context losing mangement interface configuration.
CSCvq88644	Traceback in tcp-proxy
CSCvq95058	IPSEC SA is deleted by failover which is caused by link down
CSCvq95826	DCD Causes Standby to send probes
CSCvq97346	NAT rules deleted from FDM backend after moving NAT rules in UI and deploying
CSCvr04954	Stack Units: Deploy fails after upgrade on different Domain with unable to load NDPolicy obj err
CSCvr10777	ASA Traceback in Ikev2 Daemon
CSCvr11395	Only a subset of devices where deployed from a device group during scheduled deploy
CSCvr13823	Cisco Firepower Threat Defense Software Management Access List Bypass Vulnerability
CSCvr25768	ASA may traceback on display_hole_og
CSCvr25954	FTD/LINA Standby may traceback and reload during logging command replication from Active
CSCvr27445	App-sync failure if unit tries to join HA during policy deployment
CSCvr29638	HA FTD on FPR2110 traceback after deploy ACP from FMC
CSCvr29978	Changing a rule and saving quickly might remove configuration.
CSCvr36687	Overrides cannot be added for network object if it is used in variable sets in sub domains
CSCvr50266	Dual stack ASAv failover triggered by reload issue

Bug ID	Headline
CSCvr53058	AC policy lookup done for SYN+ACK packet when tcp-intercept and a monitor AC policy is configured
CSCvr54054	Mac Rewrite Occurring for Identity Nat Traffic
CSCvr55400	FTD/LINA traceback and reload observed in thread name: cli_xml_server
CSCvr55825	Cisco ASA and FTD Software Path Traversal Vulnerability
CSCvr59927	Deployment failure if SRU install is in progress
CSCvr60111	configurations getting wiped off from standby, while deployment fails on active
CSCvr61239	Information systems must use the POST method over TLS when transmitting
CSCvr61241	Information Systems implementing file upload feature must validate the file size
CSCvr61252	systems must enforce controls that prevent confidential information from being stored within cookie
CSCvr61492	device loading slow, related REST API calls
CSCvr66768	Lina Traceback during FTD deployment when PBR config is being pushed
CSCvr81457	FTD traceback when TLS tracker (tls_trk_sniff_for_tls) attempted to free a block.
CSCvr85295	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote
CSCvs10114	Nested network object group not getting expanded for NAP rules resulting in deployment failure
CSCvs32023	Turn off egress-optimization processing
CSCvs53705	Anyconnect sessions limited incorrectly

Resolved Bugs in Version 6.4.0.7

Table last updated: 2020-02-20

Table 47: Resolved Bugs in Version 6.4.0.7

Bug ID	Headline
CSCvh75756	Duplicate preprocessor keyword: ssl
CSCvr52109	FTD may not match correct Access Control rule following a deploy to multiple devices
CSCvr88123	multi-deploy causes a sudden drop of intrusion events
CSCvr95287	Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability

Bug ID	Headline
CSCvs32023	Turn off egress-optimization processing

Resolved Bugs in Version 6.4.0.6

Note Version 6.4.0.6 was removed from the Cisco Support & Download site on 2019-12-19. If you are running this version, we recommend you upgrade. The bugs listed here are also fixed in Version 6.4.0.7.

Table last updated: 2020-04-16

Table 48: Resolved Bugs in Version 6.4.0.6

Bug ID	Headline
CSCvm48451	Intrusion Event Performance Graphs load blank on 4100 and 9300
CSCvn24920	VPN-Session doesn't get replicated to standby unit when standby device is upgraded to 9.12 image
CSCvn77388	SDI - SUSPENDED servers cause 15sec delay in the completion of a authentication with a good server
CSCvo11280	ASA Enhancement: Generate syslog message once member of the SDI cluster changes state
CSCvo28118	Traceback in VPN Clustering HA timer thread when member tries to join the cluster
CSCvo43795	OSPF Process ID doesnot change even after clearing OSPF process
CSCvo73250	ENH: ACE details for warning "found duplicate element"
CSCvo74397	ENH: Add process information to "Command Ignored, configuration in progress..."
CSCvo88762	FTD inline/transparent sends packets back through the ingress interface
CSCvp04186	cts import-pac tftp: syntax does not work
CSCvp12582	Option to display port number on access-list instead of well known port name on ASA
CSCvp23109	ASA HA IKEv2 generic RA - AnyConnect Premium All In Use incorrect on standby
CSCvp33341	Cisco ASA and Firepower Threat Defense Software WebVPN Cross-Site Scripting Vulnerability
CSCvp55901	LINA traceback on ASA in HA Active Unit repeatedly
CSCvp55941	FILE RESUME BLOCK being randomly thrown causing access issues on files from SMB share.
CSCvp56805	"Too much data during a write" messages flooding communication channel

