



Cisco Firepower Release Notes, Version 6.4

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 NON-INFRINGEMENT 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.

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

© 2019–2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Welcome 1

- Release Dates 1
- Suggested Release 3
- Sharing Data with Cisco 3
- For Assistance 4

CHAPTER 2

System Requirements 5

- FMC Platforms 5
- Device Platforms 6
- Device Management 9
- Browser Requirements 11

CHAPTER 3

Features and Functionality 13

- New Features in FMC Version 6.4 13
- New Features in FDM Version 6.4 25
- Intrusion Rules and Keywords 30
- Deprecated FlexConfig Commands 30

CHAPTER 4

Upgrade Guidelines 33

- Planning Your Upgrade 33
- Minimum Version to Upgrade 34
- Upgrade Guidelines for Version 6.4 35
 - Upgrade Caution: Firepower 7000/8000 Series to Version 6.4.0.9–6.4.0.11 38
 - EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic 38
 - TLS Crypto Acceleration Enabled/Cannot Disable 38
 - Upgrade Failure: NGIPS Devices Previously at Version 6.2.3.12 39

Upgrade Failure: Insufficient Disk Space on Container Instances	39
Renamed Upgrade and Installation Packages	39
Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv	40
RA VPN Default Setting Change Can Block VPN Traffic	41
Security Intelligence Enables Application Identification	41
Update VDB after Upgrade to Enable CIP Detection	42
Invalid Intrusion Variable Sets Can Cause Deploy Failure	42
Remove Site IDs from Version 6.1.x Firepower Threat Defense Clusters Before Upgrade	43
Upgrade Can Unregister FDM from CSSM	43
Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0	43
Access Control Can Get Latency-Based Performance Settings from SRUs	44
'Snort Fail Open' Replaces 'Failsafe' on FTD	44
Upgrade Guidelines for FXOS	45
Unresponsive Upgrades	45
Uninstall a Patch	45
Uninstall ASA FirePOWER Patches with ASDM	46
Traffic Flow and Inspection	48
Traffic Flow and Inspection for FXOS Upgrades	48
Traffic Flow and Inspection for FTD Upgrades with FMC	48
Traffic Flow and Inspection for FTD Upgrades with FDM	50
Traffic Flow and Inspection for ASA FirePOWER Upgrades	51
Traffic Flow and Inspection for NGIPSv Upgrades with FMC	51
Time and Disk Space Tests	52
Version 6.4.0.17 Time and Disk Space	54
Version 6.4.0.16 Time and Disk Space	55
Version 6.4.0.15 Time and Disk Space	55
Version 6.4.0.14 Time and Disk Space	56
Version 6.4.0.13 Time and Disk Space	57
Version 6.4.0.12 Time and Disk Space	57
Version 6.4.0.11 Time and Disk Space	58
Version 6.4.0.10 Time and Disk Space	59
Version 6.4.0.9 Time and Disk Space	59
Version 6.4.0.8 Time and Disk Space	60
Version 6.4.0.7 Time and Disk Space	61

Version 6.4.0.6 Time and Disk Space	61
Version 6.4.0.5 Time and Disk Space	61
Version 6.4.0.4 Time and Disk Space	62
Version 6.4.0.3 Time and Disk Space	62
Version 6.4.0.2 Time and Disk Space	63
Version 6.4.0.1 Time and Disk Space	64
Version 6.4.0 Time and Disk Space	64

CHAPTER 5
Install the Software 67

Installation Guidelines	67
Installation Guides	69

CHAPTER 6
Open and Resolved Bugs 71

Open Bugs	71
Open Bugs in Version 6.4.0	71
Resolved Bugs	75
Resolved Bugs in New Builds	75
Resolved Bugs in Version 6.4.0.17	75
Resolved Bugs in Version 6.4.0.16	81
Resolved Bugs in Version 6.4.0.15	87
Resolved Bugs in Version 6.4.0.14	96
Resolved Bugs in Version 6.4.0.13	96
Resolved Bugs in Version 6.4.0.12	103
Resolved Bugs in Version 6.4.0.11	122
Resolved Bugs in Version 6.4.0.10	123
Resolved Bugs in Version 6.4.0.9	129
Resolved Bugs in Version 6.4.0.8	134
Resolved Bugs in Version 6.4.0.7	136
Resolved Bugs in Version 6.4.0.6	137
Resolved Bugs in Version 6.4.0.5	139
Resolved Bugs in Version 6.4.0.4	140
Resolved Bugs in Version 6.4.0.3	144
Version 6.4.0.2 Resolved Issues	145
Resolved Bugs in Version 6.4.0.1	148

Resolved Bugs in Version 6.4.0 149



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, on page 1](#)
- [Suggested Release, on page 3](#)
- [Sharing Data with Cisco, on page 3](#)
- [For Assistance, on page 4](#)

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. We *strongly* recommend you use the latest build. If you downloaded an earlier build, do not use it. For more information, see [Resolved Bugs in New Builds, on page 75](#).

Table 1: Version 6.4 Dates

Version	Build	Date	Platforms
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

Suggested Release

To take advantage of new features and resolved issues, we recommend you upgrade all eligible appliances to at least the suggested release, including any patches. On the Cisco Support & Download site, the suggested release is marked with a gold star.

We also list the suggested release in the new feature guides:

- [Cisco Secure Firewall Management Center New Features by Release](#)
- [Cisco Secure Firewall Device Manager New Features by Release](#)

Suggested Releases for Older Appliances

If an appliance is too old to run the suggested release and you do not plan to refresh the hardware right now, choose a major version then patch as far as possible. Some major versions are designated *long-term* or *extra long-term*, so consider one of those. For an explanation of these terms, see [Cisco NGFW Product Line Software Release and Sustaining Bulletin](#).

If you are interested in a hardware refresh, contact your Cisco representative or partner contact.

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

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, on page 5](#)
- [Device Platforms, on page 6](#)
- [Device Management, on page 9](#)
- [Browser Requirements, on page 11](#)

FMC Platforms

The FMC provides a centralized firewall management console. For device compatibility with the FMC, see [Device Management, on page 9](#). For general compatibility information, see the [Cisco Secure Firewall Management Center Compatibility Guide](#).

FMC Hardware

Version 6.4 supports the following FMC hardware:

- FMC 1600, 2600, 4600
- FMC 1000, 2500, 4500
- FMC 2000, 4000
- FMC 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/on-prem clouds.

With the FMCv, you can purchase licenses that enable you to manage 2, 10, 25, or 300 devices. Note that only 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 2: Version 6.4 FMCv Platforms

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

Cloud-Delivered 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. The cloud-delivered Firewall Management Center does not have a version, and we take care of feature updates.

Note that the customer-deployed management center is often referred to as the *on-prem* FMC, even for virtual platforms.



Note The cloud-delivered management center cannot manage Version 6.4 devices.

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 9](#). 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 3: 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	—

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 2110, 2120, 2130, 2140	YES	—	YES	YES	—
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 4: 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	—	—	—
On-Prem/Private Cloud				

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
Kernel-based virtual machine (KVM)	YES	—	YES	YES
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 5: Version 6.4 NGIPS Platforms

Device Platform	FMC Compatibility	ASDM Compatibility	Notes
Firepower 7010, 7020, 7030, 7050	YES	—	—
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			
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 .

Device Platform	FMC Compatibility	ASDM Compatibility	Notes
ASA 5515-X	YES	Requires ASDM 7.12(1).	Requires ASA 9.5(2) to 9.12(x).
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 34](#).

Table 6: FMC-Device Compatibility

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

FMC Version	Oldest Device Version You Can Manage
7.1	6.5
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.

Browser Requirements

Browsers

We test with the latest versions of these popular browsers, running on currently supported versions of macOS and Microsoft Windows:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 11 (Windows only)

If you encounter issues with any other browser, or are running an operating system that has reached end of life, we ask that you switch or upgrade. If you continue to encounter issues, contact Cisco TAC.



Note We do not perform extensive testing with Apple Safari or Microsoft Edge, nor do we test Microsoft Internet Explorer with FMC walkthroughs. However, Cisco TAC welcomes feedback on issues you encounter.

Browser Settings and Extensions

Regardless of browser, you must make sure JavaScript, cookies, and TLS v1.2 remain enabled.

If you are using Microsoft Internet Explorer 11:

- For the **Check for newer versions of stored pages** browsing history option, choose **Automatically**.
- Disable the **Include local directory path when uploading files to server** custom security setting.
- Enable **Compatibility View** for the appliance IP address/URL.

Note that some browser extensions can prevent you from saving values in fields like the certificate and key in PKI objects. These extensions include, but are not limited to, Grammarly and Whatfix Editor. This happens because these extensions insert characters (such as HTML) in the fields, which causes the system to see them invalid. We recommend you disable these extensions while you're logged into our products.

Screen Resolution

Interface	Minimum Resolution
FMC	1280 x 720
7000/8000 series device (limited local interface)	1280 x 720
FDM	1024 x 768
ASDM managing an ASA FirePOWER module	1024 x 768
Firepower Chassis Manager for the Firepower 4100/9300	1024 x 768

Securing Communications

When you first log in, the system uses a self-signed digital certificate to secure web communications. Your browser should display an untrusted authority warning, but also should allow you to add the certificate to the trust store. Although this will allow you to continue, we do recommend that you replace the self-signed certificate with a certificate signed by a globally known or internally trusted certificate authority (CA).

To begin replacing the self-signed certificate:

- FMC or 7000/8000 series: Choose **System** (⚙) > **Configuration** > **HTTPS Certificate**.
- FDM: Click **Device**, then the **System Settings** > **Management Access** link, then the **Management Web Server** tab.

For detailed procedures, see the online help or the configuration guide for your product.



Note If you do not replace the self-signed certificate:

- Google Chrome does not cache static content, such as images, CSS, or JavaScript. Especially in low bandwidth environments, this can extend page load times.
- Mozilla Firefox can stop trusting the self-signed certificate when the browser updates. If this happens, you can refresh Firefox, keeping in mind that you will lose some settings; see Mozilla's [Refresh Firefox](#) support page.

Browsing from a Monitored Network

Many browsers use Transport Layer Security (TLS) v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 may fail to load. For more information, see the software advisory titled: [Failures loading websites using TLS 1.3 with SSL inspection enabled](#).



CHAPTER 3

Features and Functionality

This document describes new and deprecated features for Version 6.4, including upgrade impact. For Cisco Defense Orchestrator (CDO) deployments, see [What's New for Cisco Defense Orchestrator](#).



Important New and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade. If your upgrade skips versions, see those release notes for historical feature information and upgrade impact, or see the appropriate [New Features by Release](#) guide.

- [New Features in FMC Version 6.4, on page 13](#)
- [New Features in FDM Version 6.4, on page 25](#)
- [Intrusion Rules and Keywords, on page 30](#)
- [Deprecated FlexConfig Commands, on page 30](#)

New Features in FMC Version 6.4

Although you can manage older devices with a newer FMC, we recommend you always update your entire deployment. New traffic-handling features usually require the latest release on both the FMC *and* device. Features where devices are not obviously involved (cosmetic changes to the web interface, cloud integrations) may only require the latest version on the FMC, but that is not guaranteed. In this document, we are explicit when version requirements deviate from the standard expectation.



Note Version 6.6 is the last release to support the Cisco Firepower User Agent software as an identity source. You cannot upgrade an FMC with user agent configurations to Version 6.7+. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact your Cisco representative or partner contact.

For more information, see the [End-of-Life and End-of-Support for the Cisco Firepower User Agent](#) announcement and the [Firepower User Identity: Migrating from User Agent to Identity Services Engine](#) TechNote.

New Features

Table 7: New Features in FMC Version 6.4 Patches

New Feature	Description
<p>Version 6.4.0.17</p> <p>Smaller VDB for lower memory devices.</p>	<p>For VDB 363+, the system now installs a smaller VDB (also called <i>VDB lite</i>) 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.</p> <p>Minimum threat defense: Any</p> <p>Lower memory devices: ASA 5506-X series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X</p> <p>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.</p>
<p>Version 6.4.0.10</p> <p>Upgrades postpone scheduled tasks.</p>	<p>Upgrade impact.</p> <p>Upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot.</p> <p>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.</p> <p>Note that this feature is supported for Firepower appliances <i>running</i> Version 6.4.0.10 or any later patch. It is not supported for upgrades <i>to</i> 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.</p>
<p>Version 6.4.0.9</p> <p>Default HTTPS server certificates.</p>	<p>Upgrade impact.</p> <p>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 <i>default</i> HTTPS server certificate, which expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan.</p> <p>Your old certificate was set to expire depending on when it was generated, as follows:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>

New Feature	Description
<p>Version 6.4.0.4</p> <p>New syslog fields.</p>	<p>These new syslog fields collectively identify a unique connection event:</p> <ul style="list-style-type: none"> • Sensor UUID • First Packet Time • Connection Instance ID • Connection Counter <p>These fields also appear in syslogs for intrusion, file, and malware events, allowing connection events to be associated with those events.</p>
<p>Version 6.4.0.2</p> <p>Detection of rule conflicts in FTD NAT policies.</p>	<p>Upgrade impact.</p> <p>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 <i>duplicate</i> or <i>overlapping</i> rules). This fixes an issue where conflicting NAT rules were applied out-of-order.</p> <p>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.</p> <p>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.</p>
<p>Version 6.4.0.2</p> <p>ISE Connection Status Monitor health module.</p>	<p>A new health module, the <i>ISE Connection Status Monitor</i>, monitors the status of the server connections between the Cisco Identity Services Engine (ISE) and the FMC.</p>

Table 8: New Features in FMC Version 6.4.0

New Feature	Description
Platform	
<p>FMC 1600, 2600, and 4600.</p>	<p>We introduced the FMC models FMC 1600, 2600, and 4600.</p>
<p>FMCv for Azure.</p>	<p>We introduced FMCv for Microsoft Azure.</p>
<p>FTD on the Firepower 1010, 1120, and 1140.</p>	<p>We introduced the Firepower 1010, 1120, and 1140.</p>
<p>FTD on the Firepower 4115, 4125, and 4145.</p>	<p>We introduced the Firepower 4115, 4125, and 4145.</p>
<p>Firepower 9300 SM-40, SM-48, and SM-56 support.</p>	<p>We introduced three new security modules: SM-40, SM-48, and SM-56.</p> <p>With FXOS 2.6.1, you can mix different types of security modules in the same chassis.</p>

New Feature	Description
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.	<p>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.</p> <p>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.</p> <p>Supported platforms: FTDv for VMware</p>
Firepower Threat Defense: Routing	
Rotating (keychain) authentication for OSPFv2 routing.	<p>You can now use rotating (keychain) authentication when configuring OSPFv2 routing.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • 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 <p>Supported platforms: FTD</p>
Firepower Threat Defense: Encryption and VPN	
RA VPN: Secondary authentication.	<p>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.</p> <p>RA VPN supports secondary authentication for the AAA Only and Client Certificate and AAA authentication methods.</p> <p>New/modified pages: Devices > VPN > Remote Access > add/edit configuration > Connection Profile > AAA area</p> <p>Supported platforms: FTD</p>

New Feature	Description
Site-to-site VPN: Dynamic IP addresses for extranet endpoints.	<p>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.</p> <p>New/modified pages: Devices > VPN > Site To Site > add/edit FTD VPN topology > Endpoints tab > add endpoint > IP Address option</p> <p>Supported platforms: FTD</p>
Site-to-site VPN: Dynamic crypto maps for point-to-point topologies.	<p>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.</p> <p>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.</p> <p>New/modified pages: Devices > VPN > Site To Site > add/edit FTD VPN topology > IPsec tab > Crypto Map Type option</p> <p>Supported platforms: FTD</p>
TLS crypto acceleration.	<p>Upgrade impact.</p> <p>SSL hardware acceleration has been renamed <i>TLS crypto acceleration</i>. 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.</p> <p>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 <i>one</i> container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances.</p> <p>New FXOS CLI commands for the Firepower 4100/9300 chassis:</p> <ul style="list-style-type: none"> • show hwCrypto • config hwCrypto <p>New FTD CLI commands:</p> <ul style="list-style-type: none"> • show crypto accelerator status (replaces system support ssl-hw-status) <p>Removed FTD CLI commands:</p> <ul style="list-style-type: none"> • system support ssl-hw-accel • system support ssl-hw-status <p>Supported platforms: Firepower 2100 series, Firepower 4100/9300</p>
Event Logging and Analysis	

New Feature	Description
Improvements to syslog messages for file and malware events.	<p>Fully qualified file and malware event data can now be sent from managed devices via syslog.</p> <p>New/modified pages: Policies > Access Control > Access Control > add/edit policy > Logging tab > File and Malware Settings area</p> <p>Supported platforms: Any</p>
Search intrusion events by CVE ID.	<p>You can now search for intrusion events generated as a result of a particular CVE exploit.</p> <p>New/modified pages: Analysis > Search</p> <p>Supported platforms: FMC</p>
IntrusionPolicy field is now included in syslog.	<p>Intrusion event syslog messages now specify the intrusion policy that triggered the event.</p> <p>Supported platforms: Any</p>
Cisco SecureX integration.	<p>Cisco SecureX is a cloud offering that helps you rapidly detect, investigate, and respond to threats.</p> <p>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 <i>Cisco Threat Response (CTR)</i>.</p> <p>See the Cisco Secure Firewall Threat Defense and SecureX Integration Guide.</p> <p>New/modified pages: System > Integration > Cloud Services</p> <p>Supported platforms: FTD</p>
Splunk integration.	<p>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.</p> <p>See Cisco Secure Firewall App for Splunk User Guide.</p> <p>Supported platforms: FMC</p>
Cisco Security Analytics and Logging (SaaS) integration.	<p>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.</p> <p>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.</p> <p>See Cisco Secure Firewall Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide.</p> <p>Supported platforms: FTD with FMC</p>

New Feature	Description
Administration and Troubleshooting	
New licensing capabilities for ISA 3000.	<p>For ASA FirePOWER and FTD deployments, the ISA 3000 now supports URL Filtering and Malware licenses and their associated features.</p> <p>For FTD only, the ISA 3000 also now supports Specific License Reservation for approved customers.</p> <p>Supported platforms: ISA 3000</p>
Scheduled remote backups of managed devices.	<p>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.</p> <p>New/modified pages: System > Tools > Scheduling > add/edit task > choose Job Type: Backup > choose a Backup Type</p> <p>Supported platforms: FTD physical platforms, FTDv for VMware, Firepower 7000/8000 series</p> <p>Exceptions: No support for FTD clustered devices or container instances</p>
Ability to disable Duplicate Address Detection (DAD) on management interfaces.	<p>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.</p> <p>New/modified pages: System > Configuration > Management Interfaces > Interfaces area > edit interface > IPv6 DAD check box</p> <p>Supported platforms: FMC, Firepower 7000/8000 series</p>
Ability to disable ICMPv6 Echo Reply and Destination Unreachable messages on management interfaces.	<p>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.</p> <p>New/modified pages: System > Configuration > Management Interfaces > ICMPv6</p> <p>New/modified commands:</p> <ul style="list-style-type: none"> • configure network ipv6 destination-unreachable • configure network ipv6 echo-reply <p>Supported platforms: FMC (web interface only), managed devices (CLI only)</p>

New Feature	Description
Support for the Service-Type attribute for FTD users defined on the RADIUS server.	<p>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.</p> <p>New/modified pages: System > Users > External Authentication tab > add/edit external authentication object > Shell Access Filter</p> <p>Supported platforms: FTD</p>
View object use.	<p>The object manager now allows you to see the policies, settings, and other objects where a network, port, VLAN, or URL object is used.</p> <p>New/modified pages: Objects > Object Management > choose object type > Find Usage (binoculars) icon</p> <p>Supported platforms: FMC</p>
Hit counts for access control and prefilter rules.	<p>You can now access hit counts for access control and prefilter rules on your FTD devices.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Policies > Access Control > Access Control > add/edit policy > Analyze Hit Counts • Policies > Access Control > Prefilter > add/edit policy > Analyze Hit Counts <p>New commands:</p> <ul style="list-style-type: none"> • show rule hits • clear rule hits • cluster exec show rule hits • cluster exec clear rule hits • show cluster rule hits <p>Modified commands: show failover</p> <p>Supported platforms: FTD</p>
URL Filtering health monitor improvements.	<p>You can now configure time thresholds for URL Filtering Monitor alerts.</p> <p>New/modified pages: System > Health > Policy > add/edit policy > URL Filtering Monitor</p> <p>Supported platforms: Any</p>

New Feature	Description
Connection-based troubleshooting.	<p>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.</p> <p>New/modified commands:</p> <ul style="list-style-type: none"> • clear packet debugs • debug packet start • debug packet stop • show packet debugs <p>Supported platforms: FTD</p>
New Cisco Success Network monitoring capabilities	<p>Added the following Cisco Success Network monitoring capabilities:</p> <ul style="list-style-type: none"> • CSPA (Cisco Security Packet Analyzer) query information • Contextual cross-launch instances enabled on the FMC • TLS/SSL inspection events • Snort restarts <p>Supported platforms: FMC</p>
Security and Hardening	

New Feature	Description
Signed SRU, VDB, and GeoDB updates.	<p>So Firepower can verify that you are using the correct update files, Version 6.4.0+ uses <i>signed</i> 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.</p> <p>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:</p> <ul style="list-style-type: none"> • SRU: Cisco_Firepower_SRU-<i>date-build</i>-vrt.sh.REL.tar • VDB: Cisco_VDB_Fingerprint_Database-4.5.0-<i>version</i>.sh.REL.tar • GeoDB: Cisco_GEODB_Update-<i>date-build</i>.sh.REL.tar <p>Update files for Version 5.x through 6.3 still use the old naming scheme:</p> <ul style="list-style-type: none"> • SRU: Sourcefire_Rule_Update-<i>date-build</i>-vrt.sh • VDB: Sourcefire_VDB_Fingerprint_Database-4.5.0-<i>version</i>.sh • GeoDB: Sourcefire_Geodb_Update-<i>date-build</i>.sh <p>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.</p> <p>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.</p> <p>Supported platforms: Any</p>
SNMPv3 users can authenticate using a SHA-256 authorization algorithm.	<p>SNMPv3 users can now authenticate using a SHA-256 algorithm.</p> <p>New/modified screen: Devices > Platform Settings > SNMP > Users > Auth Algorithm Type</p> <p>Supported platforms: Firepower Threat Defense</p>
2048-bit certificate keys now required (security enhancement).	<p>Upgrade impact.</p> <p>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.</p> <p>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.</p> <p>Supported platforms: FMC</p>