Bug ID	Headline
CSCvp76944	Cisco ASA and FTD Software WebVPN CPU Denial of Service Vulnerability
CSCvp85736	Cluster master reload cause ping failure to the Management virtual IP
CSCvp87623	Upload an update gives "update request entity too large" error when using CAC(HTTPS Client Certs)
CSCvq05113	ASA failover LANTEST messages are sent on first 10 interfaces in the configuration.
CSCvq09093	VPN Pre-deploy validations takes around 20 seconds for each device
CSCvq17263	FTD LINA traceback at DATAPATH-8-15821
CSCvq24494	FP2100 - Flow oversubscribing ring/CPU core causing disruption to working flows on FP2100 platforms
CSCvq28250	ENH: ASA Cluster debug for syn cookie issues
CSCvq36042	lost heartbeat causing reload
CSCvq39317	ASA is unable to verify the file integrity
CSCvq40943	FTD 4150 VPN s2s deployment failure with 6K spokes
CSCvq44665	FTD/ASA : Traceback in Datapath with assert snp_tcp_intercept_assert_disabled
CSCvq45000	Policy deployment to FP 8000 sensor is failing when NAT is configured
CSCvq46443	Cisco Firepower Management Center Stored Cross-Site Scripting Vulnerability
CSCvq53915	Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities
CSCvq54667	SSL VPN may not be able to establish due to SSL negotiation issue
CSCvq57591	When only IP communication is disrupted on failover link LANTEST msg is not sent on data interfaces
CSCvq59702	Connection events stop coming from device after lost handshake message
CSCvq60131	ASA traceback observed when moving EZVPN spokes to the device.
CSCvq63024	Dual stacked ASAv manual failover issues
CSCvq64742	ASA5515-K9 standby traceback in Thread Name ssh
CSCvq65241	ASA Traceback on Saleen in Thread Name: IPv6 IDB
CSCvq65542	Disable asp load-balance per-packet functionality from fp2100 until all bugs fixed
CSCvq69111	Traceback: Cluster unit lina assertion in thread name:Cluster controller
CSCvq70468	ASA cluster does not flush OSPF routes
CSCvq70485	Slow "securityzones" REST API

Bug ID	Headline
CSCvq70775	FPR2100 FTD Standby unit leaking 9K blocks
CSCvq71217	High Disk Utilization due to mysql-server.err failing to rotate after CSCvn30118
CSCvq75743	ASA:BGP recursive route lookup for destination 3 hop away is failing.
CSCvq76533	F_RNA_EVENT_LIMIT for MC4000 should be 20 million
CSCvq77547	Connections fail to replicate in failover due to failover descriptor mis-match on port-channels
CSCvq80318	ASA generates incorrect error message about PCI cfg space when enumerating Internal-Data0/1
CSCvq81516	VPN events between 12 and 1 PM UTC are not displayed on the FMC
CSCvq83168	DNS lookup using mgmt VRF not possible because FMC doesn't allow interface after server address
CSCvq87703	Active device is not reporting correct peer state.
CSCvq91645	Flow Offload Hashing Change of Behavior
CSCvq92126	ASA traceback in Thread IPsec Message Handler
CSCvq94729	Deployment rollback causes momentary traffic drop when error in a LINA ONLY section of delta cli
CSCvr00892	where clause not working for external data base access
CSCvr07421	Policy deployment fails with 400+ interfaces in security zone due to incorrect formation of deployDB

Resolved Bugs in Version 6.4.0.5

Table last updated: 2020-04-16

Table 49: Resolved Bugs in Version 6.4.0.5

Bug ID	Headline
CSCvh73096	Read sAMAccountUserName from ISE when it is available
CSCvo66546	Firepower frequent traceback and restart on SFDataCorrelator process
CSCvp95663	InlineResult for IPS event missing metadata "Would have blocked"
CSCvp97061	URL Filtering Shows All URLs as Uncategorized
CSCvq32678	Upgrade anomalies result in policy deploy failure: NGFW_UPGRADE is missing in map file

Bug ID	Headline
CSCvq32681	Fail to Wire configuration disabled for multiple interface-pair inline-sets during FTD upgrades
CSCvq39083	Security Intelligence does not drop HTTPS connections to blacklisted URLs when SSL policy is enabled
CSCvq41936	Must disable and then re-enable SNMP in FMC UI after adding new user
CSCvq44594	Flooding of logs with message "Unknown HPQ rule key"
CSCvq46804	Unable to login with AD username containing upper case RADIUS
CSCvq46918	SNMPv3 User(s) deleted after upgrade
CSCvq54242	Warning "There is an empty group in the source networks" in SSL policy
CSCvq56138	User login fails into FMC GUI for LDAP user if the password contains SPACE in the string
CSCvq56462	File policy not inspecting some malware document (.doc) and Adobe flash (.swf) files.
CSCvq65092	Slow device related REST API calls
CSCvq66217	FMT | MTU value not within the permissible range
CSCvr23858	Policy deployment from FMC to FTD fails (or takes more time) due to domain_snapshot_timeout (20m)

Resolved Bugs in Version 6.4.0.4

Table last updated: 2020-04-15

Table 50: Resolved Bugs in Version 6.4.0.4

Bug ID	Headline
CSCvf83160	Traceback on Thread Name: DATAPATH-2-1785
CSCvg29468	Reduce opportunities for false positive general microengine fault
CSCvh13869	ASA IKEv2 unable to open aaa session: session limit [2048] reached
CSCvj61580	ASA traceback with Thread: DATAPATH-8-2035
CSCvk22322	ASA Traceback (watchdog timeout) when syncing config from active unit (inc. cachefs_umount)
CSCvk26612	"default Keyring's certificate is invalid, reason: expired" health alert
CSCvk29685	Traceback in DATAPATH on ASA
CSCvm36362	Route tracking failure

Bug ID	Headline
CSCvm39901	ENH: ASA - support for more than 4 servers in multiple mode.
CSCvm40288	Port-Channel issues on HA link
CSCvm64400	IKEv2: IKEv2-PROTO-2: Failed to allocate PSH from platform
CSCvm68648	Update needed for CVE-2016-8858 (OpenSSH) on Firepower software
CSCvm82966	Linux Kernel 4.14 Vulnerabilities
CSCvn76875	Graceful Restart BGP does not work intermittently
CSCvn78593	Control-plane ACL doesn't work correctly on FTD
CSCvn78870	ASA Multicontext traceback and reload due to allocate-interface out of range command
CSCvo03700	ASA may traceback in thread logger when cluster is enabled on slave unit
CSCvo14961	ASA may traceback and reload while waiting for "dns_cache_timer" process to finish.
CSCvo29989	Cisco FirePower Threat Defense Information Disclosure Vulnerability
CSCvo31695	Traceback in threadname DATAPATH-0-1668 while freeing memory block
CSCvo45755	ASA SCP transfer to box stall mid-transfer
CSCvo47390	ASA traceback in thread SSH
CSCvo48838	Lina does not properly report the error for configuration line that is too long
CSCvo51265	Cisco Adaptive Security Appliance Software Secure Copy Denial of Service Vulnerability
CSCvo55809	ASA App stuck in installing state on few images
CSCvo65741	ASA: BGP routes is cleared on routing table after failover occur and bgp routes are changed
CSCvo66534	Traceback and reload citing Datapath as affected thread
CSCvo67421	ASA: EzVPN Client does not work after software upgrade to specific releases
CSCvo68184	management-only of diagnostic I/F on secondary FTD get disappeared
CSCvo74350	ASA may traceback and reload. Potentially related to WebVPN traffic
CSCvo74625	6.4.0 - IPv6 routing doesn't work for WM and KP when mgmt gateway configure as data-interfaces
CSCvo77796	Slow deployment due to slower IntrusionPolicy step in global snapshot population
CSCvo78789	Cisco Adaptive Security Appliance Smart Tunnel Vulnerabilities
CSCvo80501	Standby Firewall reloads with a traceback upon doing a manual failover

Bug ID	Headline
CSCvo83169	Cisco ASA Software and FTD Software FTP Inspection Denial of Service Vulnerability
CSCvo87930	HTTP with ipv6 using w3m is failing
CSCvo87985	ASA sends password in plain text for "copy" command
CSCvo90153	ASA unable to authenticate users with special characters via https
CSCvo90998	LACPDUs should not be sent to snort for inline-set interfaces
CSCvo97979	The delay command in interface configuration is modified after rebooted
CSCvp12052	ASA may traceback and reload. suspecting webvpn related
CSCvp14674	ASAv Azure: Route table BGP propagation setting reset when ASAv fails over
CSCvp19910	Unable to process gtpv1 identification req message for header TEID : 0
CSCvp19998	ASA drops GTPV1 SGSN Context Req message with header TEID:0
CSCvp23137	ASA/FTD generates syslog for missing SSD 2: /dev/sdb is present. Status: Inoperable.
CSCvp30447	Syslog alerts are not sent to server when Global Rule Thresholding is disabled on Intrusion Policy
CSCvp32617	"established tcp" does not work post 9.6.2
CSCvp35141	ASA sends invalid redirect response for POST request
CSCvp35384	IKEv2 RA Generic client - stuck outgoing asp table entry - traffic encrypted with stale SPI
CSCvp38530	Unable to configure more than 100 aaa-server group limit reached
CSCvp42275	CCM Infrastructure Update for WR8
CSCvp45882	Cisco ASA Software and FTD Software SIP Inspection Denial of Service Vulnerability
CSCvp46341	Fail-to-Wire (FTW) Ports fail to recover on 2100 Firepower platforms.
CSCvp49576	FTD traceback due to watchdog on xlate_detach
CSCvp49790	Cisco ASA Software and FTD Software OSPF LSA Processing Denial of Service Vulnerability
CSCvp54261	Audit syslog for SFR module/7000/8000 devices uses TCP instead of UDP for syslog communication
CSCvp55880	Fail-Closed FTD passes packets through on Snort processes down
CSCvp59864	IP Address stuck in local pool and showing as "In Use" even when the AnyConnect client disconnects
CSCvp63068	Thread Name: CP DP SFR Event Processing traceback