New Feature	Description
Usability and Performance	
Snort restart improvements.	<p>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.</p> <p>Supported platforms: Firepower 4100/9300</p>
Performance improvement for selected IPS traffic.	<p>Upgrade impact.</p> <p>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.</p> <p>New/modified commands:</p> <ul style="list-style-type: none"> • asp inspect-dp egress optimization • show asp inspect-dp egress optimization • clear asp inspect-dp egress optimization • show conn state egress_optimization <p>For more information, see the Cisco Secure Firewall Threat Defense Command Reference. To troubleshoot issues with egress optimization, contact Cisco TAC.</p> <p>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.</p> <p>For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature.</p> <p>Supported platforms: FTD</p>
Faster SNMP event logging.	<p>Performance improvements when sending intrusion and connection events to an external SNMP trap server.</p> <p>Supported platforms: Any</p>
Faster deploy.	<p>Improvements to appliance communications and deploy framework.</p> <p>Supported platforms: FTD</p>
Faster upgrade.	<p>Improvements to the event database.</p> <p>Supported platforms: Any</p>

New Feature	Description
Firepower Management Center REST API	
New REST API capabilities.	<p>Added REST API objects to support Version 6.4.0 features:</p> <ul style="list-style-type: none"> • 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 <p>Supported platforms: FMC</p>
API Explorer based on OAS.	<p>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.</p> <p>Supported platforms: FMC</p>

Deprecated Features

Table 9: Deprecated Features in FMC Version 6.4.0

Deprecated Feature	Description
Deprecated: SSL hardware acceleration FTD CLI commands.	<p>As part of the TLS crypto acceleration feature, we removed the following FTD CLI commands:</p> <ul style="list-style-type: none"> • system support ssl-hw-accel enable • system support ssl-hw-accel disable • system support ssl-hw-status

Deprecated Feature	Description
Deprecated: Geolocation details.	<p>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.</p> <p>The new country code package has the same file name as the old all-in-one package: <code>Cisco_GEODB_Update-date-build</code>. 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.</p> <p>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.</p>

New Features in FDM Version 6.4

Table 10: New and Deprecated Features in FDM Version 6.4

Feature	Description
Firepower 1000 series device configuration.	<p>You can configure Firepower Threat Defense on Firepower 1000 series devices using FDM.</p> <p>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.</p>
Hardware bypass for the ISA 3000.	<p>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.</p>
Ability to reboot and shut down the system from the FDM CLI Console.	<p>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.</p>

Feature	Description
External Authentication and Authorization using RADIUS for Firepower Threat Defense CLI Users.	<p>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.</p> <p>We added the SSH configuration to the AAA Configuration tab on the Device > System Settings > Management Access page.</p>
Support for network range objects and nested network group objects.	<p>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).</p> <p>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.</p>
Full-text search options for objects and rules.	<p>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.</p> <p>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.</p>
Obtaining a list of supported API versions for an FDM-managed Firepower Threat Defense device.	<p>You can use the GET <code>/api/versions</code> (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.</p>
Hit counts for access control rules.	<p>You can now view hit counts for access control rules. The hit counts indicate how often connections matched the rule.</p> <p>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.</p>
Site-to-Site VPN enhancements for dynamic addressing and certificate authentication.	<p>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.</p>
Support for RADIUS servers and Change of Authorization in remote access VPN.	<p>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.</p> <p>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.</p>

Feature	Description
Multiple connection profiles and group policies for remote access VPN.	<p>You can configure more than one connection profile, and create group policies to use with the profiles.</p> <p>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.</p>
Support for certificate-based, second authentication source, and two-factor authentication in remote access VPN.	<p>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.</p> <p>We updated the RA VPN Connection wizard to support the configuration of these additional options.</p>
Support for IP address pools with multiple address ranges, and DHCP address pools, for remote access VPN.	<p>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.</p> <p>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.</p>
Active Directory realm enhancements.	<p>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.</p> <p>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.</p>
Redundancy support for ISE servers.	<p>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.</p> <p>We added an attribute for the secondary server to the ISE identity object.</p>
File/malware events sent to external syslog servers.	<p>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.</p> <p>We added the File/Malware syslog server options to the Device > System Settings > Logging Settings page.</p>

Feature	Description
Logging to the internal buffer and support for custom event log filters.	<p>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.</p> <p>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.</p>
Certificate for the FDM Web Server.	<p>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.</p>
Cisco Threat Response support.	<p>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.</p> <p>We added Cisco Threat Response to the Device > System Settings > Cloud Services page.</p>
Manually upload VDB, GeoDB, and SRU updates.	<p>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.</p> <p>We updated the Device > Updates page to allow you to select and upload a file from your workstation.</p> <p>Minimum FTD: 6.4.0.10.</p> <p>Version restrictions: This feature is not available in Version 6.5. Support returns in Version 6.6.</p>
Smaller VDB for lower memory devices.	<p>For VDB 363+, the system now installs a smaller VDB (also called <i>VDB lite</i>) 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.</p> <p>Minimum FTD: 6.4.0.17</p> <p>Lower memory devices: ASA-5508-X, ASA-5515-X, ASA-5516-X, ASA-5525-X, ASA-5545-X</p> <p>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.</p>

Feature	Description
Universal Permanent License Reservation (PLR) mode.	<p>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.</p> <p>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.</p> <p>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+.</p>
Default HTTPS server certificates.	<p>Upgrade impact.</p> <p>Patching may renew the device's current <i>default</i> HTTPS server certificate. Your certificate is set to expire depending on when it is generated, as follows:</p> <ul style="list-style-type: none"> • 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.	<p>These new syslog fields collectively identify a unique connection event:</p> <ul style="list-style-type: none"> • Sensor UUID • First Packet Time • Connection Instance ID • Connection Counter <p>These fields also appear in syslogs for intrusion, file, and malware events, allowing connection events to be associated with those events.</p> <p>Minimum FTD: 6.4.0.4</p>

Feature	Description
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 made 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 <code>/#/api-explorer</code> after logging in.

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

Intrusion rule updates (SRUs/LSPs) provide 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.

You can find your Snort version in the *Bundled Components* section of the compatibility guide, or use one of these commands:

- FMC: Choose **Help > About**.
- FDM: Use the **show summary** CLI command.

The Snort release notes contain details on new keywords. You can read the release notes on the Snort download page: <https://www.snort.org/downloads>.

Deprecated FlexConfig Commands

This document lists deprecated FlexConfig objects and commands along with the other deprecated features for this release. For a full list of prohibited commands, including those prohibited when FlexConfig was introduced and those deprecated in previous releases, see your configuration guide.



Caution In most cases, your existing FlexConfig configurations continue to work post-upgrade and you can still deploy. However, in some cases, using deprecated commands can cause deployment issues.

About FlexConfig

Some FTD features are configured using ASA configuration commands. You can use Smart CLI or FlexConfig to manually configure various ASA features that are not otherwise supported in the web interface.

Upgrades can add GUI or Smart CLI support for features that you previously configured using FlexConfig. This can deprecate FlexConfig commands that you are currently using; your configurations are *not* automatically

converted. After the upgrade, you cannot assign or create FlexConfig objects using the newly deprecated commands.

After the upgrade, examine your FlexConfig policies and objects. If any contain commands that are now deprecated, messages indicate the problem. We recommend you redo your configuration. When you are satisfied with the new configuration, you can delete the problematic FlexConfig objects or commands.



CHAPTER 4

Upgrade Guidelines

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

- [Planning Your Upgrade](#), on page 33
- [Minimum Version to Upgrade](#), on page 34
- [Upgrade Guidelines for Version 6.4](#), on page 35
- [Upgrade Guidelines for FXOS](#), on page 45
- [Unresponsive Upgrades](#), on page 45
- [Uninstall a Patch](#), on page 45
- [Traffic Flow and Inspection](#), on page 48
- [Time and Disk Space Tests](#), on page 52

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 11: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read <i>all</i> 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 12: 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 6 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 13: Upgrade Guidelines for FTD with FMC Version 6.4

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 34	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
	Open and Resolved Bugs, on page 71 , 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 FXOS, on page 45	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 38	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 38	Firepower 1010	6.4.0 only	6.4.0.3 through 6.4.0.5
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 38	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 39	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 39	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 39	FMC Firepower 7000/8000 series NGIPSv	Any	6.3+
	Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 40	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 41	FTD	6.2.0 through 6.2.3.x	6.3+
	Security Intelligence Enables Application Identification, on page 41	FMC deployments	6.1.0 through 6.2.3.x	6.3+
	Update VDB after Upgrade to Enable CIP Detection, on page 42	Any	6.1.0 through 6.2.3.x	6.3+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 42	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 43	FTD clusters	6.1.0.x	6.2.3+
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 44	FMC	6.1.0.x	6.2+
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 44	FTD	6.1.0.x	6.2+

Table 14: Upgrade Guidelines for FTD with FDM Version 6.4

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 34	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
	Open and Resolved Bugs, on page 71, 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 FXOS, on page 45	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic, on page 38	Firepower 1010	6.4.0 only	6.4.0.3 through 6.4.0.5
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 38	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 42	Any	6.1.0 through 6.2.3.x	6.3+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 42	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 43	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 43	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 15: 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 16: 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 17: 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 18: 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 FXOS

For the Firepower 4100/9300, major FTD upgrades also require an FXOS upgrade.

Major FTD versions have a specially qualified and recommended companion FXOS version. Use these combinations whenever possible because we perform enhanced testing for them. Maintenance release and patches rarely require FXOS upgrades, but you may still want to upgrade to the latest FXOS build to take advantage of resolved issues.

We also recommend the latest firmware; see the [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#).

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](#).

Minimum FXOS Version to Upgrade FTD

The minimum FXOS version to run Version 6.4 is FXOS 2.6.1.157.

Minimum FXOS Version to Upgrade FXOS

You can upgrade to any later FXOS version from as far back as FXOS 2.2.2.

Time to Upgrade FXOS

An FXOS upgrade can take up to 45 minutes and can affect traffic flow and inspection. For more information, see [Traffic Flow and Inspection for FXOS Upgrades, on page 48](#).

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 46](#) 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 19: Uninstall Order for ASA with FirePOWER Services in ASA Failover Pairs/Clusters

Configuration	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	<p>Always uninstall from the standby.</p> <ol style="list-style-type: none"> 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	<p>Make both failover groups active on the unit you are not uninstalling.</p> <ol style="list-style-type: none"> 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	<p>Disable clustering on each unit before you uninstall. Uninstall from one unit at a time, leaving the control unit for last.</p> <ol style="list-style-type: none"> 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 FXOS Upgrades

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

*Table 20: Traffic Flow and Inspection: FXOS Upgrades*

| FTD Deployment                              | Traffic Behavior                             | Method                                                                                          |
|---------------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------|
| Standalone                                  | Dropped.                                     | —                                                                                               |
| High availability                           | Unaffected.                                  | <b>Best Practice:</b> 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.                                  | <b>Best Practice:</b> 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: <b>Bypass: Standby or Bypass-Force.</b>                                |
|                                             | Dropped until at least one module is online. | Hardware bypass disabled: <b>Bypass: Disabled.</b>                                              |
|                                             | 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 21: Traffic Flow and Inspection: Software Upgrades for Standalone Devices

| Interface Configuration |                                                                                                                                                           | Traffic Behavior                                                                                                                                                                                                                                                                       |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firewall interfaces     | Routed or switched including EtherChannel, redundant, subinterfaces.<br><br>Switched interfaces are also known as bridge group or transparent interfaces. | Dropped.<br><br>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:<br><b>Bypass: Force</b>                                                                                        | Passed without inspection until you either disable hardware bypass, or set it back to standby mode.                                                                                                                                                                                    |
|                         | Inline set, hardware bypass standby mode:<br><b>Bypass: Standby</b>                                                                                       | 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:<br><b>Bypass: Disabled</b>                                                                                          | 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 22: Traffic Flow and Inspection: Deploying Configuration Changes**

| Interface Configuration |                                                                                                                                                           | Traffic Behavior                                                                                                          |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Firewall interfaces     | Routed or switched including EtherChannel, redundant, subinterfaces.<br><br>Switched interfaces are also known as bridge group or transparent interfaces. | Dropped.                                                                                                                  |
| IPS-only interfaces     | Inline set, <b>Failsafe</b> enabled or disabled.                                                                                                          | Passed without inspection.<br><br>A few packets might drop if <b>Failsafe</b> is disabled and Snort is busy but not down. |
|                         | Inline set, <b>Snort Fail Open: Down:</b> disabled.                                                                                                       | Dropped.                                                                                                                  |
|                         | Inline set, <b>Snort Fail Open: Down:</b> 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 23: Traffic Flow and Inspection: ASA FirePOWER Upgrades*

| Traffic Redirection Policy                                        | Traffic Behavior                              |
|-------------------------------------------------------------------|-----------------------------------------------|
| Fail open ( <b>sfr fail-open</b> )                                | Passed without inspection                     |
| Fail closed ( <b>sfr fail-close</b> )                             | Dropped                                       |
| Monitor only ( <b>sfr {fail-close}{{fail-open} monitor-only</b> ) | 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 24: 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 25: Traffic Flow and Inspection: Deploying Configuration Changes

| Interface Configuration                     | Traffic Behavior                                                                                                      |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Inline, <b>Failsafe</b> enabled or disabled | Passed without inspection.<br>A few packets might drop if <b>Failsafe</b> 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 Tests

For reference purposes, we provide reports of in-house time and disk space tests for FMC and device software upgrades.

### Time Tests

We report the *slowest* tested time of all software upgrades tested on a particular platform/series. Your upgrade will likely take longer than the provided times for multiple reasons, as explained in the following table. We recommend you track and record your own upgrade times so you can use them as future benchmarks.



**Caution** Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot, shut down, or 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, contact Cisco TAC.

Table 26: Time Test Conditions for Software Upgrades

| Condition                     | Details                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deployment                    | Times for device upgrades are from tests in a FMC deployments. Raw upgrade times for remotely and locally managed devices are similar, given similar conditions.                                                                                                                                                                                                                                 |
| Versions                      | For major and maintenance releases, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version. Upgrade time usually increases if your upgrade skips versions.                                                                                                                                                                              |
| Models                        | In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.                                                                                                                                                                                                                                                                                    |
| Virtual appliances            | We test with the default settings for memory and resources. However, note that upgrade time in virtual deployments is highly hardware dependent.                                                                                                                                                                                                                                                 |
| High availability/scalability | Unless otherwise noted, we test on standalone devices.<br>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                | We test on appliances with minimal configurations and traffic load.<br>Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how those things 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                    | We report times for the software upgrade itself and the subsequent reboot <i>only</i> . This does not include time for operating system upgrades, transferring upgrade packages, readiness checks, VDB and intrusion rule (SRU/LSP) updates, or deploying configurations.                                                                                                                        |

### Disk Space Tests

We report the *most* disk space used of all software upgrades tested on a particular platform/series. This includes the space needed to copy the upgrade package to the device.

We also report the space needed on the FMC (in either /Volume or /var) for the device upgrade package. If you are using FDM, ignore those values.

When we report disk space estimates for a particular location (for example, /var or /ngfw), we are reporting the disk space estimate for the partition mounted in that location. On some platforms, these locations may be on the same partition.

Without enough free disk space, the upgrade fails.

Table 27: Checking Disk Space

| Platform     | Command                                                                                                                                          |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| FMC          | Choose <b>System &gt; Monitoring &gt; Statistics</b> and select the FMC. Under Disk Usage, expand the By Partition details.                      |
| FTD with FMC | Choose <b>System &gt; Monitoring &gt; Statistics</b> and select the device you want to check. Under Disk Usage, expand the By Partition details. |
| FTD with FDM | Use the <b>show disk</b> CLI command.                                                                                                            |

## Version 6.4.0.17 Time and Disk Space

Table 28: Time and Disk Space for Version 6.4.0.17

| Platform                   | Space in /Volume | Space in /      | Space on FMC | Upgrade Time | Reboot Time |
|----------------------------|------------------|-----------------|--------------|--------------|-------------|
| FMC                        | 4.1 GB in /var   | 210 MB in /     | —            | 37 min       | 9 min       |
| FMCv: VMware               | 4.1 GB in /var   | 220 MB in /     | —            | 26 min       | 5 min       |
| Firepower 1000 series      | —                | 4.1 gB in /ngfw | 880 MB       | 10 min       | 14 min      |
| Firepower 2100 series      | —                | 3.8 GB in /ngfw | 860 MB       | 8 min        | 11 min      |
| Firepower 4100 series      | —                | 3.6 GB in /ngfw | 790 MB       | 5 min        | 8 min       |
| Firepower 9300             | —                | 3.6 GB in /ngfw | 790 MB       | 4 min        | 8 min       |
| ASA 5500-X series with FTD | 3.1 GB in /home  | 130 MB in /ngfw | 650 MB       | 13 min       | 10 min      |
| FTDv: VMware               | 3.1 GB in /home  | 130 MB in /ngfw | 650 MB       | 6 min        | 7 min       |
| Firepower 7000/8000 series | 3.9 GB in /var   | 190 MB in /     | 740 MB       | 10 min       | 18 min      |
| ASA FirePOWER              | 4.5 GB in /var   | 61 MB in /      | 690 MB       | 44 min       | 8 min       |
| NGIPSv                     | 2.4 GB in /var   | 180 MB in /     | 540 MB       | 6 min        | 4 min       |

## Version 6.4.0.16 Time and Disk Space

Table 29: Time and Disk Space for Version 6.4.0.16

| Platform                   | Space in /Volume | Space in /      | Space on FMC | Upgrade Time | Reboot Time |
|----------------------------|------------------|-----------------|--------------|--------------|-------------|
| FMC                        | 4.0 GB in /var   | 220 MB in /     | —            | 33 min       | 8 min       |
| FMCv: VMware               | 5.6 GB in /var   | 220 MB in /     | —            | 31 min       | 7 min       |
| Firepower 1000 series      | —                | 4.1 GB in /ngfw | 880 MB       | 11 min       | 13 min      |
| Firepower 2100 series      | —                | 3.6 GB in /ngfw | 860 MB       | 8 min        | 11 min      |
| Firepower 4100 series      | —                | 3.6 GB in /ngfw | 790 MB       | 5 min        | 9 min       |
| Firepower 9300             | —                | 3.6 GB in /ngfw | 790 MB       | 5 min        | 9 min       |
| ASA 5500-X series with FTD | 3.1 GB in /home  | 130 MB in /ngfw | 640 MB       | 9 min        | 5 min       |
| FTDv: VMware               | 3.6 GB in /home  | 130 MB in /ngfw | 640 MB       | 8 min        | 5 min       |
| Firepower 7000/8000 series | 3.9 GB in /var   | 190 MB in /     | 740 MB       | 11 min       | 3 min       |
| ASA FirePOWER              | 4.5 GB in /var   | 60 MB in /      | 690 MB       | 46 min       | 2 min       |
| NGIPSv                     | 2.4 GB in /var   | 190 MB in /     | 540 MB       | 6 min        | 4 min       |

## Version 6.4.0.15 Time and Disk Space

Table 30: Time and Disk Space for Version 6.4.0.15

| Platform              | Space in /Volume | Space in /      | Space on FMC | Upgrade Time | Reboot Time |
|-----------------------|------------------|-----------------|--------------|--------------|-------------|
| FMC                   | 4GB in /var      | 190 MB in /     | —            | 36 min       | 8 min       |
| FMCv: VMware          | 5.1 GB in /var   | 190 MB in /     | —            | 27 min       | 7 min       |
| Firepower 1000 series | —                | 3.2 GB in /ngfw | 610 MB       | 11 min       | 12 min      |
| Firepower 2100 series | —                | 2.8 GB in /ngfw | 580 MB       | 8 min        | 12 min      |
| Firepower 4100 series | —                | 2.7 GB in /ngfw | 520 MB       | 4 min        | 9 min       |

| Platform                   | Space in /Volume | Space in /      | Space on FMC | Upgrade Time | Reboot Time |
|----------------------------|------------------|-----------------|--------------|--------------|-------------|
| Firepower 9300             | —                | 2.7 GB in /ngfw | 520 MB       | 5 min        | 9 min       |
| ASA 5500-X series with FTD | 2.2 GB in /home  | 130 MB in /ngfw | 370 MB       | 15 min       | 41 min      |
| FTDv: VMware               | 2.2 GB in /home  | 130 MB in /     | 370 MB       | 6 min        | 6 min       |
| Firepower 7000/8000        | 3.9 GB in /var   | 190 MB in /     | 740 MB       | 11 min       | 2 min       |
| ASA FirePOWER              | 4.5 GB in /var   | 61 MB in /      | 690 MB       | 59 min       | 55 min      |
| NGIPSv                     | 2.4 GB in /var   | 190 MB in /     | 540 MB       | 7 min        | 4 min       |

## Version 6.4.0.14 Time and Disk Space

Table 31: Time and Disk Space for Version 6.4.0.14

| Platform                   | Space in /Volume | Space in /      | Space on FMC | Upgrade Time | Reboot Time |
|----------------------------|------------------|-----------------|--------------|--------------|-------------|
| FMC                        | 4.5 GB in /var   | 170 MB in /     | —            | 42 min       | 18 min      |
| FMCv: VMware               | 5.2 GB in /var   | 170 MB in /     | —            | 25 min       | 2 min       |
| Firepower 1000 series      | —                | 2.4 GB in /ngfw | 370 MB       | 11 min       | 11 min      |
| Firepower 2100 series      | —                | 1.9 GB in /ngfw | 310 MB       | 8 min        | 10 min      |
| Firepower 4100 series      | —                | 2.5 GB in /ngfw | 480 MB       | 4 min        | 9 min       |
| Firepower 9300             | —                | 2.5 GB in /ngfw | 480 MB       | 4 min        | 8 min       |
| ASA 5500-X series with FTD | 2.0 GB in /home  | 110 MB in /ngfw | 320 MB       | 12 min       | 42 min      |
| FTDv: VMware               | 1.9 GB in /home  | 110 MB in /ngfw | 320 MB       | 6 min        | 2 min       |
| Firepower 7000/8000 series | 3.7 GB in /var   | 170 MB in /     | 690 MB       | 10 min       | 2 min       |
| ASA FirePOWER              | 4.2 GB in /var   | 38 MB in /      | 640 MB       | 43 min       | 51 min      |
| NGIPSv                     | 2.2 GB in /var   | 170 MB in /     | 480 MB       | 6 min        | 4 min       |