Bug ID	Headline
CSCvp65134	ASA does not respond to DHCP request packet on BVI interface
CSCvp67257	USGv6 Failures From Kernel Upgrade [3.10 to 4.14]
CSCvp70020	After reboot, "ssh version 1 2" added to running-config
CSCvp70699	ASA Failover split brain (both units active) after rebooting a Firepower chassis
CSCvp71180	MCA+AAA+OTP with RADIUS challenge fails to send aggauth handle in challenge
CSCvp72244	Evaluate Cisco 8000 series for CVE-2019-11815
CSCvp72412	Timezone displayed in SYSLOG messages but not in the logging buffer
CSCvp73555	rna_networks is empty after Network Discovery deployment.
CSCvp79157	FTD/Firepower Policy deployment fails when running simultaneous deployment to many devices.
CSCvp80775	Unsupported runtime JavaScript exception handling in the client side WebVPN rewriter
CSCvp83687	Firepower: Network file trajectory graph does not load
CSCvp84546	ASA 9.9.2 Clientless WebVPN - HTML entities are incorrectly decoded when processing HTML
CSCvq00005	FTD Traceback and Reload on LINA Caused by SSL Decryption DND Preservation
CSCvq00675	Linux Kernel sas_expander.c Race Condition Arbitrary Code Execution ...
CSCvq06790	Snort processes dump core with memory corruption on Series 3 devices
CSCvq08684	Policy Deployment Failure due to Special Characters & encoding
CSCvq08767	Deployment failing in snort validation- SMTP: Could not allocate SMTP mime mempool
CSCvq11513	Traceback: "saml identity-provider" command will crash multi-context ASAs
CSCvq12411	ASA may traceback due to SCTP traffic despite fix CSCvj98964
CSCvq13442	When deleting context the ssh key-exchange goes to Default GLOBALLY!
CSCvq16123	Firepower Dynamic Snort Rules are Disabled After a Deployment Involving a Snort Reload
CSCvq19525	Evaluation of sfims for TCP_SACK
CSCvq21607	"ssl trust-point" command will be removed when restoring backup via CLI
CSCvq24134	ASA IKEv2 - ASA sends additional delete message after initiating a phase 2 rekey
CSCvq25626	Watchdog on ASAv when logging to buffer

Bug ID	Headline
CSCvq25912	Correlation rule alerting is not working in 6.4.0
CSCvq26794	GTP response messages with non existent cause are getting dropped with error message TID is 0
CSCvq27010	Memory leak observed when ASA-SFR dataplane communication flaps
CSCvq37902	TID fails to add source as a URL - Flat file
CSCvq39828	SFDC crashes inserting into packet_log table after upgrading to 6.4.0
CSCvq50314	Failed SSH Login attempts not being exported via syslog
CSCvq57710	Firepower Primary Detection Engine process might terminated after Manager upgrade
CSCvq61651	URL DB download failure alerts on FMC; new URL DB updates not taking effect on FMC/FDM
CSCvq86553	Traffic not matching expected ACP rule after updating to 6.4.0
CSCvq97301	Fatal Error message in FMC GUI when upgrading 5525 from 6.4.0-102 > 6.4.0.4-31 but upgrade completes

Resolved Bugs in Version 6.4.0.3

Table last updated: 2020-04-16

Table 51: Resolved Bugs in Version 6.4.0.3

Bug ID	Headline
CSCve24102	GUI should allow max 256 addresses per DHCP pool
CSCvo68448	ASA report SFR module as 'Unresponsive' after reloading ASA module on 5585 platform
CSCvp01542	FMC 6.3 Multitenancy/Domain LDAPS User/Group Download Failure Due to Certificate Location
CSCvp10132	AnyConnect connections fail with TCP connection limit exceeded error
CSCvp23579	Network FIle Trajectory page takes 90 seconds to load each time
CSCvp25570	Unable to create RAVPN Conn-Profile if group-policy attr and FQDN are edited in the same wizard flow
CSCvp32659	FDM-HA formation has failed after upgrading to 6.3.0.3-69
CSCvp33052	Firepower 8000 interfaces might flap due to unhandled resource temporarily unavailable issue
CSCvp37779	FTD show tech from troubleshooting files incomplete

Bug ID	Headline
CSCvp46173	Changes in interface-group or interface-zone in subdomain overwrites Global domain.
CSCvp56910	Help pages always show up in English
CSCvp58028	natd thread of nfm_exceptiond uses about 90% to 100% CPU time
CSCvp66559	Deploy fails on FTD HA due to exception when parsing big xml response
CSCvp72601	FMC UI: VPN Hub and Spoke topology slow loading
CSCvp72770	BCDB file copy from FMC on to vFTD getting truncated, vFTD running on Azure platform.
CSCvp75594	Deployment failure after upgrade to 6.4 in ASA5500-X running FTD
CSCvp94588	HTTP blacklist - blacklist rules are not removed from sensor when unassigned and deplyed from FMC
CSCvp97799	Policy deploy failure 6.5.0-1148 post upgrade with CC mode with openSSL call during SSL pol Export
CSCvp97916	Executing 'failover' twice on active unit, clears interface configuration on standby unit
CSCvp98066	On reset CD not clearing its flags[parseFailoverReqIssued] which prevents further node join attempts
CSCvq07914	FMC 6.4.0 - Policy deployment failure - Duplicate domain entries in domains.conf
CSCvq14586	600_schema/100_update_database.sh should return error if database update fails

Resolved Bugs in Version 6.4.0.2

Table last updated: 2020-04-16

Table 52: Resolved Bugs in Version 6.4.0.2

Bug ID	Headline
CSCuz85967	New added management interface does not have "management-only" configuration
CSCvi63474	Unable to edit the system policy of a SFR module via ASDM after upgrading to 6.2.2
CSCvk06386	FTD Files are Allowed Through Multiple Pre-existing Connections Despite the File Policy Verdict
CSCvk14242	sfstunnel process in FTD is holding large cloud db files that are already deleted
CSCvm70274	tcp proxy: ASA traceback on DATAPATH
CSCvn07452	712x devices become unstable when switching inline set from TAP to inline
CSCvn12381	4140 Multi-Instance Not Load-Balancing Correctly with 4 Instances

Bug ID	Headline
CSCvn34246	Loading AC policy editor takes too long, needs loading indicator
CSCvn45750	FMC Audit Logs will only display Admin and System as owners when deploying to 3D devices -GUI/SYSLOG
CSCvn46390	Lina msglayer performance improvements: port Hotfix BO
CSCvn57284	Unsupported EC curve x25519 on FTD
CSCvn74112	FTDv does not have configuration on initial bringup with mix of vmxnet3 and ixgbevf interfaces
CSCvn75368	IPsec VPN goes down intermittently during a re-key
CSCvn86777	Deployment on FTD with low memory results on interface nameif to be removed - finetune mmap thresh
CSCvo02097	Upgrading ASA cluster to 9.10.1.7 cause traceback
CSCvo17775	EIGRP breaks when new sub-interface is added and "mac-address auto" is enabled
CSCvo23366	Deploy failed because adaptive profiling config file corrupt
CSCvo24145	ids_event_alerter high memory usage due to large firewall_rule_cache table
CSCvo33348	Mysql traffic on non standard port is not correctly classified
CSCvo33851	ngfwManager doesn't start if ngfw.properties is empty
CSCvo41572	FMC shows connection events with packet count as 0
CSCvo45209	FTD-CLUSTER:Adding new unit in cluster can cause traffic drop
CSCvo45799	Cisco Firepower Threat Defense Software Command Injection Vulnerability
CSCvo47562	VPN sessions failing due to PKI handles not freed during rekeys
CSCvo50168	Audit Log Settings Failing Leading to being unable to edit System Settings
CSCvo56836	SCALE: with 500+ devices, UMS causes the UI to hang, especially during deploy
CSCvo58847	Enhancement to address high IKE CPU seen due to tunnel replace scenario
CSCvo60580	ASA traceback and reloads when issuing "show inventory" command
CSCvo60862	Internal Error when editing an Access Control Policy
CSCvo62031	ASA Traceback and reload while running IKE Debug
CSCvo62060	Telemetry not sent when FMC managing lots of devices
CSCvo66920	Enhancement: add counter for Duplicate remote proxy

Bug ID	Headline
CSCvo70545	Cisco Firepower Detection Engine RTF/RAR Malware and File Policy Bypass Vulnerabilities
CSCvo72179	For SMB, remote storage configuration should allow configuring version string with dot(.)
CSCvo72462	Do not decrypt rule causes traffic interruptions.
CSCvo74745	cloud agent core after generating a large number of continuous URL lookups (>30M)
CSCvo83194	Cisco Firepower Threat Defense Software Multi-Instance Container Escape Vulnerabilities
CSCvo86038	Simultaneous FINs on flow-offloaded flows lead to stale conns
CSCvo88188	SSL rules with App-ID conditions can limit decryption capability
CSCvo88306	NAT rules can get applied in the wrong order when you have duplicate rules
CSCvo89224	FMC times out after 10 mins to fetch device list for deployment
CSCvo90550	Firepower Recommendations does not enable IPS rules that are GID 3
CSCvo90805	Cisco Firepower Management Center RSS Cross-Site Scripting Vulnerabilities
CSCvp03498	Health monitoring options for ISE connectivity on FMC.
CSCvp07143	DTLS 1.2 and AnyConnect oMTU
CSCvp14576	ENH - Option to configure Port Block Allocation on FTD
CSCvp16536	ASA traceback and reload observed in Datapath due to SIP inspection.
CSCvp18878	ASA: Watchdog traceback in Datapath
CSCvp19549	FTD lina cored with Thread name: cli_xml_server
CSCvp21837	Allow FTDs to perform URL lookups directly without having to go through the FMC Pre 6.5.0
CSCvp24728	Random SGT tags added by FTD
CSCvp24787	(snort)File is not getting detected when going over HTTPS (SSL Resign)
CSCvp25583	FTD sets automatically metric 0 when we redistribute OSPF into BGP via FMC GUI.
CSCvp27263	Multiple ClamAV Vulnerabilities For Cisco Firepower Management Center for pre 6.5.0
CSCvp29692	FIPS mode gets disabled after rollback from a failed policy deploy
CSCvp35359	FMC-ISE integration doesn't work if explicit UPN doesn't match implicit UPN