## Version 6.4.0.13 Time and Disk Space

Table 32: Time and Disk Space for Version 6.4.0.13

| Platform                   | Space in /Volume | Space in /      | Space on FMC | Upgrade Time | Reboot Time |
|----------------------------|------------------|-----------------|--------------|--------------|-------------|
| FMC                        | 3.8 GB in /var   | in / 170 MB     | —            | 34 min       | 8 min       |
| FMCv: VMware               | 3.9 GB in /var   | in / 170 MB     | —            | 21 min       | 4 min       |
| Firepower 1000 series      | —                | 3.0 GB in /ngfw | 540 MB       | 11 min       | 13 min      |
| Firepower 2100 series      | —                | 2.6 GB in /ngfw | 510 MB       | 8 min        | 12 min      |
| Firepower 4100 series      | —                | 2.5 GB in /ngfw | 450 MB       | 4 min        | 9 min       |
| Firepower 9300             | —                | 2.5 GB in /ngfw | 450 MB       | 4 min        | 9 min       |
| ASA 5500-X series with FTD | 2.0 GB in /home  | 110 MB in /ngfw | 295 MB       | 12 min       | 9 min       |
| FTDv: VMware               | 1.9 GB in /home  | 110 MB in /ngfw | 295 MB       | 7 min        | 5 min       |
| Firepower 7000/8000 series | 3.7 GB in /var   | 170 MB in /     | 670 MB       | 11 min       | 14 min      |
| ASA FirePOWER              | 4.2 GB in /var   | 38 MB in /      | 660 MB       | 43 min       | 8 min       |
| NGIPSv                     | 2.2 GB in /var   | 170 MB in /     | 460 MB       | 6 min        | 4 min       |

## Version 6.4.0.12 Time and Disk Space

Table 33: Time and Disk Space for Version 6.4.0.12

| Platform              | Space in /Volume | Space in /      | Space on FMC | Upgrade Time | Reboot Time |
|-----------------------|------------------|-----------------|--------------|--------------|-------------|
| FMC                   | 3.8 GB in /var   | 170 MB in /     | —            | 25 min       | 8 min       |
| FMCv: VMware          | 3.8 GB in /var   | 170 MB in /     | —            | 27 min       | 4 min       |
| Firepower 1000 series |                  | 2.9 GB in /ngfw | 530 MB       | 10 min       | 13 min      |
| Firepower 2100 series |                  | 2.5 GB in /ngfw | 510 MB       | 8 min        | 32 min      |
| Firepower 4100 series |                  | 2.5 GB in /ngfw | 440 MB       | 4 min        | 9 min       |

| Platform                   | Space in /Volume | Space in /      | Space on FMC | Upgrade Time | Reboot Time |
|----------------------------|------------------|-----------------|--------------|--------------|-------------|
| Firepower 9300             |                  | 2.5 GB in /ngfw | 440 MB       | 4 min        | 8 min       |
| ASA 5500-X series with FTD | 1.9 GB in /home  | 110 MB in /ngfw | 290 MB       | 12 min       | 40 min      |
| FTDv: VMware               | 1.9 GB in /home  | 110 MB in /ngfw | 290 MB       | 7 min        | 5 min       |
| Firepower 7000/8000 series | 3.7 GB in /var   | 170 MB in /     | 660 MB       | 10 min       | 15 min      |
| ASA FirePOWER              | 4.2 GB in /var   | 37 MB in /      | 600 MB       | 47 min       | 51 min      |
| NGIPSv                     | 2.2 GB in /var   | 150 MB in /     | 460 MB       | 7 min        | 5 min       |

## Version 6.4.0.11 Time and Disk Space

Table 34: Time and Disk Space for Version 6.4.0.11

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time | Reboot Time |
|----------------------------|------------------|------------|--------------|--------------|-------------|
| FMC                        | 3.8 GB           | 170 MB     | —            | 30 min       | 8 min       |
| FMCv: VMware               | 4.1 GB           | 170 MB     | —            | 27 min       | 7 min       |
| Firepower 1000 series      | 3.0 GB           | 3.0 GB     | 530 MB       | 14 min       | 9 min       |
| Firepower 2100 series      | 2.5 GB           | 2.5 GB     | 510 MB       | 9 min        | 6 min       |
| Firepower 4100 series      | 1.8 GB           | 1.8 GB     | 310 MB       | 8 min        | 7 min       |
| Firepower 9300             | 1.8 GB           | 1.8 GB     | 310 MB       | 9 min        | 9 min       |
| ASA 5500-X series with FTD | 1.6 GB           | 110 MB     | 290 MB       | 12 min       | 12 min      |
| FTDv: VMware               | 4.4 GB           | 170 MB     | 290 MB       | 28 min       | 4 min       |
| Firepower 7000/8000 series | 3.6 GB           | 170 MB     | 680 MB       | 11 min       | 97 min      |
| ASA FirePOWER              | 4.2 GB           | 36 MB      | 630 MB       | 54 min       | 51 min      |
| NGIPSv                     | 2.4 GB           | 150 MB     | 470 MB       | 11 min       | 15 min      |

## Version 6.4.0.10 Time and Disk Space

Table 35: Time and Disk Space for Version 6.4.0.10

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time | Reboot Time |
|----------------------------|------------------|------------|--------------|--------------|-------------|
| FMC                        | 3.8 GB           | 170 MB     | —            | 30 min       | 8 min       |
| FMCv: VMware               | 4.1 GB           | 170 MB     | —            | 27 min       | 7 min       |
| Firepower 1000 series      | 2.9 GB           | 2.9 GB     | 560 MB       | 11 min       | 14 min      |
| Firepower 2100 series      | 2.5 GB           | 2.5 GB     | 530 MB       | 8 min        | 13 min      |
| Firepower 4100 series      | 1.8 GB           | 1.8 GB     | 330 MB       | 5 min        | 11 min      |
| Firepower 9300             | 1.8 GB           | 1.8 GB     | 330 MB       | 5 min        | 17 min      |
| ASA 5500-X series with FTD | 1.9 GB           | 110 MB     | 310 MB       | 12 min       | 31 min      |
| FTDv: VMware               | 2.0 GB           | 110 MB     | 310 MB       | 8 min        | 8 min       |
| Firepower 7000/8000 series | 3.6 GB           | 170 MB     | 680 MB       | 11 min       | 97 min      |
| ASA FirePOWER              | 4.2 GB           | 36 MB      | 630 MB       | 54 min       | 51 min      |
| NGIPSv                     | 2.4 GB           | 150 MB     | 470 MB       | 11 min       | 15 min      |

## Version 6.4.0.9 Time and Disk Space

Table 36: Time and Disk Space for Version 6.4.0.9

| Platform              | Space in /Volume | Space in / | Space on FMC | Upgrade Time | Reboot Time |
|-----------------------|------------------|------------|--------------|--------------|-------------|
| FMC                   | 3.7 GB           | 170 MB     | —            | 41 min       | 10 min      |
| FMCv: VMware          | 3.7 GB           | 170 MB     | —            | 28 min       | 6 min       |
| Firepower 1000 series | 2.9 GB           | 2.9 GB     | 530 MB       | 11 min       | 14 min      |
| Firepower 2100 series | 2.6 GB           | 2.6 GB     | 510 MB       | 10 min       | 13 min      |
| Firepower 4100 series | 1.8 GB           | 1.8 GB     | 310 MB       | 4 min        | 10 min      |

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time | Reboot Time |
|----------------------------|------------------|------------|--------------|--------------|-------------|
| Firepower 9300             | 1.8 GB           | 1.8 GB     | 310 MB       | 4 min        | 10 min      |
| ASA 5500-X series with FTD | 1.9 GB           | 290 MB     | 290 MB       | 12 min       | 42 min      |
| FTDv: VMware               | 1.9 GB           | 290 MB     | 290 MB       | 7 min        | 9 min       |
| Firepower 7000/8000 series | 3.7 GB           | 170 MB     | 650 MB       | 20 min       | 6 min       |
| ASA FirePOWER              | 4.2 GB           | 36 MB      | 600 MB       | 48 min       | 48 min      |
| NGIPSv                     | 2.1 GB           | 150 MB     | 450 MB       | 6 min        | 4 min       |

## Version 6.4.0.8 Time and Disk Space

Table 37: Time and Disk Space for Version 6.4.0.8

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time |
|----------------------------|------------------|------------|--------------|--------------|
| FMC                        | 5.0 GB           | 170 MB     | —            | 44 min       |
| FMCv: VMware               | 5.1 GB           | 170 MB     | —            | 32 min       |
| Firepower 1000 series      | 3.0 GB           | 3.0 GB     | 530 MB       | 18 min       |
| Firepower 2100 series      | 2.5 GB           | 2.5 GB     | 510 MB       | 18 min       |
| Firepower 4100 series      | 1.8 GB           | 1.8 GB     | 310 MB       | 14 min       |
| Firepower 9300             | 2.0 GB           | 2.0 GB     | 310 MB       | 11 min       |
| ASA 5500-X series with FTD | 1.8 GB           | 110 MB     | 290 MB       | 17 min       |
| FTDv: VMware               | 1.9 GB           | 110 MB     | 290 MB       | 12 min       |
| Firepower 7000/8000 series | 3.7 GB           | 190 MB     | 650 MB       | 25 min       |
| ASA FirePOWER              | 2.2 GB           | 110 MB     | 590 MB       | 16 min       |
| NGIPSv                     | 2.1 GB           | 150 MB     | 450 MB       | 9 min        |

## Version 6.4.0.7 Time and Disk Space

*Table 38: Time and Disk Space for Version 6.4.0.7*

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time |
|----------------------------|------------------|------------|--------------|--------------|
| FMC                        | 4.9 GB           | 170 MB     | —            | 41 min       |
| FMCv: VMware               | 5.1 GB           | 170 MB     | —            | 32 min       |
| Firepower 1000 series      | 2.9 GB           | 2.9 GB     | 530 MB       | 17 min       |
| Firepower 2100 series      | 2.4 GB           | 2.4 GB     | 500 MB       | 17 min       |
| Firepower 4100 series      | 1.7 GB           | 1.7 GB     | 310 MB       | 15 min       |
| Firepower 9300             | 2.4 GB           | 2.4 GB     | 310 MB       | 12 min       |
| ASA 5500-X series with FTD | 1.9 GB           | 110 MB     | 290 MB       | 18 min       |
| FTDv: VMware               | 1.8 GB           | 110 MB     | 290 MB       | 9 min        |
| Firepower 7000/8000 series | 3.7 GB           | 190 MB     | 650 MB       | 28 min       |
| ASA FirePOWER              | 4.2 GB           | 36 MB      | 590 MB       | 54 min       |
| NGIPSv                     | 2.3 GB           | 150 MB     | 450 MB       | 9 min        |

## Version 6.4.0.6 Time and Disk Space

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.

## Version 6.4.0.5 Time and Disk Space

*Table 39: Time and Disk Space for Version 6.4.0.5*

| Platform              | Space in /Volume | Space in / | Space on FMC | Upgrade Time |
|-----------------------|------------------|------------|--------------|--------------|
| FMC                   | 5.0 GB           | 170 MB     | —            | 39 min       |
| FMCv: VMware          | 3.7 GB           | 170 MB     | —            | 27 min       |
| Firepower 1000 series | 2.9 GB           | 2.9 GB     | 530 MB       | 26 min       |
| Firepower 2100 series | 2.5 GB           | 2.5 GB     | 500 MB       | 16 min       |
| Firepower 4100 series | 1.8 GB           | 1.8 GB     | 310 MB       | 12 min       |
| Firepower 9300        | 1.8 GB           | 1.8 GB     | 310 MB       | 11 min       |

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time |
|----------------------------|------------------|------------|--------------|--------------|
| ASA 5500-X series with FTD | 1.8 GB           | 110 MB     | 290 MB       | 20 min       |
| FTDv: VMware               | 1.8 GB           | 110 MB     | 290 MB       | 10 min       |
| Firepower 7000/8000 series | 3.6 GB           | 170 MB     | 650 MB       | 26 min       |
| ASA FirePOWER              | 4.1 GB           | 36 MB      | 590 MB       | 45 min       |
| NGIPSv                     | 2.1 GB           | 150 MB     | 450 MB       | 10 min       |

## Version 6.4.0.4 Time and Disk Space

Table 40: Time and Disk Space for Version 6.4.0.4

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time |
|----------------------------|------------------|------------|--------------|--------------|
| FMC                        | 4.4 GB           | 170 MB     | —            | 35 min       |
| FMCv: VMware               | 4.8 GB           | 170 MB     | —            | 31 min       |
| Firepower 1000 series      | 2.9 GB           | 2.9 GB     | 520 MB       | 28 min       |
| Firepower 2100 series      | 2.4 GB           | 2.4 GB     | 500 MB       | 10 min       |
| Firepower 4100 series      | 2.0 GB           | 2.0 GB     | 310 MB       | 12 min       |
| Firepower 9300             | 1.7 GB           | 1.7 GB     | 310 MB       | 10 min       |
| ASA 5500-X series with FTD | 1.8 GB           | 110 MB     | 290 MB       | 29 min       |
| FTDv: VMware               | 1.8 GB           | 110 MB     | 290 MB       | 8 min        |
| Firepower 7000/8000 series | 3.6 GB           | 170 MB     | 650 MB       | 24 min       |
| ASA FirePOWER              | 4.2 GB           | 36 MB      | 600 MB       | 55 min       |
| NGIPSv                     | 2.1 GB           | 150 MB     | 550 MB       | 10 min       |

## Version 6.4.0.3 Time and Disk Space

Table 41: Time and Disk Space for Version 6.4.0.3

| Platform | Space in /Volume | Space in / | Space on FMC | Upgrade Time |
|----------|------------------|------------|--------------|--------------|
| FMC      | 3.2 GB           | 24 MB      | —            | 34 min       |

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time |
|----------------------------|------------------|------------|--------------|--------------|
| FMCv: VMware               | 2.5 GB           | 23 MB      | —            | 25 min       |
| Firepower 1000 series      | 2.9 GB           | 2.9 GB     | 520 MB       | 22 min       |
| Firepower 2100 series      | 2.4 GB           | 2.4 GB     | 500 MB       | 19 min       |
| Firepower 4100 series      | 1.7 GB           | 1.7 GB     | 310 MB       | 12 min       |
| Firepower 9300             | 1.7 GB           | 1.7 GB     | 310 MB       | 14 min       |
| ASA 5500-X series with FTD | 1.8 GB           | 110 MB     | 290 MB       | 18 min       |
| FTDv: VMware               | 1.8 GB           | 110 MB     | 290 MB       | 12 min       |
| Firepower 7000/8000 series | 1.9 GB           | 21 MB      | 370 MB       | 20 min       |
| ASA FirePOWER              | 2.5 GB           | 2.5 GB     | 320 MB       | 28 min       |
| NGIPSv                     | 690 MB           | 21 MB      | 210 MB       | 8 min        |

## Version 6.4.0.2 Time and Disk Space

Table 42: Time and Disk Space for Version 6.4.0.2

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time |
|----------------------------|------------------|------------|--------------|--------------|
| FMC                        | 3.1 GB           | 24 MB      | —            | 39 min       |
| FMCv: VMware               | 2.5 GB           | 23 MB      | —            | 24 min       |
| Firepower 2100 series      | 1.9 GB           | 1.9 GB     | 480 MB       | 19 min       |
| Firepower 4100 series      | 2.3 GB           | 2.3 GB     | 290 MB       | 11 min       |
| Firepower 9300             | 1.7 GB           | 1.7 GB     | 290 MB       | 11 min       |
| ASA 5500-X series with FTD | 1.8 GB           | 110 MB     | 270 MB       | 21 min       |
| FTDv: VMware               | 1.2 GB           | 110 MB     | 270 MB       | 10 min       |
| Firepower 7000/8000 series | 1.9 GB           | 36 MB      | 350 MB       | 20 min       |
| ASA FirePOWER              | 2.0 GB           | 21 MB      | 300 MB       | 34 min       |
| NGIPSv                     | 630 MB           | 21 MB      | 190 MB       | 10 min       |

## Version 6.4.0.1 Time and Disk Space

Table 43: Time and Disk Space for Version 6.4.0.1

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time |
|----------------------------|------------------|------------|--------------|--------------|
| FMC                        | 1.8 GB           | 24 MB      | —            | 50 min       |
| FMCv: VMware               | 1.8 GB           | 23 MB      | —            | 20 min       |
| Firepower 2100 series      | 1.4 GB           | 1.4 GB     | 300 MB       | 17 min       |
| Firepower 4100 series      | 1.1 GB           | 1.1 GB     | 95 MB        | 9 min        |
| Firepower 9300             | 1.1 GB           | 1.1 GB     | 95 MB        | 10 min       |
| ASA 5500-X series with FTD | 550 MB           | 110 MB     | 76 MB        | 16 min       |
| FTDv: VMware               | 550 MB           | 110 MB     | 76 MB        | 15 min       |
| Firepower 7000/8000 series | 59 MB            | 21 MB      | 2 MB         | 14 min       |
| ASA FirePOWER              | 85 MB            | 20 MB      | 2 MB         | 30 min       |
| NGIPSv                     | 45 MB            | 21 MB      | 2 MB         | 10 min       |

## Version 6.4.0 Time and Disk Space

Table 44: Time and Disk Space for Version 6.4.0

| Platform                   | Space in /Volume | Space in / | Space on FMC | Upgrade Time |
|----------------------------|------------------|------------|--------------|--------------|
| FMC                        | 13.3 GB          | 26 MB      | —            | 41 min       |
| FMCv: VMware               | 13.6 GB          | 29 MB      | —            | 30 min       |
| Firepower 2100 series      | 12 MB            | 8.9 GB     | 950 MB       | 20 min       |
| Firepower 4100 series      | 10 MB            | 7.5 GB     | 920 MB       | 6 min        |
| Firepower 9300             | 10 MB            | 7.7 GB     | 920 MB       | 7 min        |
| ASA 5500-X series with FTD | 9.0 GB           | 110 KB     | 1.1 GB       | 24 min       |
| FTDv: VMware               | 7.5 GB           | 100 KB     | 1.1 GB       | 12 min       |
| Firepower 7000/8000 series | 7.7 GB           | 19 MB      | 980 MB       | 34 min       |
| ASA FirePOWER              | 11.5 GB          | 22 MB      | 1.3 GB       | 66 min       |

| <b>Platform</b> | <b>Space in /Volume</b> | <b>Space in /</b> | <b>Space on FMC</b> | <b>Upgrade Time</b> |
|-----------------|-------------------------|-------------------|---------------------|---------------------|
| NGIPSv          | 6.5 GB                  | 19 MB             | 840 MB              | 16 min              |





## 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, on page 67](#)
- [Installation Guides, on page 69](#)

## 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 be 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 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 45: 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 46: 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 47: Scenarios for Full Reimages**

| Model                                          | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firepower 1000 series<br>Firepower 2100 series | If you use the <b>erase configuration</b> 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.<br><br>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).<br><br>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 48: Installation Guides**

| Platform                        | Guide                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>FMC</b>                      |                                                                                                        |
| FMC 1600, 2600, 4600            | <a href="#">Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide</a>           |
| FMC 1000, 2500, 4500            | <a href="#">Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide</a>           |
| FMC 750, 1500, 2000, 3500, 4000 | <a href="#">Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide</a> |
| FMCv                            | <a href="#">Cisco Secure Firewall Management Center Virtual Getting Started Guide</a>                  |
| <b>FTD</b>                      |                                                                                                        |

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



# CHAPTER 6

## Open and Resolved Bugs

This document lists open and resolved bugs for Version 6.4 devices and management centers.



**Important** 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. We also do not list open bugs for patches. If you have a support contract, you can obtain up-to-date bug lists with the [Cisco Bug Search Tool](#).