Bug ID	Headline
CSCvp36425	Cisco ASA & FTD Software Cryptographic TLS and SSL Driver Denial of Service Vulnerability
CSCvp43474	REST API query /api/fmc_config/v1/domain/UUID/devices/devicerecords fails
CSCvp43536	On upgraded FMC Device FXOS devices are shown dirty even after successful deployment.
CSCvp54634	Wrong rule matched when using ambiguous DND
CSCvp58310	integrate pxgrid capability, connection hang, curl hang issues
CSCvp66222	Cisco Firepower Detection Engine RTF/RAR Malware and File Policy Bypass Vulnerabilities
CSCvp67392	ASA/FTD HA Data Interface Heartbeat dropped due to Reverse Path Check
CSCvp75098	Misleading deploy Warning message when Flex Config policy is being deployed
CSCvp78197	Policy deployment remove and add back ospf neighbor
CSCvp81967	Slowness in loading Device Management page on FMC when there are over 500 managed devices
CSCvp82945	NAT policy apply failing with error duplicate
CSCvp96934	Ensure Error Message with Dup NATs Is Clear and Actionable
CSCvq07573	FMC Global Pre-deployment Phase takes longer after upgrade to 6.4
CSCvq09209	Policy deployment failed with error snort validation failed (Bad value specified for memcap)
CSCvq34224	Firepower Primary Detection Engine process terminated after Manager upgrade

Resolved Bugs in Version 6.4.0.1

Table last updated: 2019-05-15

Table 53: Resolved Bugs in Version 6.4.0.1

Bug ID	Headline
CSCvh51853	Random packet drops by session preprocessor
CSCvp59960	Network discovery not working with network groups containing literals - user or Cisco created.

Resolved Bugs in Version 6.4.0

Table last updated: 2020-04-21

Table 54: Resolved Bugs in Version 6.4.0

Bug ID	Headline
CSCuz85967	New added management interface does not have "management-only" configuration
CSCvc56570	Policy deployment failure causes momentary traffic drop and established connection failure
CSCvf83504	SYS_FW_INTERFACE_NAME_LIST and SYS_FW_NON_INLINE_INTERFACE_NAME_LIST not recognizing subinterface
CSCvg11366	Make sure cleanup happens after calls to for File::Temp when used by MOJO, Syncd.pl, etc
CSCvg74603	eStreamer archive events are not pruned correctly by diskmanager
CSCvh93045	FMC should clean database itself if same device(same SN) with different ip try to get registered
CSCvi01404	ssl inspection policy may cause sites using ECDSA signed certificates to fail
CSCvi16039	Firepower Management Center not accepting various characters in SNMPv3 password
CSCvi16074	Firepower Management Center misleading errors when entering SNMPv3 passwords
CSCvi25965	Sybase upgrade: After SRU Install, zombie defunct process causes policy deployment failure
CSCvi32569	Excessive logging in mysql-server.err log causes huge log files in FTD
CSCvi49522	POST or PUT rule with application tag, search, or category filter -> Unable to access ACP rules GUI
CSCvi71622	Traceback in DATAPATH on standby FTD
CSCvi81022	Cisco Firepower Threat Defense SSL/TLS Policy Bypass Vulnerability
CSCvi89202	disk space check omitted when upgrade is resumed
CSCvi93680	User should be alerted that firstboot failed
CSCvj08826	FMC: ibdata1 file is growing to large in size (From 300Gb to 2.4TB+ seen)
CSCvj13960	seeing high CPU when SNMP is enabled
CSCvj27949	FMC does not use correct time offset in summer.
CSCvj39253	File policy is blocking xlsm when inspect archive option is enabled
CSCvj50451	Unable to add a network object 0.0.0.0/32 on FMC