- [Open Bugs, on page 71](#)
- [Resolved Bugs, on page 75](#)

## Open Bugs

### Open Bugs in Version 6.4.0

Table last updated: 2022-11-02

**Table 49: Open Bugs in Version 6.4.0**

| Bug ID                     | Headline                                                                                          |
|----------------------------|---------------------------------------------------------------------------------------------------|
| <a href="#">CSCvo00852</a> | Lina CPU is low and traffic gets lost for FTDv ESXi 12 core and FTDv KVM 12 core platforms        |
| <a href="#">CSCvo03589</a> | App agent heart beat can miss in MI scenario                                                      |
| <a href="#">CSCvo40478</a> | FMC Dashboard is showing incorrect value as FMC latest product updates                            |
| <a href="#">CSCvo80725</a> | vFTD 6.4 fails to establish OSPF adjacency due to "ERROR: ip_multicast_ctl failed to get channel" |
| <a href="#">CSCvp06568</a> | NAP policy/SSL policy name name unknown in syslog on 6.3 FTD managed by 6.4 FMC                   |
| <a href="#">CSCvp19669</a> | Users not showing correctly in FDM Events                                                         |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvp21403</a> | Validation: Data Plane - Management Access does not handle RA-VPN port collision                     |
| <a href="#">CSCvp23703</a> | first boot script S97compress-client-resources failed in FTD quietly.                                |
| <a href="#">CSCvp25570</a> | Unable to create RAVPN Conn-Profile if group-policy attr and FQDN are edited in the same wizard flow |
| <a href="#">CSCvp29817</a> | Fail to update login history when converting TempID to RealID. 1x log per ID, history lost           |
| <a href="#">CSCvp30194</a> | ASA SFR: seeing "Error importing SFO: Unable to load container" while trying to import ACP with IPS  |
| <a href="#">CSCvp33797</a> | User with sessions on FMC not properly updated after user info is downloaded from AD                 |
| <a href="#">CSCvp37229</a> | few preprocessors won't be enabled if enable from 'My Changes' layer of Policy Layers                |
| <a href="#">CSCvp45752</a> | If a custom app is added in sub domain, snort doesn't restart on registered devices at older version |
| <a href="#">CSCvp47260</a> | Generating troubleshooting files stopped in Japanese                                                 |
| <a href="#">CSCvp47535</a> | Newly Added Application protocol are not able to view under Hosts                                    |
| <a href="#">CSCvp48523</a> | Access Policy doesn't reflect the modified user correctly                                            |
| <a href="#">CSCvp48525</a> | Unable to edit scheduled task on Task details                                                        |
| <a href="#">CSCvp48534</a> | Unable to add categories in intrusion rule                                                           |
| <a href="#">CSCvp48545</a> | Unable to Create Alerts with Japanese Name                                                           |
| <a href="#">CSCvp48565</a> | VPN Troubleshooting logs setup takes abnormal time span                                              |
| <a href="#">CSCvp56916</a> | S2S VPN Wizard showing no pre-configured certificates available                                      |
| <a href="#">CSCvp56951</a> | FDM/FTDvirtual unable to support/deploy "ignore-ipsec-keyusage" flexconfig object                    |
| <a href="#">CSCvp57096</a> | Upgrade to 6.4.0 may fail due to ids_event_msg_map table having NULL entries in the msg field        |
| <a href="#">CSCvp59960</a> | Network discovery not working with network groups containing literals - user or Cisco created.       |
| <a href="#">CSCvq29993</a> | 6.4.0-102 2140 w/ SSL policy runs out of 1550 and 9472 blocks. doesn't recover                       |
| <a href="#">CSCvq33956</a> | Optimizing memory allocation of deploy process(AQS subgroup) to allow huge policy deployments        |
| <a href="#">CSCvq36298</a> | Cannot change MTU size on ASAv/FTDv after upgrade                                                    |
| <a href="#">CSCvq78471</a> | Removing a BVI and its DHCP pool simultaneously causes policy deploy failures                        |

| Bug ID                     | Headline                                                                                          |
|----------------------------|---------------------------------------------------------------------------------------------------|
| <a href="#">CSCvr01675</a> | Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability              |
| <a href="#">CSCvr35854</a> | Apache HTTP Server URL Normalization Denial of Service Vulnerability                              |
| <a href="#">CSCvr35855</a> | Apache HTTP Server mod_http2 Use-After-Free Denial of Service Vulnerab                            |
| <a href="#">CSCvr35856</a> | Apache HTTP Server mod_auth_digest Race Condition Access Control Bypas                            |
| <a href="#">CSCvr57468</a> | RunQuery not compatible with Java Development Kit 13                                              |
| <a href="#">CSCvs05066</a> | Snort file mempool corruption leads to performance degradation and process failure.               |
| <a href="#">CSCvs24215</a> | Firepower Device Manager (FDM) option to disable SSL rekey is not reflected on the config         |
| <a href="#">CSCvs37065</a> | Snort crash due to missing data in /ngfw/var/sf/fwcfg/interface_info.conf file                    |
| <a href="#">CSCvs50931</a> | Policy deployment fails subsequent to SRU                                                         |
| <a href="#">CSCvs56923</a> | SQL client not able to query FMC using external database access                                   |
| <a href="#">CSCvs61881</a> | Certificate mapping for AnyConnect on FTD no longer working.                                      |
| <a href="#">CSCvs74586</a> | Firepower FTD transparent does not decode non-ip packets                                          |
| <a href="#">CSCvs82829</a> | Calls fail once anyconnect configuration is added to the site to site VPN tunnel                  |
| <a href="#">CSCvs88186</a> | Using same variable names between byte_extract and byte_math accross SIDs breaks snort validation |
| <a href="#">CSCvt01763</a> | Application classification is not retried if a flow is marked brute force failed.                 |
| <a href="#">CSCvt03557</a> | The time/timezone set on GUI is inconsistent on Virtual firepower management center               |
| <a href="#">CSCvt06666</a> | SFR httpsd process down after upgrade failure from 6.3.0.4 to 6.4                                 |
| <a href="#">CSCvt16642</a> | FMC not sending some audit messages to remote syslog server                                       |
| <a href="#">CSCvt16723</a> | log rotation for ngfw-onbox logs NOT happening at expected log size                               |
| <a href="#">CSCvt18051</a> | RabbitMQ keeps crashing if dets file is corrupt                                                   |
| <a href="#">CSCvt20235</a> | Firepower 4100 series all FTW interfaces link flap at the same time but occur rarely              |
| <a href="#">CSCvt21986</a> | Inconsistent allocation of cores for snort and lina between instances                             |
| <a href="#">CSCvt34894</a> | Snort consumes memory causing block depletion                                                     |
| <a href="#">CSCvt35233</a> | Excessive logging from the daq modules process_snort_verdict verdict blacklist                    |
| <a href="#">CSCvt35730</a> | FDM deployment error if 2nd tunnel has overlapping crypto ACL                                     |
| <a href="#">CSCvt37745</a> | Traceback while secondary reverting from active to standby                                        |
| <a href="#">CSCvt42955</a> | SID 26932 false positive which triggers on QUIC traffic instead of NTP                            |

| Bug ID                     | Headline                                                                                        |
|----------------------------|-------------------------------------------------------------------------------------------------|
| <a href="#">CSCvt52607</a> | Reduce SSL HW mode flow table memory usage to reduce the probability of Snort going in D state  |
| <a href="#">CSCvt56923</a> | FTD manual certificate enrollment fails with "&" (ampersand) in Organisation subject field      |
| <a href="#">CSCvt62147</a> | ASA traceback and reload on process name LINA                                                   |
| <a href="#">CSCvt63407</a> | FP 2k running FTD 6.4.0.7 traceback and reload on process name LINA                             |
| <a href="#">CSCvt64696</a> | AAA RADIUS server connection failure                                                            |
| <a href="#">CSCvt66136</a> | 6.4.0.9 upgrade from 6.4.0 with CC mode causes httpd.conf to have an incorrect config           |
| <a href="#">CSCvt66875</a> | AppId caches proxy IP instead of tunneled IP for ultrasurf                                      |
| <a href="#">CSCvt67832</a> | FTD Traceback and Reload on Lina thread due to lock contention                                  |
| <a href="#">CSCvt68131</a> | FTD traceback and reload on thread "IKEv2 Mgd Timer Thread"                                     |
| <a href="#">CSCvt70854</a> | 6.6.0-90: [Firepower 1010] Tomcat restarted during SRU update because of out of memory          |
| <a href="#">CSCvt70866</a> | sfiproxy may fail to bind listeners for secondary FMC                                           |
| <a href="#">CSCvt72683</a> | NAT policy configuration after NAT policy deployment on FP 8130 is not seen                     |
| <a href="#">CSCvt80126</a> | ASA traceback and reload for the CLI "show asp table socket 18421590 det"                       |
| <a href="#">CSCvt80172</a> | Supervisor software needs to be upgraded to address CVE-2017-11610                              |
| <a href="#">CSCvt86906</a> | Stunnel 5.00 through 5.13, when using the redirect option, does not re                          |
| <a href="#">CSCvt87064</a> | WebCore/platform/network/soup/SocketStreamHandleImplSoup.cpp in the li                          |
| <a href="#">CSCvu32449</a> | FDM: AnyConnect "Validation failed due to duplicate name:"                                      |
| <a href="#">CSCvu43355</a> | FTD Lina traceback and reload in the QOS function                                               |
| <a href="#">CSCvu44697</a> | Firepower 4100/9300 - Fail-to-wire (FTW) EPM ports link flap during show tech collection        |
| <a href="#">CSCvu46584</a> | In GNOME glib-networking through 2.64.2, the implementation of GTIsCli                          |
| <a href="#">CSCvu53481</a> | FTD upgrade fails due to HA config sync taking over 1h                                          |
| <a href="#">CSCvu56286</a> | FDM - New firewall session getting created after performing HA Failover for traffic in progress |
| <a href="#">CSCvu61711</a> | FMC cannot add ACL rule with geolocation because "An internal error occurred."                  |
| <a href="#">CSCvu70529</a> | Binary rules (SO rules) are not loaded when snort reloads                                       |

| Bug ID                     | Headline                                                                 |
|----------------------------|--------------------------------------------------------------------------|
| <a href="#">CSCvu85127</a> | Unable to deploy if device with same UUID is trying to connect           |
| <a href="#">CSCvv00254</a> | 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. We *strongly* recommend you use the latest build. 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 50: Version 6.4 New Builds**

| Version | New Build | Released   | Packages           | Platforms                                                      | Resolves                                                                                                                                                                                                                                                                                                                                    |
|---------|-----------|------------|--------------------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.4.0.2 | 35        | 2019-07-03 | Upgrade            | FMC/FMCv<br>FTD/FTDv,<br>except<br>Firepower<br>1000<br>series | <a href="#">CSCvq34224</a> : Firepower Primary Detection Engine process terminated after Manager upgrade<br><br>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<br>Reimage | FMC/FMCv                                                       | <a href="#">CSCvr95287</a> : Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability<br><br>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 6.4.0.17

Table last updated: 2020-09-28

**Table 51: Resolved Bugs in Version 6.4.0.17**

| Bug ID                     | Headline                                                 |
|----------------------------|----------------------------------------------------------|
| <a href="#">CSCvs74586</a> | Firepower FTD transparent does not decode non-ip packets |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvt25221</a> | FTD traceback in Thread Name cli_xml_server when deploying QoS policy                                |
| <a href="#">CSCvv24552</a> | ASA/FTD: Traceback and Reload in Thread Name: Route Table Timestamp Update                           |
| <a href="#">CSCvx00655</a> | ASA/SFR service card failure due to timeout getting CriticalStatus from PM                           |
| <a href="#">CSCvx09860</a> | 700-1158: 9 out of 150 VTI sessions down                                                             |
| <a href="#">CSCvy26511</a> | Tune unmanaged disk alert thresholds for low end platforms                                           |
| <a href="#">CSCvy30077</a> | deploying anyconnect group-alias causes breaking HA and ungraceful failover                          |
| <a href="#">CSCvz00961</a> | AnyConnect connection failure related to ASA truncated/corrupt config                                |
| <a href="#">CSCvz41551</a> | FP2100: ASA/FTD with threat-detection statistics may traceback and reload in Thread Name 'lina'      |
| <a href="#">CSCvz54471</a> | ASA:Failed ASA in HA pair not recovering by itself, after an "HA state progression failed"           |
| <a href="#">CSCvz70958</a> | High Control Plane CPU due to dhcpp_add_ip1_stby                                                     |
| <a href="#">CSCwa04262</a> | Cisco ASA Software SSL VPN Client-Side Request Smuggling Vulnerability via "/"URI                    |
| <a href="#">CSCwa72528</a> | user-name from certificate feature does not work with SER option                                     |
| <a href="#">CSCwa81427</a> | External Authorization randomly fails on ASA when using LDAP over SSL                                |
| <a href="#">CSCwb44848</a> | ASA/FTD Traceback and reload in Process Name: lina                                                   |
| <a href="#">CSCwc03507</a> | No-buffer drops on Internal Data interfaces despite little evidence of CPU hog                       |
| <a href="#">CSCwc64923</a> | ASA/FTD may traceback and reload in Thread Name 'lina' ip routing ndbshr                             |
| <a href="#">CSCwc67687</a> | ASA HA failover triggers HTTP server restart failure and ASDM outage                                 |
| <a href="#">CSCwc68656</a> | ASA CLI for TCP Maximum unprocessed segments                                                         |
| <a href="#">CSCwc74841</a> | FMC RSS Feed broken because FeedBurner is no longer active - "Unable to parse feed"                  |
| <a href="#">CSCwc89796</a> | ASA/FTD may traceback and reload in Thread Name 'appagent_async_client_receive_thread' hog detection |
| <a href="#">CSCwc95290</a> | ESP rule missing in vpn-context may cause IPSec traffic drop                                         |
| <a href="#">CSCwc99242</a> | ISA3000 LACP channel member SFP port suspended after reload                                          |
| <a href="#">CSCwd04210</a> | ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT                                          |
| <a href="#">CSCwd05772</a> | Cisco FXOS Software Arbitrary File Write Vulnerability                                               |
| <a href="#">CSCwd06005</a> | ASA/FTD Cluster Traceback and Reload during node leave                                               |

| Bug ID                     | Headline                                                                                       |
|----------------------------|------------------------------------------------------------------------------------------------|
| <a href="#">CSCwd11855</a> | ASA/FTD may traceback and reload in Thread Name 'ikev2_fo_event'                               |
| <a href="#">CSCwd19053</a> | ASA/FTD may traceback with large number of network objects deployment using distribute-list    |
| <a href="#">CSCwd22413</a> | EIGRPv6 - Crashed with "mem_lock: Assertion mem_refcount' failed" on LINA.                     |
| <a href="#">CSCwd23188</a> | ASA/FTD may traceback and reload in Thread Name 'lina'                                         |
| <a href="#">CSCwd25256</a> | ASA/FTD Transactional Commit may result in mismatched rules and traffic loss                   |
| <a href="#">CSCwd26867</a> | Device should not move to Active state once Reboot is triggered                                |
| <a href="#">CSCwd31181</a> | Lina traceback and reload - VPN parent channel (SAL) has an invalid underlying channel         |
| <a href="#">CSCwd33811</a> | Cluster registration is failing because DATA_NODE isn't joining the cluster                    |
| <a href="#">CSCwd35726</a> | Cisco FXOS Software Arbitrary File Write Vulnerability                                         |
| <a href="#">CSCwd38774</a> | ASA: Traceback and reload due to clientless webvpn session closure                             |
| <a href="#">CSCwd38775</a> | ASA/FTD may traceback and reload in Thread lina                                                |
| <a href="#">CSCwd38805</a> | Syslog 106016 is not rate-limited by default                                                   |
| <a href="#">CSCwd39468</a> | ASA/FTD Traceback and reload when configuring ISAKMP captures on device                        |
| <a href="#">CSCwd40260</a> | Serviceability Enhancement - Unable to parse payload are silently drop by ASA/FTD              |
| <a href="#">CSCwd41083</a> | ASA traceback and reload due to DNS inspection                                                 |
| <a href="#">CSCwd48633</a> | ASA - traceback and reload when Webvpn Portal is used                                          |
| <a href="#">CSCwd49018</a> | After establishing multicontext HA ,SNMP no longer outputs interface information.              |
| <a href="#">CSCwd50218</a> | ASA restore is not applying vlan configuration                                                 |
| <a href="#">CSCwd53135</a> | ASA/FTD: Object Group Search Syslog for flows exceeding threshold                              |
| <a href="#">CSCwd56254</a> | "show tech-support" generation does not include "show inventory" when run on FTD               |
| <a href="#">CSCwd56296</a> | FTD Lina traceback and reload in Thread Name 'IP Init Thread'                                  |
| <a href="#">CSCwd56774</a> | Misleading drop reason in "show asp drop"                                                      |
| <a href="#">CSCwd56995</a> | Clientless Accessing Web Contents using application/octet-stream vs text/plain                 |
| <a href="#">CSCwd61016</a> | ASA: Standby may get stuck in "Sync Config" status upon reboot when there is EEM is configured |
| <a href="#">CSCwd63580</a> | FPR2100: Increase in failover convergence time with ASA in Appliance mode                      |
| <a href="#">CSCwd63961</a> | AC clients fail to match DAP rules due to attribute value too large                            |

| Bug ID                     | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCwd69454</a> | Port-channel interfaces of secondary unit are in waiting status after reload                        |
| <a href="#">CSCwd74116</a> | S2S Tunnels do not come up due to DH computation failure caused by DSID Leak                        |
| <a href="#">CSCwd78624</a> | ASA configured with HA may traceback and reload with multiple input/output error messages           |
| <a href="#">CSCwd82235</a> | LINA Traceback on FPR-1010 under Thread Name: update_cpu_usage                                      |
| <a href="#">CSCwd83141</a> | CCL/CLU filters are not working correctly                                                           |
| <a href="#">CSCwd84868</a> | Observing some devcmd failures and checkheaps traceback when flow offload is not used.              |
| <a href="#">CSCwd85927</a> | Traceback and reload when webvpn users match DAP access-list with 36k elements                      |
| <a href="#">CSCwd88641</a> | Deployment changes to push VDB package based on Device model and snort engine                       |
| <a href="#">CSCwd89095</a> | Stratix5950 and ISA3000 LACP channel member SFP port suspended after reload                         |
| <a href="#">CSCwd91421</a> | ASA/FTD may traceback and reload in logging_cfg processing                                          |
| <a href="#">CSCwd93376</a> | Clientless VPN users are unable to download large files through the WebVPN portal                   |
| <a href="#">CSCwd94096</a> | Anyconnect users unable to connect when ASA using different authentication and authorization server |
| <a href="#">CSCwd95436</a> | Primary ASA traceback upon rebooting the secondary                                                  |
| <a href="#">CSCwd95908</a> | ASA/FTD traceback and reload, Thread Name: rtcli async executor process                             |
| <a href="#">CSCwd96755</a> | ASA is unexpected reload when doing backup                                                          |
| <a href="#">CSCwd97020</a> | ASA/FTD: External IDP SAML authentication fails with Bad Request message                            |
| <a href="#">CSCwe03529</a> | FTD traceback and reload while deploying PAT POOL                                                   |
| <a href="#">CSCwe05913</a> | FTD traceback/reloads - Icmp error packet processing involves snp_nat_xlate_identity                |
| <a href="#">CSCwe07722</a> | Cluster data unit drops non-VPN traffic with ASP reason "VPN reclassify failure                     |
| <a href="#">CSCwe14174</a> | FTD - 'show memory top-usage' providing improper value for memory allocation                        |
| <a href="#">CSCwe18974</a> | ASA/FTD may traceback and reload in Thread Name: CTM Daemon                                         |
| <a href="#">CSCwe20043</a> | 256-byte memory block gets depleted on start if jumbo frame is enabled with FTD on ASA5516          |
| <a href="#">CSCwe21187</a> | ASA/FTD may drop multicast packets due to no-mcast-intrf ASP drop reason until UDP timeout expires  |
| <a href="#">CSCwe21280</a> | Multicast connection built or teardown syslog messages may not always be generated                  |
| <a href="#">CSCwe29529</a> | FTD MI does not adjust PVID on vlans attached to BVI                                                |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCwe29583</a> | ASA/FTD may traceback and reload in Thread Name 'None' at lua_getinfo                                |
| <a href="#">CSCwe29850</a> | ASA/FTD Show chunkstat top command implementation                                                    |
| <a href="#">CSCwe36176</a> | ASA/FTD: High failover delay with large number of (sub)interfaces and http server enabled            |
| <a href="#">CSCwe38029</a> | Multiple traceback seen on standby unit.                                                             |
| <a href="#">CSCwe40463</a> | Stale IKEv2 SA formed during simultaneous IKE SA handling when missing delete from the peer          |
| <a href="#">CSCwe42061</a> | Deleting a BVI in FTD interfaces is causing packet drops in other BVIs                               |
| <a href="#">CSCwe44311</a> | FP2100:Update LINA asa.log files to avoid recursive messages-&lt;date>.1.gz rotated filenames        |
| <a href="#">CSCwe44672</a> | Syslog ASA-6-611101 is generated twice for a single ssh connection                                   |
| <a href="#">CSCwe45779</a> | ASA/FTD drops traffic to BVI if floating conn is not default value due to no valid adjacency         |
| <a href="#">CSCwe51286</a> | ASA/FTD may traceback and reload in Thread Name 'lina'                                               |
| <a href="#">CSCwe59737</a> | ASA/FTD reboots due to traceback pointing to watchdog timeout on p3_tree_lookup                      |
| <a href="#">CSCwe61928</a> | PIM register packets are not sent to RP after a reload if FTD uses a default gateway to reach the RP |
| <a href="#">CSCwe61969</a> | ASA Multicontext 'management-only' interface attribute not synced during creation                    |
| <a href="#">CSCwe63067</a> | ASA/FTD may traceback and reload in Thread Name 'lina' due to due to tcp intercept stat              |
| <a href="#">CSCwe63232</a> | ASA/FTD: Ensure flow-offload states within cluster are the same                                      |
| <a href="#">CSCwe64404</a> | ASA/FTD may traceback and reload                                                                     |
| <a href="#">CSCwe64563</a> | The command "neighbor x.x.x.x ha-mode graceful-restart" removed when deleting any created context    |
| <a href="#">CSCwe65634</a> | ASA - Standby device may traceback and reload during synchronization of ACL DAP                      |
| <a href="#">CSCwe66132</a> | ASA/FTD may traceback and reload in Thread Name 'lina'                                               |
| <a href="#">CSCwe67751</a> | Last fragment from SIP IPv6 packets has MF equal to 1, flagging that more packets are expected       |
| <a href="#">CSCwe67816</a> | ASA / FTD Traceback and reload when removing isakmp capture                                          |
| <a href="#">CSCwe74328</a> | AnyConnect - mobile devices are not able to connect when hostscan is enabled                         |
| <a href="#">CSCwe78977</a> | ASA/FTD may traceback and reload in Thread Name 'pix_flash_config_thread'                            |

| Bug ID                     | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCwe79072</a> | ASA/FTD may traceback and reload in Thread Name 'lina'                                              |
| <a href="#">CSCwe80278</a> | Dynamic interface NAT rules cause SSH/ICMP to fail with nat-no-xlate-to-pat-pool in ASA cluster     |
| <a href="#">CSCwe85432</a> | ASA/FTD traceback and reload on thread DATAPATH-14-11344 when SIP inspection is enabled             |
| <a href="#">CSCwe86225</a> | ASA/FTD traceback and reload due citing thread name: cli_xml_server in tm_job_add                   |
| <a href="#">CSCwe89030</a> | Serial number attribute from the subject DN of certificate should be taken as the username          |
| <a href="#">CSCwe90720</a> | ASA Traceback and reload in parse thread due ha_msg corruption                                      |
| <a href="#">CSCwe92905</a> | ngfwManager process continuously restarting leading to ZMQ Out of Memory traceback                  |
| <a href="#">CSCwe93489</a> | Threat-detection does not recognize exception objects with a prefix in IPv6                         |
| <a href="#">CSCwe93532</a> | ASA/FTD may traceback and reload in Thread Name 'lina'.                                             |
| <a href="#">CSCwe95757</a> | ASA/FTD may traceback and reload in Thread Name 'lina'                                              |
| <a href="#">CSCwf04831</a> | ASA/FTD may traceback and reload in Thread Name 'ci/console'                                        |
| <a href="#">CSCwf10910</a> | FTD : Traceback in ZMQ running 7.3.0                                                                |
| <a href="#">CSCwf14126</a> | ASA Traceback and reload citing process name 'lina'                                                 |
| <a href="#">CSCwf14811</a> | TCP normalizer needs stats that show actions like packet drops                                      |
| <a href="#">CSCwf17042</a> | ASDM replaces custom policy-map with default map on class inspect options at backup restore.        |
| <a href="#">CSCwf20338</a> | ASA may traceback and reload in Thread Name 'DHCPv6 Relay'                                          |
| <a href="#">CSCwf22005</a> | ASA Packet-tracer displays the first ACL rule always, though matches the right ACL                  |
| <a href="#">CSCwf23564</a> | Unable to establish BGP when using MD5 authentication over GRE TUNNEL and FTD as passthrough device |
| <a href="#">CSCwf26534</a> | ASA/FTD: Connection information in SIP-SDP header remains untranslated with destination static Any  |
| <a href="#">CSCwf33574</a> | ASA access-list entries have the same hash after upgrade                                            |
| <a href="#">CSCwf33904</a> | [IMS_7_4_0] - Virtual FDM Upgrade fails: HA configStatus='OUT_OF_SYNC after UpgradeOnStandby        |
| <a href="#">CSCwf42144</a> | ASA/FTD may traceback and reload citing process name "lina"                                         |
| <a href="#">CSCwf44537</a> | 99.20.1.16 lina crash on nat_remove_policy_from_np                                                  |
| <a href="#">CSCwf49573</a> | ASA/FTD: Traceback and reload when issuing 'show memory webvpn all objects'                         |

| Bug ID                     | Headline                                                                       |
|----------------------------|--------------------------------------------------------------------------------|
| <a href="#">CSCwf54418</a> | Reduce time taken to clear stale IKEv2 SAs formed after Duplicate Detection    |
| <a href="#">CSCwf78321</a> | ASA: Checkheaps traceback and reload due to Clientless WebVPN                  |
| <a href="#">CSCwf95147</a> | OSPFv3 Traffic is Centralized in Transparent Mode                              |
| <a href="#">CSCwh13821</a> | ASA/FTD may traceback and reload in when changing capture buffer size          |
| <a href="#">CSCwh23100</a> | Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability |
| <a href="#">CSCwh23567</a> | PAC Key file missing on standby on reload                                      |

## Resolved Bugs in Version 6.4.0.16

Table last updated: 2022-11-21

**Table 52: Resolved Bugs in Version 6.4.0.16**

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvs27235</a> | nat-no-xlate-to-pat-pool drops when master leaves cluster and after rebalance                        |
| <a href="#">CSCvu84127</a> | Firepower may reboot for no apparent reason                                                          |
| <a href="#">CSCvu87906</a> | Backup file keep growing in 6.6.0-90 (Unified Event Files are Incorrectly Included In Backup)        |
| <a href="#">CSCvu96069</a> | HA during failover active having traffic with high CPU the system may reload unexpected              |
| <a href="#">CSCvv52349</a> | No utility to handle XFS corruption on 2100/1000 series Firepower devices                            |
| <a href="#">CSCvv97527</a> | asa config timeout command breaks snort's DAQ configuration                                          |
| <a href="#">CSCvw29647</a> | FTD: NAS-IP-Address:0.0.0.0 in Radius Request packet as network interface for aaa-server not defined |
| <a href="#">CSCvw52083</a> | FXOS logrotate does not rotate properly all the log files                                            |
| <a href="#">CSCvw72260</a> | ASA upgrade failed with: "CSP directory does not exist - STOP_FAILED Application_Not_Found"          |
| <a href="#">CSCvw82067</a> | ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic                                |
| <a href="#">CSCvw94160</a> | CIAM: openssl CVE-2020-1971                                                                          |
| <a href="#">CSCvw98315</a> | FXOS reporting old FTD version after FTD upgrade to 6.7.0                                            |
| <a href="#">CSCvx89827</a> | Not able to set Bangkok time zone in FPR 2110                                                        |
| <a href="#">CSCvy50598</a> | BGP table not removing connected route when interface goes down                                      |
| <a href="#">CSCvy65178</a> | Need dedicated Rx rings for to the box BGP traffic on Firepower platform                             |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvy73130</a> | FP4100 platform: Active-Standby changed to dual Active after running "show conn" command             |
| <a href="#">CSCvy86817</a> | Cruz ASIC CLU filter has the incorrect src/dst IP subnet when a custom CCL IP subnet is set          |
| <a href="#">CSCvy90162</a> | Traceback watchdog bark at Unicorn Proxy Thread from scaled AC-SSL-SAML Auth TVM profile             |
| <a href="#">CSCvy95520</a> | Cisco Firepower Management Center and Firepower Threat Defense Software SSH DoS Vulnerability        |
| <a href="#">CSCvy96895</a> | ASA disconnects the VTY session using of Active IP address and Standby MAC address after failed over |
| <a href="#">CSCvz05767</a> | FP-1010 HA link goes down or New hosts unable to connect to the device                               |
| <a href="#">CSCvz15755</a> | FTD - Port-channel not coming up after upgrade and may generate core file                            |
| <a href="#">CSCvz55140</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 117, seq 17)                                 |
| <a href="#">CSCvz60142</a> | ASA/FTD stops serving SSL connections                                                                |
| <a href="#">CSCvz61689</a> | Port-channel member interfaces are lost and status is down after software upgrade                    |
| <a href="#">CSCvz71596</a> | "Number of interfaces on Active and Standby are not consistent" should trigger warning syslog        |
| <a href="#">CSCvz75988</a> | Inconsistent logging timestamp with RFC5424 enabled                                                  |
| <a href="#">CSCvz78816</a> | ASA disconnects the ssh, https session using of Active IP address and Standby MAC address after FO   |
| <a href="#">CSCvz83432</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 121, seq 18)                                 |
| <a href="#">CSCvz85683</a> | Wrong syslog message format for 414004                                                               |
| <a href="#">CSCvz85913</a> | ASN.1 strings are represented internally within OpenSSL as an ASN1_STR for CISCO-SSL-1.0.2           |
| <a href="#">CSCwa04395</a> | User Agent session processing crashes SFDataCorrelator on 6.6.5 standalone sensors                   |
| <a href="#">CSCwa05385</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 19)                                 |
| <a href="#">CSCwa20758</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20)                                 |
| <a href="#">CSCwa32286</a> | WR6, WR8 and LTS18 commit id update in CCM layer (sprint 125, seq 21)                                |
| <a href="#">CSCwa41936</a> | Cisco FTD Bleichenbacher Attack Vulnerability                                                        |
| <a href="#">CSCwa46905</a> | WM 1010 speed/duplex setting is not getting effect and causes unstable interface                     |
| <a href="#">CSCwa50145</a> | FPR8000 sensor UI login creates shell user with basic privileges                                     |

| Bug ID                     | Headline                                                                                               |
|----------------------------|--------------------------------------------------------------------------------------------------------|
| <a href="#">CSCwa55562</a> | Different CG-NAT port-block allocated for same source IP causing per-host PAT port block exhaustion    |
| <a href="#">CSCwa67884</a> | Conditional flow-offload debugging produces no output                                                  |
| <a href="#">CSCwa75966</a> | ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped     |
| <a href="#">CSCwa76564</a> | ASDM session/quota count mismatch in ASA when multiple context switch before and after failover        |
| <a href="#">CSCwa76822</a> | Tune throttling flow control on syslog-ng destinations                                                 |
| <a href="#">CSCwa90615</a> | WR8 and LTS18 commit id update in CCM layer (seq 24)                                                   |
| <a href="#">CSCwa91070</a> | Cgroup triggering oom-k for backup process                                                             |
| <a href="#">CSCwb01983</a> | Cisco Firepower Management Center Cross-Site Scripting Vulnerability                                   |
| <a href="#">CSCwb01990</a> | Cisco Firepower Management Center Cross-Site Scripting Vulnerability                                   |
| <a href="#">CSCwb01995</a> | Cisco Firepower Management Center Cross-Site Scripting Vulnerability                                   |
| <a href="#">CSCwb02006</a> | Cisco Firepower Management Center Cross-Site Scripting Vulnerability                                   |
| <a href="#">CSCwb02026</a> | Cisco Firepower Management Center Cross-Site Scripting Vulnerability                                   |
| <a href="#">CSCwb05291</a> | Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability                         |
| <a href="#">CSCwb06847</a> | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'                                     |
| <a href="#">CSCwb07908</a> | Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0                                            |
| <a href="#">CSCwb08644</a> | ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test                  |
| <a href="#">CSCwb13294</a> | WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 25)                                            |
| <a href="#">CSCwb15795</a> | Audit message not generated by: no logging enable from ASA v9.12                                       |
| <a href="#">CSCwb17963</a> | Unable to identify dynamic rate limiting mechanism & not following msg limit per/sec at syslog server. |
| <a href="#">CSCwb24039</a> | ASA traceback and reload on routing                                                                    |
| <a href="#">CSCwb26212</a> | ASA drops existing anyconnect sessions and stop accepting new anyconnect sessions                      |
| <a href="#">CSCwb28849</a> | ASA/FTD: Mitigation of OpenSSL vulnerability CVE-2022-0778                                             |
| <a href="#">CSCwb41361</a> | WR8, LTS18 and LTS21 commit id update in CCM layer (seq 26)                                            |
| <a href="#">CSCwb41854</a> | Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability                             |
| <a href="#">CSCwb46949</a> | LTS18 commit id update in CCM layer (seq 27)                                                           |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCwb51707</a> | ASA Traceback and reload in process name: lina                                                       |
| <a href="#">CSCwb52401</a> | Cisco Firepower Threat Defense Software Privilege Escalation Vulnerability                           |
| <a href="#">CSCwb53172</a> | FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated                            |
| <a href="#">CSCwb53328</a> | ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url                   |
| <a href="#">CSCwb53694</a> | Cisco Firepower Management Center Software XML External Entity Injection Vulnerability               |
| <a href="#">CSCwb57615</a> | Configuring pbr access-list with line number failed.                                                 |
| <a href="#">CSCwb59465</a> | ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem |
| <a href="#">CSCwb59488</a> | ASA/FTD Traceback in memory allocation failed                                                        |
| <a href="#">CSCwb61901</a> | Cisco Firepower Management Center Cross-Site Scripting Vulnerability                                 |
| <a href="#">CSCwb61908</a> | Cisco Firepower Management Center Cross-Site Scripting Vulnerability                                 |
| <a href="#">CSCwb65447</a> | FTD: AAB cores are not complete and not decoding                                                     |
| <a href="#">CSCwb65718</a> | FMC is stuck on loading SI objects page                                                              |
| <a href="#">CSCwb66761</a> | Cisco Firepower Threat Defense Software Generic Routing Encapsulation DoS Vulnerability              |
| <a href="#">CSCwb67040</a> | FP4112 4115 Traceback & reload on Thread Name: netfs_thread_init                                     |
| <a href="#">CSCwb68642</a> | ASA traceback in Thread Name: SXP CORE                                                               |
| <a href="#">CSCwb71460</a> | ASA traceback in Thread Name: fover_parse and triggered by snmp related functions                    |
| <a href="#">CSCwb74571</a> | PBR not working on ASA routed mode with zone-members                                                 |
| <a href="#">CSCwb74938</a> | ASA traceback and reload with error "assertion "0" failed: file "timer_services.c", line 165"        |
| <a href="#">CSCwb78971</a> | Fatal error: Upgrade Failed: Invalid password: A blank or masked password is not allowed             |
| <a href="#">CSCwb79812</a> | RIP is advertising all connected Anyconnect users and not matching route-map for redistribution      |
| <a href="#">CSCwb80192</a> | WR6, WR8 commit id update in CCM layer(Seq 30)                                                       |
| <a href="#">CSCwb80559</a> | FTD offloads SGT tagged packets although it should not                                               |
| <a href="#">CSCwb82796</a> | ASA/FTD firewall may traceback and reload when tearing down IKE tunnels                              |
| <a href="#">CSCwb83388</a> | ASA HA Active/standby tracebacks seen approximately every two months.                                |

| Bug ID                     | Headline                                                                                    |
|----------------------------|---------------------------------------------------------------------------------------------|
| <a href="#">CSCwb86118</a> | TPK ASA: Device might get stuck on ftp copy to disk                                         |
| <a href="#">CSCwb87498</a> | Lina traceback and reload during EIGRP route update processing.                             |
| <a href="#">CSCwb87950</a> | Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability  |
| <a href="#">CSCwb88587</a> | Cisco Firepower Management Center Cross-Site Scripting Vulnerability                        |
| <a href="#">CSCwb89963</a> | ASA Traceback & reload in thread name: Datapath                                             |
| <a href="#">CSCwb90074</a> | ASA: Multiple Context Mixed Mode SFR Redirection Validation                                 |
| <a href="#">CSCwb92709</a> | We can't monitor the interface via "snmpwalk" once interface is removed from context.       |
| <a href="#">CSCwb92937</a> | Error 403: Forbidden when expanding in view group objects                                   |
| <a href="#">CSCwb93914</a> | Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability  |
| <a href="#">CSCwb93932</a> | ASA/FTD traceback and reload with timer services assertion                                  |
| <a href="#">CSCwb94190</a> | ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled. |
| <a href="#">CSCwb97251</a> | ASA/FTD may traceback and reload in Thread Name 'ssh'                                       |
| <a href="#">CSCwc02133</a> | Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability                  |
| <a href="#">CSCwc02488</a> | ASA/FTD may traceback and reload in Thread Name 'None'                                      |
| <a href="#">CSCwc02700</a> | Fragmented packets are dropped when unit leaves cluster                                     |
| <a href="#">CSCwc03069</a> | Interface internal data0/0 is up/up from cli but up/down from SNMP polling                  |
| <a href="#">CSCwc08676</a> | WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 32)                            |
| <a href="#">CSCwc09414</a> | ASA/FTD may traceback and reload in Thread Name 'ci/console'                                |
| <a href="#">CSCwc10037</a> | Cisco Firepower Management Center Cross-Site Scripting Vulnerability                        |
| <a href="#">CSCwc10792</a> | ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete             |
| <a href="#">CSCwc11597</a> | ASA tracebacks after SFR was upgraded to 6.7.0.3                                            |
| <a href="#">CSCwc11663</a> | ASA traceback and reload when modifying DNS inspection policy via CSM or CLI                |
| <a href="#">CSCwc13017</a> | FTD/ASA traceback and reload at at ../inspect/proxy.h:439                                   |
| <a href="#">CSCwc13994</a> | ASA - Restore not remove the new configuration for an interface setup after backup          |
| <a href="#">CSCwc18312</a> | "show nat pool cluster" commands run within EEM scripts lead to traceback and reload        |
| <a href="#">CSCwc23695</a> | ASA/FTD can not parse UPN from SAN field of user's certificate                              |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCwc25207</a> | WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 33)                                     |
| <a href="#">CSCwc26648</a> | ASA/FTD Traceback and Reload in Thread name Lina or Datatath                                         |
| <a href="#">CSCwc28532</a> | 9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing        |
| <a href="#">CSCwc28806</a> | ASA Traceback and Reload on process name Lina                                                        |
| <a href="#">CSCwc32246</a> | NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used            |
| <a href="#">CSCwc36905</a> | ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c                              |
| <a href="#">CSCwc38567</a> | ASA/FTD may traceback and reload while executing SCH code                                            |
| <a href="#">CSCwc40413</a> | Memory leak in rulesd0, rulesd1, rulesd2, rulesd3 on IPS 8350                                        |
| <a href="#">CSCwc41590</a> | Upgrade fail & App Instance fail to start with err "CSP_OP_ERROR. CSP signature verification error." |
| <a href="#">CSCwc41661</a> | FTD Multiple log files with zero byte size.                                                          |
| <a href="#">CSCwc44289</a> | FTD - Traceback and reload when performing IPv4 & IPv6 NAT translations                              |
| <a href="#">CSCwc45108</a> | ASA/FTD: GTP inspection causing 9344 sized blocks leak                                               |
| <a href="#">CSCwc45397</a> | ASA HA - Restore in primary not remove new interface configuration done after backup                 |
| <a href="#">CSCwc46569</a> | WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 34)                                          |
| <a href="#">CSCwc49095</a> | ASA/FTD 2100 platform traceback and reload when fragments are coalesced and sent to PDTS             |
| <a href="#">CSCwc50887</a> | FTD - Traceback and reload on NAT IPv4&IPv6 for UDP flow redirected over CCL link                    |
| <a href="#">CSCwc51326</a> | FXOS-based Firepower platform showing 'no buffer' drops despite high values for RX ring watermarks   |
| <a href="#">CSCwc52351</a> | ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP          |
| <a href="#">CSCwc53280</a> | ASA parser accepts incomplete network statement under OSPF process and is present in show run        |
| <a href="#">CSCwc54984</a> | IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response   |
| <a href="#">CSCwc60037</a> | ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context                 |
| <a href="#">CSCwc60907</a> | WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 35)                                     |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCwc61912</a> | ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6                                        |
| <a href="#">CSCwc64565</a> | ASA Traceback and reload in aaa_shim_thread                                                          |
| <a href="#">CSCwc66757</a> | ASA/FTD may traceback and reload in Thread Name 'lina'                                               |
| <a href="#">CSCwc72284</a> | TACACS Accounting includes an incorrect IPv6 address of the client                                   |
| <a href="#">CSCwc73224</a> | Call home configuration on standby device is lost after reload                                       |
| <a href="#">CSCwc74103</a> | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-11-32591'                                  |
| <a href="#">CSCwc79366</a> | During the deployment time, device got stuck processing the config request.                          |
| <a href="#">CSCwc81960</a> | Unable to configure 'match ip address' under route-map when using object-group in access list        |
| <a href="#">CSCwc88897</a> | ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy       |
| <a href="#">CSCwc90091</a> | ASA 9.12(4)47 with <user-statistics>, will affects the "policy-server xxxx global" visibility.       |
| <a href="#">CSCwc93166</a> | Using write standby in a user context leaves secondary firewall license status in an invalid state   |
| <a href="#">CSCwc94501</a> | ASA/FTD tracebacks due to ctm_n5 resets                                                              |
| <a href="#">CSCwc96805</a> | traceback and reload due to tcp intercept stat in thread unicorn                                     |
| <a href="#">CSCwd00386</a> | ASA/FTD may traceback and reload when clearing the configuration due to "snp_clear_acl_log_flow_all" |
| <a href="#">CSCwd11303</a> | ASA might generate traceback in ikev2 process and reload                                             |

## Resolved Bugs in Version 6.4.0.15

Table last updated: 2022-05-11

**Table 53: Resolved Bugs in Version 6.4.0.15**

| Bug ID                     | Headline                                                                          |
|----------------------------|-----------------------------------------------------------------------------------|
| <a href="#">CSCvx10555</a> | A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker            |
| <a href="#">CSCvt85766</a> | FPR2k: FCM Syslog Remote Destinations tab disappeared after upgrading             |
| <a href="#">CSCwa53489</a> | Lina Traceback and Reload Due to invalid memory access while accessing Hash Table |
| <a href="#">CSCvw94160</a> | CIAM: openssl CVE-2020-1971                                                       |
| <a href="#">CSCvx06920</a> | WR6, WR8 and LTS18 commit id update in CCM layer (sprint 103, seq 5)              |

| Bug ID                     | Headline                                                                                    |
|----------------------------|---------------------------------------------------------------------------------------------|
| <a href="#">CSCvz89327</a> | OSPFv2 flow missing cluster centralized "c" flag                                            |
| <a href="#">CSCwa26535</a> | IPv6 PMTU discovery does not work for RA VPN Client with tunneled route                     |
| <a href="#">CSCvz92016</a> | Cisco ASA and FTD Software Web Services Interface Privilege Escalation Vulnerability        |
| <a href="#">CSCvz05541</a> | ASA55XX: Expansion module interfaces not coming up after a software upgrade                 |
| <a href="#">CSCvz15755</a> | FTD - Port-channel not coming up after upgrade and may generate core file                   |
| <a href="#">CSCvx24245</a> | ASA Traceback and reload in <code>occam_group_free</code>                                   |
| <a href="#">CSCvw37340</a> | Vulnerability in the MySQL Server product of Oracle MySQL (component:                       |
| <a href="#">CSCvx98807</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 109, seq 9)                         |
| <a href="#">CSCvx16700</a> | FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC" |
| <a href="#">CSCwa40223</a> | Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability               |
| <a href="#">CSCvx47550</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 105, seq 6)                         |
| <a href="#">CSCvw43510</a> | Heap-based buffer overflow in the <code>test_compr_eb</code> function in Info-ZIP ...       |
| <a href="#">CSCvz89126</a> | ASDM session/quota count mismatch in ASA when multiple context switchover is done from ASDM |
| <a href="#">CSCvy66530</a> | lrzsz before version 0.12.21~rc can leak information to the receiving                       |
| <a href="#">CSCvy66531</a> | There's a flaw in libxml2's <code>xmllint</code> in versions before 2.9.11. An atta         |
| <a href="#">CSCvt25917</a> | FTD CLI - Fail to display the disabled local user and cannot enable back                    |
| <a href="#">CSCwa19443</a> | Flow Offload - Compare state values remains in error state for longer periods               |
| <a href="#">CSCvz82562</a> | ASA/FTD: site-to-site VPN - traffic incorrectly fragmented                                  |
| <a href="#">CSCvz68336</a> | SSL decryption not working due to single connection on multiple in-line pairs               |
| <a href="#">CSCwa05385</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 19)                        |
| <a href="#">CSCvx37833</a> | Diskmanager improperly pruning connection events leads to corrupt files                     |
| <a href="#">CSCwa73172</a> | ASA reload and traceback in Thread Name: PIX Garbage Collector                              |
| <a href="#">CSCvz41761</a> | FMC Does not allow to create an EIGRP authentication secret key using the \$ character      |
| <a href="#">CSCvz92932</a> | ASA show tech execution causing spike on CPU and impacting to IKEv2 sessions                |
| <a href="#">CSCvx73164</a> | Lasso SAML Implementation Vulnerability Affecting Cisco Products: June 2021                 |
| <a href="#">CSCvz76966</a> | Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DNS DoS    |