Bug ID	Headline
CSCvj57511	ASDM: Disabled Rule state of layer policy is reverted to inherit after committing the changes
CSCvj70886	API-Explorer needs to support 4096-bit certificates
CSCvj81798	OOM when deployed an access rule with 10 src/10 dest n/w, 10 src/10 dest ports, 10 subintf in a zone
CSCvk20209	External Auth for FMC not working for RADIUS object through ISE.
CSCvk20381	Traceback loop seen on fresh ASAv Azure, KVM and VMWare deployments
CSCvk23653	ip pool is getting negated before it is dereferenced from group policy
CSCvk29558	FTD VPN : Disabling S2S option "Certificate OU field to determine the tunnel" won't take effect
CSCvk33503	Flexconfig ethertype command is not parsed which results in deployment failure
CSCvk34648	Firepower 2100 tunnel flap at data rekey with high throughput IPsec VPN traffic
CSCvk43854	Cisco Firepower Threat Defense Detection Engine Policy Bypass Vulnerability
CSCvk45941	Need better logging for deploy failure - bad character in VPN policy
CSCvk56984	Multiple Vulnerabilities in tomcat
CSCvm04150	All health modules were marked as deleted in health module table after first boot script ran twice
CSCvm05768	Required fields in https server certificate
CSCvm41983	Policy Deployment page final 'deploy' click takes it back to 'Deploy' window.
CSCvm50153	FMC - Deployment failure due to VPN split-tunnel extended ACL using manually entered ip range
CSCvm54029	6.4.0 - invalid IPV6 RA_VPN sessions are processed by ADI and put into user_ip_map files
CSCvm54062	Action-queue task got stuck after a file copy from active to standby.
CSCvm60056	After downloading custom DNS security intelligence feed, the webGUI timestamp is not updated
CSCvm62846	restore of TID | Config only backup failed:
CSCvm63199	newly configured interface's are not showing for capture command
CSCvm68999	Deployment failure on KP - Detection reconfiguration failed
CSCvm70274	tcp proxy: ASA traceback on DATAPATH
CSCvm72980	FDM :- FTD does not send complete chain in SSL handshake

Bug ID	Headline
CSCvm78028	Unable to add 2 filters with same 'Traffic direction' & 'Filter on Route Type' in RIP configuration
CSCvm84459	bad call_home_ca file prevents smart licensing registration
CSCvm85453	FMC HA : SNMP traps not being sent from New Active FMC post the failover
CSCvm86008	Policy Deployment: Delta config doesn't get copied to running config, LINA config remains unchanged
CSCvm88294	High Disk utilization due to partition force drain not occurring
CSCvm90290	ImageMagick package in Firepower software may be outdated
CSCvm92210	Unable to deploy anyconnect Group-Url in FTD if it contains user defined port number
CSCvm96642	DSA certificates are currently not supported for Active Authentication.
CSCvn00312	Deploy getting stuck when trying to display errors and warnings
CSCvn12373	Policy deploy fails on rna_attribute dup key for FMC HA
CSCvn13880	Unit traceback at Thread PIM IPv4 or IGMP IPv4 due to timer events when multicast routing is enabled
CSCvn14276	'arp permit-nonconnected' is not supported by FlexConfig
CSCvn14511	FMC does not accept curly brace (e.g. "{") in SNMP user authentication configuration
CSCvn19609	Flex Object editor might introduce unexpected line breaks resulting in poliocy deployment failure
CSCvn23926	OSPFv3 interface authentication SPI must be unique for each interface of a device
CSCvn24920	VPN-Session doesn't get replicated to standby unit when standby device is upgraded to 9.12 image
CSCvn29101	Cisco Firepower Management Center MySQL Unix Millennium 2028 Date Vulnerability
CSCvn31882	Flex configuration statements gets duplicated if Deployment mode is set to "Everytime"
CSCvn36022	FMC Object Management to provide information about every ACP/Device that uses a given object
CSCvn38101	no ui check for nat overlap with standby address
CSCvn39960	Configuring protected networks for hub and spoke VPN in FMC doesn't take affect on lina CLI.
CSCvn44222	6.3.0-79: HA upgrade/deployment fails from from missing RAVPN diskfiles on secondary
CSCvn46358	overloading of the lina msglyr infra due to the sending of VPN status messages

Bug ID	Headline
CSCvn47504	VMware balloon driver should be disabled for 6.x
CSCvn48907	Cisco Firepower Management Center Persistent Cross-Site Scripting Vulnerability
CSCvn58125	Reports generated in blank filtering on dashbord
CSCvn67084	Failed to delete local manager during adding FMC as manager
CSCvn71592	After FMC reboot, intrusion events generated by Snort are not sent to FMC and show up in webGUI
CSCvn75713	CVE Nmap Version on FMC
CSCvn75722	CVE Nmap Version on FMC
CSCvn75729	CVE Nmap Version on FMC
CSCvn81898	Device name doesn't exist in a syslog message if syslog alerting for connection events is configured
CSCvn82823	FTD HA Interface Monitoring change does not take effect, when interface nameif is case sensitive
CSCvn82891	Multiple Vulnerabilities in httpd
CSCvn85761	FMC Does not allow to create a secret key using special characters in object name
CSCvn91775	FMC GUI should not allow to create a certificate map with numeric name in Objects > VPN > Cert Maps
CSCvo04444	Ikev2 tunnel creation fails
CSCvo06383	FMC upgrade from version 6.0.1 to 6.1.0 fails due to database being down
CSCvo19433	Flexconfig document should specify the extent of effect from incorrect config
CSCvo19666	28 Core instance is achieving 20% lower performance than expected
CSCvo20847	Active FTP fails through Cluster due to xlate allocation corruption upon sync
CSCvo24624	Upgrade failure from 6.3.0 -> 6.4.0-1299
CSCvo31831	Deleting a base policy does not delete the EOs of child policies
CSCvo35129	Need correction in epoll_wait event handling
CSCvo35283	Cluster unit getting crash for unit addition/removal for HTTP/POP3 traffic over GRE
CSCvo38051	segfault in ctm_ipsec_pfkey_parse_msg at ctm_ipsec_pfkey.c:602
CSCvo42884	Cannot make Site-to-site VPN changes on FTD after upgrading to 6.3
CSCvo45675	FMC upgrade process should check configuration that would be invalid after upgrade
CSCvo63168	temp_id leak if Sybase connection fails

Bug ID	Headline
CSCvo63232	UIMP not updating users from a realm that resides in a child domain.
CSCvo65521	Restoring backup fails due to incorrect TID directory
CSCvo66575	pxGrid connection broken with ISE 2.6 and ISE 2.4p6 and 2.3p6
CSCvo70866	SGT tag shows untagged in server packet for every client packet with SGT tag with some value
CSCvo72232	ERR_SSL_BAD_RECORD_MAC_ALERT or SSL_ERROR_BAD_MAC_ALERT in the browser
CSCvo72238	FMC backup fails when FTD cluster is managed in domain and sub-domain AC Policy is assigned to it
CSCvo72659	Edits made to existing correlation rule do not take effect.
CSCvo74397	ENH: Add process information to "Command Ignored, configuration in progress..."
CSCvo74765	FDM policy deployment failure due to Lina Response timed out after 10000 milliseconds
CSCvo76866	Traceback on 2100 - watchdog
CSCvo80725	vFTD 6.4 fails to establish OSPF adjacency due to "ERROR: ip_multicast_ctl failed to get channel"
CSCvo81073	Unable to load Device Management page or upgrade FMC due to missing NGFWHA EO
CSCvo83574	Device goes into a bad state when switching the inline set from TAP mode
CSCvo86038	Simultaneous FINs on flow-offloaded flows lead to stale conns
CSCvo94486	Snort process exits while processing Security Intelligence.
CSCvp04134	Traceback in HTTP Cli Exec when upgrading to 9.12.1
CSCvp12239	KP - Secondary/Standby device going Active after upgrade to patch 6.3.0.3-58
CSCvp25581	in FMC-HA user_group_map entries are wiped out in split-brain
CSCvp25782	EventHandler core while pruning metadata cache
CSCvp45149	Traceback while Reverting the primary system as active
CSCvp48453	[DOC] Restoring Version 6.x+ Firepower 7000/8000 device from backup does not reset the mgmt IP
CSCvp66488	FirePower sent unexpected SNMP trap based off of a snort rule
CSCvp67392	ASA/FTD HA Data Interface Heartbeat dropped due to Reverse Path Check

Bug ID	Headline
CSCvp70833	ASA/FTD: Twice nat Rule with same service displaying error "ERROR: NAT unable to reserve ports"
CSCvq12070	Not able to establish more than 2 simultaneous ASDM sessions
CSCvq24494	FP2100 - Flow oversubscribing ring/CPU core causing disruption to working flows on FP2100 platforms
CSCvq32250	BGP Next Hop Incorrectly Programmed in HA Active/Standby Pair
CSCvq88644	Traceback in tcp-proxy
CSCvr06515	Access-control-config hit counter not incrementing
CSCvr10777	ASA Traceback in Ikev2 Daemon
CSCvr28532	policy deployment failure due to Snort validation failure
CSCvr35956	Block double-free when combining ServerKeyExchange and ClientKeyExchange fails causes lina traceback
CSCvr45752	FTD HA: deployment fails if one of the units is unhealthy (FDM)
CSCvr51998	ASA Static route disappearing from asp table after learning default route via BGP
CSCvr52410	After registering a new FTD, the subsequent policy deploy fails
CSCvr55400	FTD/LINA traceback and reload observed in thread name: cli_xml_server
CSCvr60111	configurations getting wiped off from standby, while deployment fails on active
CSCvr92327	ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'
CSCvs15972	Network Performance Degradation when SSL policy is enabled
CSCvs32023	Turn off egress-optimization processing
CSCvs52227	Firewall engine debug logs being produced in syslog without actually enabling debugs.
CSCvs55937	Deployment fails for FDM due to neo4j error
CSCvs59056	ASA/FTD Tunneled Static Routes are Ignored by Suboptimal Lookup if Float-Conn is Enabled
CSCvs81763	vFTD not able to pass vlan tagged traffic (trunk mode)
CSCvs91389	FTD Traceback Lina process
CSCvs91869	FPR-1000 Series Random Number Generation Error