| Bug ID                     | Headline                                                                                     |
|----------------------------|----------------------------------------------------------------------------------------------|
| <a href="#">CSCvy02448</a> | Time sync do not work correctly for ASA on FPFPR2100 series platform                         |
| <a href="#">CSCwa15291</a> | A crafted request uri-path can cause mod_proxy to forward the request to an origin server... |
| <a href="#">CSCwa79494</a> | Traffic keep failing on Hub when IPSec tunnel from Spoke flaps                               |
| <a href="#">CSCwa87315</a> | ASA/FTD may traceback and reload in Thread Name 'IP Address Assign'                          |
| <a href="#">CSCvx47628</a> | In OpenLDAP through 2.4.57 and 2.5.x through 2.5.1alpha, an assertion                        |
| <a href="#">CSCwa04134</a> | The in-memory certificate cache in strongSwan before 5.9.4 has a remot                       |
| <a href="#">CSCvy89658</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 114, seq 13)                         |
| <a href="#">CSCvw43529</a> | Integer overflow in the DHCP client (udhcp) in BusyBox before 1.25. ...                      |
| <a href="#">CSCvw62288</a> | ASA: 256 byte block depletion when syslog rate is high                                       |
| <a href="#">CSCvy60285</a> | The mq_notify function in the GNU C Library (aka glibc) through 2.33 has a use-after-free    |
| <a href="#">CSCvy60574</a> | Port dcosAG leak fix CSCvx14602 to KP/WM                                                     |
| <a href="#">CSCvw72260</a> | ASA upgrade failed with: "CSP directory does not exist - STOP_FAILED Application_Not_Found"  |
| <a href="#">CSCvw90923</a> | WR6, WR8 and LTS18 commit id update in CCM layer (sprint 101, seq 4)                         |
| <a href="#">CSCvz95108</a> | FTD Deployment failure post upgrade due to major version change on device                    |
| <a href="#">CSCvy96698</a> | Resolve spurious status actions checking speed values twice in FXOS portmgr                  |
| <a href="#">CSCvu84127</a> | Firepower may reboot for no apparent reason                                                  |
| <a href="#">CSCvx54585</a> | nfm-burnin.sh fails: Incorrect Expanded Geryon base and media CPLD                           |
| <a href="#">CSCwa28822</a> | FTD moving UI management from FDM to FMC causes traffic to fail                              |
| <a href="#">CSCvw98315</a> | FXOS reporting old FTD version after FTD upgrade to 6.7.0                                    |
| <a href="#">CSCwb18252</a> | FTD/ASA: Traceback on BFD function causing unexpected reboot                                 |
| <a href="#">CSCwa26038</a> | ICMP inspection causes packet drops that are not logged appropriately                        |
| <a href="#">CSCvv21602</a> | cfprApSmMonitorTable is missing in the FP2K MIB                                              |
| <a href="#">CSCwa44950</a> | ASA/FTD - Memory leak observed when VPN is deployed                                          |
| <a href="#">CSCvw48829</a> | Timezone in "show clock" is different from which in "show run clock"                         |
| <a href="#">CSCvz08387</a> | ASP drop capture output may display incorrect drop reason                                    |
| <a href="#">CSCvx41045</a> | High CPU utilization in sfmbservice in FMC                                                   |

| Bug ID                     | Headline                                                                                     |
|----------------------------|----------------------------------------------------------------------------------------------|
| <a href="#">CSCvw98603</a> | Multiple vulnerabilities in SQLite                                                           |
| <a href="#">CSCwa41834</a> | ASA/FTD traceback and reload due to pix_startup_thread                                       |
| <a href="#">CSCvx47634</a> | The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and                        |
| <a href="#">CSCvy30016</a> | SSL decryption policy may cause performance degradation in Snort                             |
| <a href="#">CSCvx47636</a> | A flaw was discovered in ldap_X509dn2bv in OpenLDAP before 2.4.57 lead                       |
| <a href="#">CSCvu41615</a> | Cisco FTD Software Snort Out of Memory Denial of Service Vulnerability                       |
| <a href="#">CSCvw43537</a> | The recv_and_process_client_pkt function in networking/ntpd.c in bus ...                     |
| <a href="#">CSCvz51157</a> | In librt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/s                       |
| <a href="#">CSCvz30558</a> | Cisco Firepower Management Center Cross-site Scripting Vulnerability                         |
| <a href="#">CSCvz36933</a> | Sensor SNMP process may restart when policy deploy                                           |
| <a href="#">CSCvy60295</a> | A flaw was found in OpenLDAP. openLDAP's slapd server trigger an assertion failure.          |
| <a href="#">CSCvy60294</a> | There's a flaw in libxml2 in versions before 2.9.11. An attacker who i                       |
| <a href="#">CSCvy60292</a> | There is a flaw in the xml entity encoding functionality of libxml2 in                       |
| <a href="#">CSCvz05687</a> | Fragmented Certificate request failed for DND flow                                           |
| <a href="#">CSCwa30114</a> | "Error:NAT unable to reserve ports" when using a range of ports in an object service         |
| <a href="#">CSCwa74900</a> | Traceback and reload after enabling debug webvpn cifs 255                                    |
| <a href="#">CSCvy64145</a> | WR6 and WR8 commit id update in CCM layer(sprint 113, seq 12)                                |
| <a href="#">CSCvu75930</a> | Service module not returning error to supervisor when SMA resources are depleted             |
| <a href="#">CSCvz76746</a> | While implementing management tunnel a user can use open connect to bypass anyconnect.       |
| <a href="#">CSCwa96759</a> | Lina may traceback and reload on tcpmod_proxy_handle_mixed_mode                              |
| <a href="#">CSCvw97256</a> | Need handling of rmu read failure to ignore link state update when link state API read fails |
| <a href="#">CSCvz55140</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 117, seq 17)                         |
| <a href="#">CSCvs42388</a> | Gratuitous logging of string: "Memory stats information for preprocessor is NULL"            |
| <a href="#">CSCvz05767</a> | FP-1010 HA link goes down or New hosts unable to connect to the device                       |
| <a href="#">CSCvy10789</a> | FTD 2110 ascii characters are disallowed in LDAP password                                    |
| <a href="#">CSCwa58686</a> | ASA/FTD Change in OGS compilation behavior causing boot loop                                 |

| Bug ID                     | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvz71064</a> | Deleting The Context From ASA taking Almost 2 Minutes with ikev2 tunnel                            |
| <a href="#">CSCvz46333</a> | FTD policy deployment failure due to internal socket connection loss                               |
| <a href="#">CSCwa56975</a> | DHCP Offer not seen on control plane                                                               |
| <a href="#">CSCvs84242</a> | FMC Deployment Failure when removing Auto NAT and correlated network object                        |
| <a href="#">CSCvz32623</a> | An integer overflow in util-linux through 2.37.1 can potentially cause                             |
| <a href="#">CSCvy04430</a> | Management Sessions fail to connect after several weeks                                            |
| <a href="#">CSCvy95329</a> | Incorrect Access rule matching because of ac rule entry missing                                    |
| <a href="#">CSCvw43541</a> | infrees.c in zlib 1.2.8 might allow context-dependent attackers to ...                             |
| <a href="#">CSCvy04343</a> | ASA in PLR mode,"license smart reservation" is failing.                                            |
| <a href="#">CSCvw43544</a> | The crc32_big function in crc32.c in zlib 1.2.8 might allow context- ...                           |
| <a href="#">CSCvz24238</a> | Cisco Firepower Management Center Cross-site Scripting Vulnerability                               |
| <a href="#">CSCwa06960</a> | ASA Traceback and Reload due to CTM daemon during internal health test                             |
| <a href="#">CSCvx66329</a> | FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh |
| <a href="#">CSCvy95520</a> | Incorporate fail2ban into IMS to prevent SSH DOS attack                                            |
| <a href="#">CSCwa65389</a> | ASA traceback and reload in Unicorn Admin Handler when change interface configuration via ASDM     |
| <a href="#">CSCwa32286</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 125, seq 21)                               |
| <a href="#">CSCvx95884</a> | High CPU and massive "no buffer" drops during HA bulk sync and during normal conn sync             |
| <a href="#">CSCvr39217</a> | Fxos Snmp-user is not persistent after reboot                                                      |
| <a href="#">CSCwb01700</a> | ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA                    |
| <a href="#">CSCwa08262</a> | AnyConnect users with mapped group-policies take attributes from default GP under the tunnel-group |
| <a href="#">CSCvw93159</a> | Firepower 2100: ASA/FTD generates message "Local disk 2 missing on server 1/1"                     |
| <a href="#">CSCvy03045</a> | Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed  |
| <a href="#">CSCvx89827</a> | Not able to set Bangkok time zone in FPR 2110                                                      |
| <a href="#">CSCvx91317</a> | A remote code execution issue was discovered in MariaDB 10.2 before 10                             |

| Bug ID                     | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvz85913</a> | ASN.1 strings are represented internally within OpenSSL as an ASN1_STR for CISCO-SSL-1.0.2         |
| <a href="#">CSCvz65181</a> | Cisco Firepower Threat Defense Software Security Intelligence DNS Feed Bypass Vulnerabilit         |
| <a href="#">CSCvv17599</a> | Multiple vulnerabilities in cpe:2.3:o:linux:linux_kernel:4.14.187:                                 |
| <a href="#">CSCvw16165</a> | Firepower 1010 Series stops passing traffic when a member of the port-channel is down              |
| <a href="#">CSCvw52083</a> | FXOS logrotate does not rotate properly all the log files                                          |
| <a href="#">CSCvz33468</a> | ASA/FTD - NAT stops translating source addresses after changes to object-groups in manual NAT Rule |
| <a href="#">CSCvy60305</a> | A flaw was found in ImageMagick in versions before 7.0.11. has a potential cipher leak             |
| <a href="#">CSCvv52349</a> | No utility to handle XFS corruption on 2100/1000 series Firepower devices                          |
| <a href="#">CSCvw09745</a> | NFE ports are down after upgrade to 6.4.0.10-86 before reapplying AC policy                        |
| <a href="#">CSCvw43555</a> | A heap-based buffer overflow exists in Info-Zip UnZip version &lt;= 6.0 ...                        |
| <a href="#">CSCwa85043</a> | Traceback: ASA/FTD may traceback and reload in Thread Name 'Logger'                                |
| <a href="#">CSCvw43559</a> | BusyBox project BusyBox wget version prior to commit 8e2174e9bd836e5 ...                           |
| <a href="#">CSCvy08798</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 110, seq 10)                               |
| <a href="#">CSCvx10520</a> | curl 7.20.0 through 7.70.0 is vulnerable to improper restriction of na                             |
| <a href="#">CSCwa13873</a> | ASA Failover Split Brain caused by delay on state transition after "failover active" command run   |
| <a href="#">CSCvy60284</a> | A flaw was found in OpenLDAP in versions before 2.4.56. This flaw allo                             |
| <a href="#">CSCvx67468</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 107, seq 7)                                |
| <a href="#">CSCvv55066</a> | FPR1010: Internal-Data0/0 and data interfaces are flapping during SMB file transfer                |
| <a href="#">CSCwa56449</a> | ASA traceback in HTTP cli EXEC code                                                                |
| <a href="#">CSCvx33904</a> | Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation                |
| <a href="#">CSCwa85138</a> | Multiple issues with transactional commit diagnostics                                              |
| <a href="#">CSCvx97053</a> | Unable to configure ipv6 address/prefix to same interface and network in different context         |
| <a href="#">CSCvz25066</a> | fs/seq_file.c in the Linux kernel 3.16 through 5.13.x before 5.13.4 do                             |

| Bug ID                     | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCwa33898</a> | Cisco Adaptive Security Appliance Software Clientless SSL VPN Heap Overflow Vulnerability           |
| <a href="#">CSCvz25064</a> | The wordexp function in the GNU C Library (aka glibc) through 2.33 may                              |
| <a href="#">CSCwa68660</a> | FTP inspection stops working properly after upgrading the ASA to 9.12.4.x                           |
| <a href="#">CSCvy98027</a> | Application interface down whereas physical interface Up on FXOS                                    |
| <a href="#">CSCvp69087</a> | core_svc_sam_dme found after upgrade                                                                |
| <a href="#">CSCwa36535</a> | Standby unit failed to join failover due to large config size.                                      |
| <a href="#">CSCvx13835</a> | Multiple vulnerabilities in bind                                                                    |
| <a href="#">CSCvz73146</a> | FTD - Traceback in Thread Name: DATAPATH                                                            |
| <a href="#">CSCvz61767</a> | Policy deployment with SNMPv2 or SNMPv1 configuration fails                                         |
| <a href="#">CSCvt64238</a> | FXOS pktmgr Rx Drops counter keeps increasing in LACP Port-Channel                                  |
| <a href="#">CSCvy41763</a> | Cisco Firepower Threat Defense Software XML Injection Vulnerability                                 |
| <a href="#">CSCwa87597</a> | ASA/FTD Failover: Joining Standby reboots when receiving configuration replication from Active mate |
| <a href="#">CSCvx49720</a> | BIND servers are vulnerable if they are running an affected version an                              |
| <a href="#">CSCvs68576</a> | Deploy failure when deleting auto nat rule due to double negate                                     |
| <a href="#">CSCvy60333</a> | ImageMagick before 7.0.8-50 has a "use of uninitialized value" vulnerability                        |
| <a href="#">CSCwb01919</a> | FP2140 ASA 9.16.2 HA units traceback and reload at lua_getinfo (getfuncname)                        |
| <a href="#">CSCvr38379</a> | Upgraded FTD will not reimage to base FTD version with the use of 'auto-install' feature in FPR2100 |
| <a href="#">CSCvx10514</a> | An issue was discovered in p11-kit 0.21.1 through 0.23.21. Multiple in                              |
| <a href="#">CSCvw43489</a> | The NEEDBITS macro in the inflate_dynamic function in inflate.c for ...                             |
| <a href="#">CSCvr33586</a> | FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded                             |
| <a href="#">CSCvx10519</a> | curl 7.62.0 through 7.70.0 is vulnerable to an information disclosure                               |
| <a href="#">CSCwa94894</a> | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-4-9608'                                   |
| <a href="#">CSCvz09106</a> | Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability                                  |
| <a href="#">CSCwa55878</a> | FTD Service Module Failure: False alarm of "ND may have gone down"                                  |
| <a href="#">CSCwa11079</a> | Pre allocate sub context for DRBG health test                                                       |
| <a href="#">CSCvz44645</a> | FTD may traceback and reload in Thread Name 'lina'                                                  |

| Bug ID                     | Headline                                                                                          |
|----------------------------|---------------------------------------------------------------------------------------------------|
| <a href="#">CSCwa77083</a> | Host information is missing when Security Zones are configured in Network Discovery rules         |
| <a href="#">CSCwa61218</a> | Polling OID "1.3.6.1.4.1.9.9.171.1.3.2.1.2" gives negative index value of the associated tunnel   |
| <a href="#">CSCvx26927</a> | TLS site not loading when it has segmented and retransmitted CH                                   |
| <a href="#">CSCvz91218</a> | Statelink hello messages dropped on Standby unit due to interface ring drops on high rate traffic |
| <a href="#">CSCwa20758</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20)                              |
| <a href="#">CSCwa40719</a> | Traceback: Secondary firewall reloading in Threadname: fover_parse                                |
| <a href="#">CSCvy35948</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 111, seq 11)                              |
| <a href="#">CSCwa67882</a> | Offloaded GRE tunnels may be silently un-offloaded and punted back to CPU                         |
| <a href="#">CSCvy60322</a> | In BIND 9.0.0 -&gt; 9.11.29, 9.12.0 -&gt; 9.16.13, and versions BIND 9.9.3-S                      |
| <a href="#">CSCvy60320</a> | A race condition in Linux kernel SCTP sockets (net/sctp/socket.c) befo                            |
| <a href="#">CSCvy12991</a> | Chassis local date and time may drift back to midnight Jan 1 2015 after reboot                    |
| <a href="#">CSCvy60326</a> | Integer overflow in the htmdoc 1.9.11 and before may allow attackers                              |
| <a href="#">CSCvv24647</a> | FTD 2100 - SNMP: incorrect values returned for Ethernet statistics polling                        |
| <a href="#">CSCvx49717</a> | An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before                             |
| <a href="#">CSCvw13348</a> | WR6, WR8 and LTS18 commit id update in CCM layer (sprint 98, seq 2)                               |
| <a href="#">CSCwa97784</a> | ASA: Jumbo sized packets are not fragmented over the L2TP tunnel                                  |
| <a href="#">CSCvx78968</a> | ASA/FTD Traceback and reload on Thread Name: IKEv2 Daemon with VTIs configured                    |
| <a href="#">CSCwa29810</a> | ASA Certificate enrollment via Local CA server is not possible                                    |
| <a href="#">CSCwa60574</a> | ASA traceback and reload on snp_ha_trans_alloc_msg_muxbuf_space function                          |
| <a href="#">CSCwa14485</a> | Cisco Firepower Threat Defense Software Denial of Service Vulnerability                           |
| <a href="#">CSCvw43546</a> | In the add_match function in libbb/lineedit.c in BusyBox through 1.2 ...                          |
| <a href="#">CSCwa61361</a> | ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR                      |
| <a href="#">CSCvy24921</a> | SNMPv3 - SNMP EngineID changes after every configuration change                                   |
| <a href="#">CSCvx47642</a> | An integer underflow was discovered in OpenLDAP before 2.4.57 leading                             |
| <a href="#">CSCvx47643</a> | A flaw was discovered in OpenLDAP before 2.4.57 leading to a slapd cra                            |

| Bug ID                     | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvx47644</a> | A flaw was discovered in OpenLDAP before 2.4.57 leading to an assertio                             |
| <a href="#">CSCvz30582</a> | Cisco Firepower Management Center Cross-site Scripting Vulnerability                               |
| <a href="#">CSCvy18166</a> | AAB snort core due to high volume traffic logging                                                  |
| <a href="#">CSCvv95277</a> | FPR2100 High disk usage in partition /opt/cisco/platform/logs due to growth of httpd log files     |
| <a href="#">CSCwa18858</a> | ASA drops non DNS traffic with reason "label length 164 bytes exceeds protocol limit of 63 bytes"  |
| <a href="#">CSCvw02334</a> | ipv6 route table ( data and management ) in a multi-context environment.                           |
| <a href="#">CSCvx91341</a> | An issue was discovered in GNOME GLib before 2.66.8. When g_file_repla                             |
| <a href="#">CSCwa40237</a> | Cisco Firepower Management Center File Upload Security Bypass Vulnerability                        |
| <a href="#">CSCvv79459</a> | WR6, WR8 and LTS18 commit id update in CCM layer (sprint 94, seq 1)                                |
| <a href="#">CSCvz86256</a> | Primary ASA should send GARP as soon as split-brain is detected and peer becomes cold standby      |
| <a href="#">CSCwb07981</a> | Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server |
| <a href="#">CSCvt67167</a> | Data Unit traceback and reload without traffic at Thread Name : "logger"                           |
| <a href="#">CSCvx49716</a> | An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before                              |
| <a href="#">CSCvw43508</a> | Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZ ...                           |
| <a href="#">CSCwb25809</a> | Single Pass - Traceback due to stale ifc                                                           |
| <a href="#">CSCwa31373</a> | duplicate ACP rules are generated on FMC 6.6.5 after rule copy.                                    |
| <a href="#">CSCwa11088</a> | Access rule-ordering gets automatically changed while trying to edit it before page refresh/load   |
| <a href="#">CSCvq39187</a> | KP: Host key verification is getting failed while ssh to host                                      |
| <a href="#">CSCvz83432</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 121, seq 18)                               |
| <a href="#">CSCvw43610</a> | In IJG JPEG (aka libjpeg) before 9d, jpeg_mem_available() in jmemnob ...                           |
| <a href="#">CSCvz81342</a> | Diskmanager not pruning AMP File Capture files                                                     |
| <a href="#">CSCwa57115</a> | New access-list are not taking effect after removing non-existence ACL with objects.               |

## Resolved Bugs in Version 6.4.0.14

Table last updated: 2022-02-17

**Table 54: Resolved Bugs in Version 6.4.0.14**

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

## Resolved Bugs in Version 6.4.0.13

Table last updated: 2021-12-02

**Table 55: Resolved Bugs in Version 6.4.0.13**

| Bug ID                     | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCum03297</a> | ENH: ASA should save the timestamp of the MAXHOG in 'show proc cpu-hog'                             |
| <a href="#">CSCvg66052</a> | 2 CPU Cores continuously spike on firepower appliances                                              |
| <a href="#">CSCvi58484</a> | Cluster: ping sourced from FTD/ASA to external IPs may if reply lands on different cluster unit     |
| <a href="#">CSCvm76755</a> | DP-CP arp-in and adj-absent queues need to be separated                                             |
| <a href="#">CSCvp16933</a> | Cisco Firepower Threat Defense Software Shell Access Vulnerability                                  |
| <a href="#">CSCvp69936</a> | ASA : Traceback on tcp_intercept Thread name : Threat detection                                     |
| <a href="#">CSCvq39187</a> | KP: Host key verification is getting failed while ssh to host                                       |
| <a href="#">CSCvq43454</a> | ENH : Support a tolerance time for the "NotValidBefore" timestamp, while using SAML auth            |
| <a href="#">CSCvq54299</a> | After restart of both A/S units, not all context configs may be loaded when using SL on 2100        |
| <a href="#">CSCvr11958</a> | AWS FTD: Deployment failure with ERROR: failed to set interface to promiscuous mode                 |
| <a href="#">CSCvr33586</a> | FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded                             |
| <a href="#">CSCvr38379</a> | Upgraded FTD will not reimage to base FTD version with the use of 'auto-install' feature in FPR2100 |
| <a href="#">CSCvr39217</a> | Fxos Snmp-user is not persistent after reboot                                                       |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvs27336</a> | Traceback on ASA by Smart Call Home process                                                          |
| <a href="#">CSCvs47365</a> | Event rate seen on FMC slows down or stops coming from devices using FXOS 2.9.1 update               |
| <a href="#">CSCvt10944</a> | ctm crashed while sending emix traffic over VTI tunnel                                               |
| <a href="#">CSCvt15348</a> | ASA show processes cpu-usage output is misleading on multi-core platforms                            |
| <a href="#">CSCvt25917</a> | FTD CLI - Fail to display the disabled local user and cannot enable back                             |
| <a href="#">CSCvt31292</a> | FTD device might not send events to SSE                                                              |
| <a href="#">CSCvt64238</a> | FXOS pktmgr Rx Drops counter keeps increasing in LACP Port-Channel                                   |
| <a href="#">CSCvt85766</a> | FPR2k: FCM Syslog Remote Destinations tab disappeared after upgrading                                |
| <a href="#">CSCvu36302</a> | %ASA-3-737403 is used incorrectly when vpn-addr-assign local reuse-delay is configured               |
| <a href="#">CSCvu97242</a> | FTD 2100: Corefile and crashinfo might both be truncated and incomplete in the event of a crash      |
| <a href="#">CSCvv07917</a> | ASA learning a new route removes asp route table created by floating static                          |
| <a href="#">CSCvv20780</a> | Policy deploy fails with "Failed to hold the deployment transaction" error                           |
| <a href="#">CSCvv24647</a> | FTD 2100 - SNMP: incorrect values returned for Ethernet statistics polling                           |
| <a href="#">CSCvv43190</a> | Crypto engine errors when GRE header protocol field doesn't match protocol field in inner ip header  |
| <a href="#">CSCvv48594</a> | Memory leak: due to snp_tcp_intercept_stat_top_n_integrate() in threat detection                     |
| <a href="#">CSCvv48942</a> | Snmpwalk showing traffic counter as 0 for failover interface                                         |
| <a href="#">CSCvv55248</a> | Syslogs generated for ACL transaction commit are not in consistent format & not available some times |
| <a href="#">CSCvv62499</a> | FMC: Remove_peers.pl script should work when FTD is member of a cluster                              |
| <a href="#">CSCvv71097</a> | traceback: ASA reloaded snp_fdb_destroy_fh_callback+104                                              |
| <a href="#">CSCvv79459</a> | WR6, WR8 and LTS18 commit id update in CCM layer (sprint 94, seq 1)                                  |
| <a href="#">CSCvv84172</a> | Dangling ref in Clustered table and EO upon failed registration                                      |
| <a href="#">CSCvv85029</a> | ASA5555 traceback and reload on Thread Name: ace_work                                                |
| <a href="#">CSCvv89715</a> | Fastpath rules for Firepower 8000 series stack disappear randomly from the FMC                       |
| <a href="#">CSCvw03628</a> | ASA will not import CA certificate with name constraint of RFC822Name set as empty                   |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvw06298</a> | ASA duplicate MAC addresses in Shared Interfaces of different Contexts causing traffic impact        |
| <a href="#">CSCvw13348</a> | WR6, WR8 and LTS18 commit id update in CCM layer (sprint 98, seq 2)                                  |
| <a href="#">CSCvw16165</a> | Firepower 1010 Series stops passing traffic when a member of the port-channel is down                |
| <a href="#">CSCvw18614</a> | ASA/FTD traceback in the LINA process                                                                |
| <a href="#">CSCvw48829</a> | Timezone in "show clock" is different from which in "show run clock"                                 |
| <a href="#">CSCvw62526</a> | ASA traceback and reload on engineering ASA build - 9.12.3.237                                       |
| <a href="#">CSCvw68593</a> | A flaw in the way reply ICMP packets are limited in the Linux kernel f                               |
| <a href="#">CSCvw71405</a> | FPR1120 running ASA traceback and reload in crypto process.                                          |
| <a href="#">CSCvw90923</a> | WR6, WR8 and LTS18 commit id update in CCM layer (sprint 101, seq 4)                                 |
| <a href="#">CSCvw93159</a> | Firepower 2100: ASA/FTD generates message "Local disk 2 missing on server 1/1"                       |
| <a href="#">CSCvw93276</a> | Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability                        |
| <a href="#">CSCvw97256</a> | Need handling of rmu read failure to ignore link state update when link state API read fails         |
| <a href="#">CSCvx04003</a> | Lack of throttling of ARP miss indications to CP leads to oversubscription                           |
| <a href="#">CSCvx06920</a> | WR6, WR8 and LTS18 commit id update in CCM layer (sprint 103, seq 5)                                 |
| <a href="#">CSCvx14031</a> | IPv4 DACL stuck on Active device when DACL removed after CoA for IKEv2 Session, traffic not impacted |
| <a href="#">CSCvx16134</a> | 100% cpu-usage for some processes seen in "show processes cpu-usage" though using multicore          |
| <a href="#">CSCvx23833</a> | IKEv2 rekey - Invalid SPI for ESP packet using new SPI received right after Create_Child_SA response |
| <a href="#">CSCvx24537</a> | SAML: SAML Authentication may fail if we have 2 or more IDP certs with same Subject Name             |
| <a href="#">CSCvx25719</a> | X-Frame-Options header is not set in webvpn response pages                                           |
| <a href="#">CSCvx29814</a> | IP address in DHCP GIADDR field is reversed after sending DHCP DECLINE to DHCP server                |
| <a href="#">CSCvx33904</a> | Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation                  |
| <a href="#">CSCvx34237</a> | ASA reload with FIPS failure                                                                         |
| <a href="#">CSCvx42081</a> | FPR4150 ASA Standby Ready unit Loops to failed and remove config to install it again                 |

| Bug ID                     | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvx43150</a> | On the FMC, process of registration of member device post RMA is not successful                     |
| <a href="#">CSCvx45976</a> | ASA/FTD Watchdog forced traceback and reload in Threadname: vnet-proxy (rip: socks_proxy_datarelay) |
| <a href="#">CSCvx47230</a> | X-Frame-Options header support for older versions of IE and windows platforms                       |
| <a href="#">CSCvx47550</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 105, seq 6)                                 |
| <a href="#">CSCvx49715</a> | Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may                              |
| <a href="#">CSCvx50980</a> | ASA CP CPU wrong calculation leads to high percentage (100% CP CPU)                                 |
| <a href="#">CSCvx54235</a> | ASP capture dispatch-queue-limit shows no packets                                                   |
| <a href="#">CSCvx57417</a> | Smart Tunnel Code signing certificate renewal                                                       |
| <a href="#">CSCvx64478</a> | Unwanted console output during SAML transactions                                                    |
| <a href="#">CSCvx65745</a> | FPR2100: enable kernel panic on octeon for UE events to trigger crash                               |
| <a href="#">CSCvx66329</a> | FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh  |
| <a href="#">CSCvx67468</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 107, seq 7)                                 |
| <a href="#">CSCvx68355</a> | ASA - unable to import CA certificate when countryName is encoded as UTF8                           |
| <a href="#">CSCvx71571</a> | ASA: "ERROR: Unable to delete entries from Hash Table" with CSM                                     |
| <a href="#">CSCvx75963</a> | ASA traceback while taking captures                                                                 |
| <a href="#">CSCvx77768</a> | Traceback and reload due to Umbrella                                                                |
| <a href="#">CSCvx80830</a> | VPN conn fails from same user if Radius server sends a dACL and vpn-simultaneous-logins is set to 1 |
| <a href="#">CSCvx86621</a> | ASA(lina) clock (always shows Jan 2010) does not sync properly with fxos                            |
| <a href="#">CSCvx87709</a> | FPR 2100 running ASA in HA. Traceback and reload on watchdog during failover                        |
| <a href="#">CSCvx95255</a> | Supportive change in ASA to differentiate, new ASDM connections from existing ASDM context switch   |
| <a href="#">CSCvx95884</a> | High CPU and massive "no buffer" drops during HA bulk sync and during normal conn sync              |
| <a href="#">CSCvx97632</a> | ASA traceback and reload when copying files with long destination filenames using cluster command   |
| <a href="#">CSCvx98807</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 109, seq 9)                                 |
| <a href="#">CSCvy01752</a> | Traceback on FPR 4115 in Thread - Lic HA Cluster                                                    |

| Bug ID                     | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvy02448</a> | Time sync do not work correctly for ASA on FPFPR2100 series platform                                |
| <a href="#">CSCvy02703</a> | ASA/FTD tracebacks due to CTM message handler                                                       |
| <a href="#">CSCvy03006</a> | improve debugging capability for uauth                                                              |
| <a href="#">CSCvy03045</a> | Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed   |
| <a href="#">CSCvy03907</a> | Creation/Edit of Access Control Policy fails with error 'Rule Name Already Exists'                  |
| <a href="#">CSCvy04869</a> | AnyConnect certificate authentication fails if user certificate has 8192 bits key size              |
| <a href="#">CSCvy07491</a> | ASA traceback when re-configuring access-list                                                       |
| <a href="#">CSCvy08798</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 110, seq 10)                                |
| <a href="#">CSCvy08908</a> | Port-forwarding application blocked by Java                                                         |
| <a href="#">CSCvy10583</a> | ASA Traceback and Reload in Thread Name: DATAPATH                                                   |
| <a href="#">CSCvy10789</a> | FTD 2110 ascii characters are disallowed in LDAP password                                           |
| <a href="#">CSCvy12782</a> | FTD/ASA: PATed traffic impacted when configured on ixgbe-vf SRIOV interfaces in HA                  |
| <a href="#">CSCvy14721</a> | ssl traffic dropped by FTD while CH packet has a destination port no greater than source port       |
| <a href="#">CSCvy16179</a> | ASA cluster Traceback with Thread Name: Unicorn Admin Handler even when running fix for CSCuz67596  |
| <a href="#">CSCvy17078</a> | Traceback: ASA on FPR 2110 traceback and reload on process Lina                                     |
| <a href="#">CSCvy17365</a> | REST API Login Page Issue                                                                           |
| <a href="#">CSCvy17470</a> | ASA Traceback and reload on the A/S failover pair at IKEv2                                          |
| <a href="#">CSCvy18366</a> | LINA Crash from pdts_pd_segment.c:1941 on FPR1k & ISA3k                                             |
| <a href="#">CSCvy21334</a> | Active tries to send CoA update to Standby in case of "No Switchover"                               |
| <a href="#">CSCvy23349</a> | FTD unnecessarily ACKing TCP flows on inline-pair deployment                                        |
| <a href="#">CSCvy25849</a> | ASA fails to process the OCSP response when the string 'OK' is missing in the HTTP response         |
| <a href="#">CSCvy31424</a> | QP FTD application fails to start due to outdated affinity.conf following FXOS/FTD upgrade          |
| <a href="#">CSCvy33105</a> | Ambiguous command error is shown for 'show route bgp' or 'show route isis' if DNS lookup is enabled |
| <a href="#">CSCvy33676</a> | UN-NAT created on FTD once a prior dynamic xlate is created                                         |

| Bug ID                     | Headline                                                                                       |
|----------------------------|------------------------------------------------------------------------------------------------|
| <a href="#">CSCvy35737</a> | FTD traceback and reload during anyconnect package verification                                |
| <a href="#">CSCvy35948</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 111, seq 11)                           |
| <a href="#">CSCvy39621</a> | ASA/FTD sends continuous Radius Access Requests Even After Max Retry Count is Reached          |
| <a href="#">CSCvy39659</a> | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-15-14815'                            |
| <a href="#">CSCvy43447</a> | FTD traceback and reload on Lic TMR Thread on Multi Instance FTD                               |
| <a href="#">CSCvy46026</a> | "Unable to load container (UUID)" when try to open a device under Devices > Device management  |
| <a href="#">CSCvy47108</a> | Remote Access IKEv2 VPN session cannot be established because of stuck Uauth entry             |
| <a href="#">CSCvy48159</a> | ASA Traceback & reload on process name lina due to memory header validation                    |
| <a href="#">CSCvy49732</a> | ASA/FTD may traceback and reload in Thread Name 'ssh'                                          |
| <a href="#">CSCvy50011</a> | ASA traceback in IKE Daemon process and reload                                                 |
| <a href="#">CSCvy51814</a> | Firepower flow-offload stops offloading all existing and new flows                             |
| <a href="#">CSCvy52074</a> | ASA/FTD may traceback and reload in Thread Name 'webvpn_task'                                  |
| <a href="#">CSCvy53461</a> | RSA keys & Certs get removed post reload on WS-SVC-ASA-SM1-K7 with ASA code 9.12.x             |
| <a href="#">CSCvy55356</a> | CPU hogs less than 10 msec are produced contrary to documentation                              |
| <a href="#">CSCvy57905</a> | VTI tunnel interface stays down post reload on KP/WM platform in HA                            |
| <a href="#">CSCvy60574</a> | Port dcosAG leak fix CSCvx14602 to KP/WM                                                       |
| <a href="#">CSCvy61008</a> | Time out of sync between Lina and FXOS                                                         |
| <a href="#">CSCvy64145</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 113, seq 12)                           |
| <a href="#">CSCvy64492</a> | ASAv adding non-identity L2 entries for own addresses on MAC table and dropping HA hellos      |
| <a href="#">CSCvy64911</a> | Debugs for: SNMP MIB value for crasLocalAddress is not showing the IP address                  |
| <a href="#">CSCvy67756</a> | Firepower Services HTTPS traffic stops working when matching Do not decrypt rule in SSL policy |
| <a href="#">CSCvy69189</a> | FTD HA stuck in bulk state due to stuck vpnfol_sync/Bulk-sync keytab                           |
| <a href="#">CSCvy72846</a> | ASA accounting reports incorrect Acct-Session-Time                                             |
| <a href="#">CSCvy74781</a> | The standby device is sending the keep alive messages for ssl traffic after the failover       |

| Bug ID                     | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvy80202</a> | Intrusion Event Performance Graphs load blank on 4100 despite of fix of CSCvm48451                 |
| <a href="#">CSCvy89658</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 114, seq 13)                               |
| <a href="#">CSCvy91668</a> | PAT pool exhaustion with stickiness traffic could lead to new connection drop.                     |
| <a href="#">CSCvy92990</a> | FTD traceback and reload related to SSL after upgrade to 7.0                                       |
| <a href="#">CSCvy96625</a> | Revert 'fix' introduced by CSCvr33428 and CSCvy39659                                               |
| <a href="#">CSCvy96698</a> | Resolve spurious status actions checking speed values twice in FXOS portmgr                        |
| <a href="#">CSCvy98027</a> | Application interface down whereas physical interface Up on FXOS                                   |
| <a href="#">CSCvy98458</a> | FP21xx -traceback "Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header"       |
| <a href="#">CSCvz00383</a> | FTD lina traceback and reload in thread Name Checkheaps                                            |
| <a href="#">CSCvz00699</a> | Traceback in webvpn and reload experienced periodically after ASA upgrade                          |
| <a href="#">CSCvz05189</a> | FTD reload with Lina traceback during xlate replication in Cluster                                 |
| <a href="#">CSCvz07614</a> | ASA: Orphaned SSH session not allowing us to delete a policy-map from CLI                          |
| <a href="#">CSCvz15529</a> | ASA traceback and reload thread name: Datapath                                                     |
| <a href="#">CSCvz20544</a> | ASA/FTD may traceback and reload in loop processing Anyconnect profile                             |
| <a href="#">CSCvz20679</a> | FTDv - Lina Traceback and reload                                                                   |
| <a href="#">CSCvz21886</a> | Twice nat's un-nat not happening if nat matches a pbr acl that matches a port number instead of IP |
| <a href="#">CSCvz25434</a> | ASA/FTD blackholes traffic due to 1550 block depletion when BVI is configured as DHCP client       |
| <a href="#">CSCvz27714</a> | Interface flapping on 8350 sensor during policy deployments                                        |
| <a href="#">CSCvz29233</a> | ASA: ARP entries from custom context not removed when an interface flap occurs on system context   |
| <a href="#">CSCvz34831</a> | If ASA fails to download DACL it will never stop trying                                            |
| <a href="#">CSCvz37306</a> | ASDM session is not served for new user after doing multiple context switches in existing user     |
| <a href="#">CSCvz38361</a> | BGP packets dropped for non directly connected neighbors                                           |
| <a href="#">CSCvz39565</a> | ASA/FTD Traceback and Reload during bulk VPN session connect                                       |
| <a href="#">CSCvz39646</a> | ASA/AnyConnect - Stale RADIUS sessions                                                             |

| Bug ID                     | Headline                                                                                        |
|----------------------------|-------------------------------------------------------------------------------------------------|
| <a href="#">CSCvz40352</a> | ASA traffic dropped by Implicit ACL despite the fact of explicit rules present on Access-list   |
| <a href="#">CSCvz43414</a> | Internal ldap attribute mappings fail after HA failover                                         |
| <a href="#">CSCvz43455</a> | ASAv observed traceback while upgrading hostscan                                                |
| <a href="#">CSCvz48407</a> | Traceback and reload in Thread Name: DATAPATH-15-18621                                          |
| <a href="#">CSCvz53142</a> | ASA does not use the interface specified in the name-server command to reach IPv6 DNS servers   |
| <a href="#">CSCvz57710</a> | conf t is converted to disk0:/t under context-config mode                                       |
| <a href="#">CSCvz58710</a> | ASA traceback due to SCTP traffic.                                                              |
| <a href="#">CSCvz60901</a> | ASA: IPv6 Neighbor reachability issues                                                          |
| <a href="#">CSCvz60970</a> | ASA Traceback in Thread Name: DATAPATH-4-23199 in enic_put / FREEB when sending LU to statelink |
| <a href="#">CSCvz64470</a> | ASA/FTD Traceback and reload due to memory corruption when generating ICMP unreachable message  |
| <a href="#">CSCvz66795</a> | ASA traceback and reload in SSH process when executing the command "show access-list"           |
| <a href="#">CSCvz69571</a> | ASA log shows wrong value of the transferred data after the anyconnect session terminated.      |
| <a href="#">CSCvz73709</a> | ASA/FTD Standby unit fails to join HA                                                           |
| <a href="#">CSCvz77744</a> | OSPFv3: FTD Wrong "Forwarding address" added in ospfv3 database                                 |
| <a href="#">CSCvz81934</a> | Revert 'fix' introduced by CSCvx95884                                                           |
| <a href="#">CSCvz84850</a> | ASA/FTD traceback and reload caused by "timer services" function                                |
| <a href="#">CSCvz87824</a> | 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 56: Resolved Bugs in Version 6.4.0.12**

| Bug ID                     | Headline                                                  |
|----------------------------|-----------------------------------------------------------|
| <a href="#">CSCtx83747</a> | Syslog 718055 contains wrongly formatted MAC address      |
| <a href="#">CSCui74211</a> | Expired DHCP-Client leases not purged on ASA-standby unit |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCuj60109</a> | ENH: SFP transceivers attached to ASA-IC-6GE-SFP-A are not shown by CLI                              |
| <a href="#">CSCuj99176</a> | Make ASA-SSM cplane keepalives more tolerable to communication delays                                |
| <a href="#">CSCun74870</a> | ASA IKEv2: NO-PROPOSAL-CHOSEN sent instead of TS_UNSUPPORTED                                         |
| <a href="#">CSCuq47482</a> | ENH: ASA show tech should include "show module x detail"                                             |
| <a href="#">CSCut44164</a> | ASA: Add additional crypto stats to "show tech"                                                      |
| <a href="#">CSCuu60064</a> | ENH: ASAv show tech should include "show vm"                                                         |
| <a href="#">CSCuu84198</a> | DHCPRelay debugs should highlight invalid parameters from DHCP server                                |
| <a href="#">CSCuw51499</a> | TCM doesn't work for ACE addition/removal, ACL object/object-group edits                             |
| <a href="#">CSCuy53106</a> | ASA OS incorrectly calculates certificate expiry date in Syslog 717054                               |
| <a href="#">CSCvb92169</a> | ASA should provide better fragment-related logs and ASP drop reasons                                 |
| <a href="#">CSCvc40724</a> | Invalid group URL causes improperly formatted message back to AnyConnect                             |
| <a href="#">CSCvf88062</a> | CTM: Nitrox S/G lengths need to be validated                                                         |
| <a href="#">CSCvg59385</a> | ASA scansafe connector takes too long to failover to secondary CWS Tower                             |
| <a href="#">CSCvg69380</a> | ASA - rare cp processing corruption causes console lock                                              |
| <a href="#">CSCvg73237</a> | ENH: Configure CAC as an absolute value as well instead of just percentage of total VPN capacity.    |
| <a href="#">CSCvh30209</a> | Traceback in mfib_idb_get when toggling multicast on/off repeatedly                                  |
| <a href="#">CSCvh85504</a> | "Backlog Status" health module false negative alerts                                                 |
| <a href="#">CSCvi07901</a> | CISCO-REMOTE-ACCESS-MONITOR-MIB crasIPSecNumSessions is zero on ASA for IKEv2 AnyConnect             |
| <a href="#">CSCvi85020</a> | Order of SSH configuration generates "SSH version 1 is not secure." error messages at boot           |
| <a href="#">CSCvk51778</a> | "show inventory" (or) "show environment" on ASA 5515/5525/5545/5555 shows up Driver/ioctl error logs |
| <a href="#">CSCvm15088</a> | ENH: Add PSU details in "show environment" for ASA5525                                               |
| <a href="#">CSCvm78605</a> | ASA Failover: 'show interface tunnel' shows tunnel source as standby IP address                      |
| <a href="#">CSCvm82290</a> | ASA core blocks depleted when host unreachable in IRB/TFW configuration                              |
| <a href="#">CSCvm98585</a> | CPU hog from idfw module observed in 5525 FTD                                                        |
| <a href="#">CSCvn12453</a> | Implement debug menu command to show RX ring number a flow is hashed to                              |

| Bug ID                     | Headline                                                                                        |
|----------------------------|-------------------------------------------------------------------------------------------------|
| <a href="#">CSCvn16864</a> | ENH: Missing Content-Security-Policy Header in ASA HTTP WebVPN portal                           |
| <a href="#">CSCvn16877</a> | ENH: Missing X-Content-Type-Options Header in ASA HTTP WebVPN portal                            |
| <a href="#">CSCvn16887</a> | ENH: Missing X-XSS-Protection Header in ASA HTTP WebVPN portal                                  |
| <a href="#">CSCvn64647</a> | ASA traceback and reload due to tcp_retrans_timeout internal thread handling                    |
| <a href="#">CSCvn82441</a> | [SXP] Issue with establishing SXP connection between ASA on FPR-2110 and switches               |
| <a href="#">CSCvn93683</a> | ASA: cluster exec show commands not show all output                                             |
| <a href="#">CSCvn95731</a> | ASA traceback and reload on Thread Name SSH                                                     |
| <a href="#">CSCvo11623</a> | ASAv/Azure: Smart Licensing does not use hostname from custom template for registration         |
| <a href="#">CSCvo12504</a> | ASA: Failover fsm gets stuck in a multicontext in case of module difference.                    |
| <a href="#">CSCvo33227</a> | BusyBox udhcp Components Out-of-Bounds Read Information Disclosure Vul                          |
| <a href="#">CSCvo33896</a> | snmpd(): insufficient memory to handle queries                                                  |
| <a href="#">CSCvo34210</a> | ASA running 9.6.4.20 Traceback in threadname Unicorn Proxy Thread                               |
| <a href="#">CSCvo58030</a> | Failover mac address configured on interface does not allow to delete subinterface              |
| <a href="#">CSCvo64516</a> | ASA fails command authorization if tcp syslog is down.                                          |
| <a href="#">CSCvo68887</a> | Timestamp in Crash File name says UTC but is local timezone                                     |
| <a href="#">CSCvo78772</a> | ENH: ASA WebVPN should send "Cache-Control: no-store" instead of "Cache-Control: no-cache"      |
| <a href="#">CSCvo81249</a> | ASA may cause high-rate of DNS queries between ASA (acting as a DNS client) and a server        |
| <a href="#">CSCvo86485</a> | incorrect HTML <base> tag handling by Grammar Based Parser                                      |
| <a href="#">CSCvo87430</a> | FTD : Can't deploy ISAKMP VPNs containing question marks                                        |
| <a href="#">CSCvo99076</a> | ENH: IKEv2 quick connection preempt for static IP assigned to client by AAA                     |
| <a href="#">CSCvp09083</a> | ASA working as DHCP server drops DHCP renewal request packet sent by DHCP clients               |
| <a href="#">CSCvp10079</a> | DB switch role failed on FMC HA switch                                                          |
| <a href="#">CSCvp13352</a> | ASA continues to do TCP keepalives for Client side connections even after vpn session times out |
| <a href="#">CSCvp16618</a> | URL inside HTML base tag is not rewritten after it is handled by GBP                            |
| <a href="#">CSCvp23530</a> | OSPF neighbor command not replicated to standby after write standby or reload                   |

| Bug ID                     | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvp29554</a> | Traceback and reload due to a watchdog timeout when accessing filesystem (webvpn related)          |
| <a href="#">CSCvp29803</a> | Apache HTTP Server Modules Scripts Arbitrary Code Execution Vulnerab ...                           |
| <a href="#">CSCvp31311</a> | There should be enough PKI handles for the max sessions on a given platform                        |
| <a href="#">CSCvp38774</a> | WebVPN rewriter not loading website correctly                                                      |
| <a href="#">CSCvp42484</a> | IS-IS hello packet length not updated to correct mtu when mtu modified                             |
| <a href="#">CSCvp42722</a> | ASA does not generate logging message 611103 for any syslog destination (buffer, trap, etc)        |
| <a href="#">CSCvp52437</a> | ASA   Saving configuration, give message "Platform does not support appliance mode configuration." |
| <a href="#">CSCvp56719</a> | Cisco FMC and FTD Software sftunnel Pass the Hash Vulnerability                                    |
| <a href="#">CSCvp57417</a> | Upon downgrade of an ASA, the firewall may traceback and reload                                    |
| <a href="#">CSCvp67033</a> | ASA: Cannot distinguish name aliases for IPv6 and displays a "incomplete command" error message    |
| <a href="#">CSCvp69229</a> | OpenSSL 0-byte Record Padding Oracle Information Disclosure Vulnerabil                             |
| <a href="#">CSCvp71766</a> | Radius authentication fails when sourced from BVI across a VPN tunnel                              |
| <a href="#">CSCvp71879</a> | limit-resource CLI for ssh/telnet has no effect if quota-CLI is not configured                     |
| <a href="#">CSCvp72624</a> | SNMP Limit for OID 1.3.6.1.2.1.4.35 (ipNetToPhysicalTable)                                         |
| <a href="#">CSCvp73394</a> | Failover ASA IKEv2 VTI: Secondary ASA sends standby IP as the traffic selector                     |
| <a href="#">CSCvp75965</a> | primary FPR2110 crash after customer configure syslog setting on FMC                               |
| <a href="#">CSCvp76904</a> | With dhcp-network-scope configured incorrectly, DHCP debugs on ASA show wrong gateway and netmask. |
| <a href="#">CSCvp77226</a> | ASA traceback and reload on sysopt traffic detailed in multicontext mode                           |
| <a href="#">CSCvp78171</a> | ASA in cluster fail to synchronise IPv6 ND table with peer units.                                  |
| <a href="#">CSCvp91905</a> | ASA will add the newly configured IPv6 Address to the current link-local address                   |
| <a href="#">CSCvp94478</a> | ASA scp quite slow                                                                                 |
| <a href="#">CSCvp96658</a> | Inconsistency in timezone for show logging in newer versions                                       |
| <a href="#">CSCvq00560</a> | ASA silently drops packets which violate ESP Authentication data field size (ICV)                  |
| <a href="#">CSCvq15976</a> | ASA Memory Leak - snp_svc_insert_dtls_session                                                      |
| <a href="#">CSCvq17551</a> | Syslog 711004 not consistently triggering event manager event                                      |

| Bug ID                     | Headline                                                                                  |
|----------------------------|-------------------------------------------------------------------------------------------|
| <a href="#">CSCvq22358</a> | Disabling anti-replay for one context it disables it for other contexts as well           |
| <a href="#">CSCvq27016</a> | FMC shows 'Unable to fetch failover history..' for FTD HA.                                |
| <a href="#">CSCvq37913</a> | VPN-sessiondb does not replicate to standby ASA                                           |
| <a href="#">CSCvq47743</a> | AnyConnect and Management Sessions fail to connect after several weeks                    |
| <a href="#">CSCvq49124</a> | ASA on FP1010 Traceback in http_exec_cli thread                                           |
| <a href="#">CSCvq49718</a> | Observed Traceback in ASA with dns debugs enabled while resolving FQDN Entries            |
| <a href="#">CSCvq50944</a> | OSPFv3 neighborship is flapping every ~30 minutes                                         |
| <a href="#">CSCvq54620</a> | FPR4110 crashes after using 'vpn-sessions logoff all'                                     |
| <a href="#">CSCvq54624</a> | DTLS AnyConnect tunnel doesn't resume due to cache miss                                   |
| <a href="#">CSCvq55426</a> | Adding an ipv6 default route causes CLI to hang for 50 seconds                            |
| <a href="#">CSCvq58729</a> | 2140: crypto accelerator status show SOFTWARE mode by default                             |
| <a href="#">CSCvq65864</a> | Traceback in HTTP Cli Exec with rest-api agent enabled                                    |
| <a href="#">CSCvq70536</a> | FTD: Deployment failure when breaking HA and graceful-restart is present on config        |
| <a href="#">CSCvq73595</a> | ASA webvpn unable to extract username from cert UPN if username is longer than 32 chars   |
| <a href="#">CSCvq76706</a> | Ability to clear message logged statistics in output of "show logging"                    |
| <a href="#">CSCvq78126</a> | V route is missing even after setting the reverse route in Crypto map config in HA-IKEv2  |
| <a href="#">CSCvq79042</a> | FQDN ACL entries incomplete due to DNS response from server is large and truncated        |
| <a href="#">CSCvq81410</a> | ASA::Unable to execute any ASA command via http using safari browser.                     |
| <a href="#">CSCvq81692</a> | ASA: After changing admin-context, call-home does not use new admin context setting       |
| <a href="#">CSCvq83060</a> | SNMP: Cannot get failover link information from oid in multiple mode                      |
| <a href="#">CSCvq84444</a> | Configuring static routes causes "Route Session" rerr counter to increment on standby ASA |
| <a href="#">CSCvq87625</a> | ENH: Addition of 'show run all sysopt' to 'show tech' output                              |
| <a href="#">CSCvq92240</a> | Memory leak observed while running AnyConnect ssl vpn tests                               |
| <a href="#">CSCvq93640</a> | WRL6 and WRL8 commit id update in CCM layer (sprint 67)                                   |
| <a href="#">CSCvq93836</a> | ENH: Addition of 'show logging setting' to 'show tech' output                             |
| <a href="#">CSCvq98396</a> | ASA: crypto session handles leak on the standby unit                                      |

| Bug ID                     | Headline                                                                                          |
|----------------------------|---------------------------------------------------------------------------------------------------|
| <a href="#">CSCvq99107</a> | Hot swap of SFP is not taking effect on the ASA                                                   |
| <a href="#">CSCvr03705</a> | We need to have default route with AD and tunneled at the same time for the same next hub.        |
| <a href="#">CSCvr04203</a> | Memory leak observed while running AnyConnect ssl vpn tests                                       |
| <a href="#">CSCvr09399</a> | Dynamic flow-offload can't be disabled                                                            |
| <a href="#">CSCvr12018</a> | ASA: VPN traffic fails to take the tunnel route when the default route is learnt over BGP.        |
| <a href="#">CSCvr15503</a> | ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA                   |
| <a href="#">CSCvr20486</a> | FTD 1010 Passive interfaces does not receive unicast packets                                      |
| <a href="#">CSCvr20757</a> | Block leak on ASA while running Cisco Umbrella DNS inspection                                     |
| <a href="#">CSCvr20876</a> | low memory causes kernel to invoke - oom and reload device - modified rlimit for KP               |
| <a href="#">CSCvr23580</a> | Can't delete 2 or more than two IP address-pool                                                   |
| <a href="#">CSCvr23986</a> | Cisco ASA & FTD devices may reload under conditions of low memory and frequent complete MIB walks |
| <a href="#">CSCvr33428</a> | FMC generates Connection Events from a SYN flood attack                                           |
| <a href="#">CSCvr35872</a> | ASA traceback Thread Name: DATAPATH with PBR configured                                           |
| <a href="#">CSCvr37486</a> | established rules in asp table are not un-installed on config removal                             |
| <a href="#">CSCvr37502</a> | libexpat Improper Parsing Denial of Service Vulnerability                                         |
| <a href="#">CSCvr39516</a> | lina segfault/reload caused by malloc failure in modexp-octeon                                    |
| <a href="#">CSCvr50509</a> | Some 3DES related configurations are lost after booted                                            |
| <a href="#">CSCvr50630</a> | ASA Traceback: SCTP bulk sync and HA synchronization                                              |
| <a href="#">CSCvr50718</a> | ASA   Incorrect handling of ICMP-TYPE objects for ICMP6 rules                                     |
| <a href="#">CSCvr51426</a> | ASA is not sending the mask in the accounting packets                                             |
| <a href="#">CSCvr55518</a> | Missing clean up on rule creation failure.                                                        |
| <a href="#">CSCvr57605</a> | ASA after reload had license context count greater than platform limits                           |
| <a href="#">CSCvr58411</a> | RRI on static HUB/SPOKE config is not working on HUB when a new static SPOKE is added or deleted  |
| <a href="#">CSCvr60195</a> | ASA/FTD may traceback and reload when repeatedly adding/removing multicast commands               |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvr68146</a> | Unable to auto-rejoin FTD cluster                                                                    |
| <a href="#">CSCvr68872</a> | Secondary unit exceed platform context count limit in split brain scenario when failover link down   |
| <a href="#">CSCvr72648</a> | BIGNUM leak in ec_bits()                                                                             |
| <a href="#">CSCvr80164</a> | WR6 and WR8 commit id update in CCM layer(sprint 72)                                                 |
| <a href="#">CSCvr83372</a> | I/O error occurred while writing; fd='28', error='Resource temporarily unavailable (11)'             |
| <a href="#">CSCvr86077</a> | ASA Traceback/pagefault in Datapath due to re_multi_match_ascii                                      |
| <a href="#">CSCvr90079</a> | HSTS config option not updated on show run all                                                       |
| <a href="#">CSCvr90462</a> | Improve ipv6 duplicate address detection to avoid disabling ipv6 in case of transient active-active  |
| <a href="#">CSCvr92311</a> | Standby ASA logging %ASA-4-720022: (VPN-Secondary) Cannot find trust point __tmpCiscoM1Root__        |
| <a href="#">CSCvr98924</a> | ASA traceback and reload due to routing subsystem                                                    |
| <a href="#">CSCvr99642</a> | ASA traceback and reload multiple times with trace "webvpn_periodic_signal"                          |
| <a href="#">CSCvs02954</a> | ASA OSPF: Prefix removed from the RIB when topology changes, then added back when another SPF is run |
| <a href="#">CSCvs04179</a> | ASA - 9.8.4.12 traceback and reload in ssh or fover_rx Thread                                        |
| <a href="#">CSCvs05262</a> | Decrement TTL display wrong result                                                                   |
| <a href="#">CSCvs13204</a> | ASAv failover traffic on SR-IOV interfaces might be dropped due to interface-down                    |
| <a href="#">CSCvs16073</a> | snmp poll failure with host and host-group configured                                                |
| <a href="#">CSCvs27264</a> | mroute entries on ASA not getting refreshed.                                                         |
| <a href="#">CSCvs28213</a> | ASA Traceback in Thread Name SSH with assertion slib_malloc.c                                        |
| <a href="#">CSCvs29779</a> | ASA may traceback and reload while waitinPC g for "DATAPATH-12-1899" process to finish.              |
| <a href="#">CSCvs31159</a> | Incorrect empty location handling inside CSCOGet_location wrapper                                    |
| <a href="#">CSCvs31443</a> | ASA reporting negative memory values on "%ASA-5-321001: Resource 'memory' limit" message             |
| <a href="#">CSCvs31470</a> | OSPF Hello causing 9K block depletion, control point CPU 100% and cluster unstable.                  |
| <a href="#">CSCvs32907</a> | Addition of debug counters for STRAP implementation.                                                 |
| <a href="#">CSCvs33102</a> | ASA/FTD may traceback and reload in Thread Name 'EIGRP-IPv4'                                         |

| Bug ID                     | Headline                                                                                      |
|----------------------------|-----------------------------------------------------------------------------------------------|
| <a href="#">CSCvs33852</a> | After upgrade to version 9.6.4.34 is not possible to add an access-group                      |
| <a href="#">CSCvs38785</a> | Inconsistent timestamp format in syslog                                                       |
| <a href="#">CSCvs39589</a> | ASA doesn't honor SSH Timeout When Data Channel is not Negotiated                             |
| <a href="#">CSCvs40230</a> | ICMP not working and failed with inspect-icmp-seq-num-not-matched                             |
| <a href="#">CSCvs43154</a> | Secondary ASA is unable to join the failover due to aggressive warning messages.              |
| <a href="#">CSCvs45111</a> | WR6 and WR8 commit id update in CCM layer(sprint 75)                                          |
| <a href="#">CSCvs45548</a> | reactivation-mode timed causing untimely reactivation of failed server                        |
| <a href="#">CSCvs47283</a> | Traffic may match an access-list incorrectly with object-group-search enabled                 |
| <a href="#">CSCvs48437</a> | ASA cannot send syslog to two UDP ports at same time                                          |
| <a href="#">CSCvs52108</a> | ASA Traceback Due to Umbrella Inspection                                                      |
| <a href="#">CSCvs52169</a> | ASA sends malformed RADIUS message when device-id from AnyConnect is too long                 |
| <a href="#">CSCvs55603</a> | ICMP Reply Dropped when matched by ACL                                                        |
| <a href="#">CSCvs56802</a> | Cisco Firepower 2100 Series SSL/TLS Inspection Denial of Service Vulnerability                |
| <a href="#">CSCvs59487</a> | Observed crash in KP device while upgrading to 99.14.1.64 image.                              |
| <a href="#">CSCvs59558</a> | Failover mac address getting removed on the reload of the Primary active unit                 |
| <a href="#">CSCvs59966</a> | false reported value for OID "cipSecGlobalActiveTunnels" - same as ASDM                       |
| <a href="#">CSCvs60254</a> | libxml2 xmlParseBalancedChunkMemoryRecover Memory Leak Vulnerability                          |
| <a href="#">CSCvs63484</a> | SAML tokens are not removed from hash table                                                   |
| <a href="#">CSCvs70260</a> | IKEv2 vpn-filter drops traffic with implicit deny after volume based rekey collision          |
| <a href="#">CSCvs71698</a> | Management default route conflicts with default data routing                                  |
| <a href="#">CSCvs71969</a> | Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability          |
| <a href="#">CSCvs72378</a> | ASDM session being abruptly terminated when switching between different contexts              |
| <a href="#">CSCvs72450</a> | FXOS - Recover hwclock of service module from corruption due to simultaneous write collision  |
| <a href="#">CSCvs73663</a> | ASA Traceback on IPsec message handler Thread                                                 |
| <a href="#">CSCvs73754</a> | ASA/FTD: Block 256 size depletion caused by ARP of BVI not assigned to any physical interface |
| <a href="#">CSCvs76605</a> | Wrong Module version listed for FXOS 2.6(1.174)                                               |

| Bug ID                     | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvs77818</a> | Traceback: spin_lock_fair_mode_enqueue: Lock (np_conn_shrlock_t) is held for a long time           |
| <a href="#">CSCvs82726</a> | Placeholder to address CSCvs31470 in Multi-Context Mode                                            |
| <a href="#">CSCvs84542</a> | ASA traceback with thread: idfw_proc                                                               |
| <a href="#">CSCvs85196</a> | ASA SIP connections drop after several consecutive failovers: pinhole timeout/closed by inspection |
| <a href="#">CSCvs87795</a> | ASA: backup context failed to "ERROR: No such file or directory"                                   |
| <a href="#">CSCvs88413</a> | Port-channel bundling is failing after upgrade to 9.8 version                                      |
| <a href="#">CSCvs90100</a> | ASA/FTD may traceback and reload in Thread Name 'License Thread'                                   |
| <a href="#">CSCvs94486</a> | CSCvs59487 requires additional fix for resolution                                                  |
| <a href="#">CSCvs97863</a> | Reduce number of fsync calls during close in flash file system                                     |
| <a href="#">CSCvs97908</a> | Invalid scp session terminates other active http, scp sessions                                     |
| <a href="#">CSCvt00255</a> | Upgrade kernel to cpe:2.3:o:linux:linux_kernel:4.14.187:                                           |
| <a href="#">CSCvt01282</a> | WR6 and WR8 commit id update in CCM layer(sprint 79)                                               |
| <a href="#">CSCvt05862</a> | IPv6 DNS server resolution fails when the server is reachable over the management interface.       |
| <a href="#">CSCvt06606</a> | Flow offload not working with combination of FTD 6.2(3.10) and FXOS 2.6(1.169)                     |
| <a href="#">CSCvt06841</a> | Incorrect access-list hitcount seen when configuring it with a capture on ASA                      |
| <a href="#">CSCvt08492</a> | Events are not generated on FDM after FXOS upgrade                                                 |
| <a href="#">CSCvt11302</a> | On FPR devices when FIPS is enabled cannot create webtype ACLs                                     |
| <a href="#">CSCvt11547</a> | Cisco Firepower Device Manager Software Filesystem Space Exhaustion Denial of Service Vuln         |
| <a href="#">CSCvt11661</a> | DOC - Clarify the meaning of mp-svc-flow-control under show asp drop                               |
| <a href="#">CSCvt11742</a> | ASA/FTD may traceback and reload in Thread Name 'ssh'                                              |
| <a href="#">CSCvt12463</a> | ASA: Traceback in thread Unicorn Admin Handler                                                     |
| <a href="#">CSCvt13301</a> | Default Syslog using non-standard port does not work for Intrusion events                          |
| <a href="#">CSCvt13822</a> | ASA: VTI rejecting IPsec tunnel due to no matching crypto map entry                                |
| <a href="#">CSCvt15056</a> | SFR managed by ASDM: System policy does not apply.                                                 |
| <a href="#">CSCvt17912</a> | stress, pushing platform limits causing segfault/reload in lina_free_exec_st                       |

| Bug ID                     | Headline                                                                                         |
|----------------------------|--------------------------------------------------------------------------------------------------|
| <a href="#">CSCvt18199</a> | IPv6 Nat rejected with error "overlaps with inside standby interface address" for Standalone ASA |
| <a href="#">CSCvt22356</a> | Health-check monitor-interface debounce-time in ASA Cluster resets to 9000ms after ASA reboot    |
| <a href="#">CSCvt23643</a> | VPN failover recovery is taking approx. 30 seconds for data to resume                            |
| <a href="#">CSCvt25225</a> | ASA: Active unit HA traceback and reload during Config Sync state during OSPF sync               |
| <a href="#">CSCvt26031</a> | ASAv Unable to register smart licensing with IPv6                                                |
| <a href="#">CSCvt26530</a> | FTD failed over due to 'Inspection engine in other unit has failed due to snort failure'         |
| <a href="#">CSCvt27585</a> | Observed traceback on 2100 while performing Failover Switch from Standby.                        |
| <a href="#">CSCvt30731</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 80)                                      |
| <a href="#">CSCvt35945</a> | Encryption-3DES-AES should not be required when enabling ssh version 2 on 9.8 train              |
| <a href="#">CSCvt36542</a> | Multi-context ASA/LINA on FPR not sending DHCP release message                                   |
| <a href="#">CSCvt38279</a> | Erase disk0 on ISA3000 causes file system not supported                                          |
| <a href="#">CSCvt39977</a> | Invalid packet data when PSNG_TCP_PORTSCAN [122:1:1] rule alerts.                                |
| <a href="#">CSCvt41357</a> | "no logging permit-hostdown" does not block connections when syslog host is inaccessible         |
| <a href="#">CSCvt43136</a> | Multiple Cisco Products Snort TCP Fast Open File Policy Bypass Vulnerability                     |
| <a href="#">CSCvt43967</a> | Pad packets received from RA tunnel which are less than or equal 46 bytes in length with zeros   |
| <a href="#">CSCvt46289</a> | ASA LDAPS connection fails on Firepower 1000 Series                                              |
| <a href="#">CSCvt48601</a> | Cisco Firepower Managment Center Software Stored Cross-Site Scripting Vulnerability              |
| <a href="#">CSCvt50528</a> | Warning Message for default settings with Installation of Certificates in ASA/FTD - CLI          |
| <a href="#">CSCvt51349</a> | Fragmented packets forwarded to fragment owner are not visible on data interface captures        |
| <a href="#">CSCvt51987</a> | Traffic outage due to 80 size block exhaustion on the ASA FPR9300 SM56                           |
| <a href="#">CSCvt53640</a> | ASA5585 may traceback and reload after upgrading SFR from 6.4.0 to 6.4.0.x                       |
| <a href="#">CSCvt54182</a> | LINA cores are generated when FTD is configured to do SSL decryption.                            |
| <a href="#">CSCvt63027</a> | Cisco Firepower Management Center XML Entity Expansion Vulnerability                             |

| Bug ID                     | Headline                                                                                          |
|----------------------------|---------------------------------------------------------------------------------------------------|
| <a href="#">CSCvt63484</a> | ASA High CPU with igb_saleen_io_sfp_mod_poll_thre process                                         |
| <a href="#">CSCvt64035</a> | remote access mib - SNMP 64 bit only reporting 4Gb before wrapping around                         |
| <a href="#">CSCvt64952</a> | "Show crypto accelerator load-balance detail" has missing and undefined output                    |
| <a href="#">CSCvt65982</a> | Route Fallback doesn't happen on Slave unit, upon RRI route removal.                              |
| <a href="#">CSCvt68294</a> | Adjust Firepower 4120 Maximum VPN Session Limit to 20,000                                         |
| <a href="#">CSCvt70664</a> | ASA: acct-session-time accounting attribute missing from Radius Acct-Requests for AnyConnect      |
| <a href="#">CSCvt71529</a> | ASA traceback and reload during SSL handshake                                                     |
| <a href="#">CSCvt72683</a> | NAT policy configuration after NAT policy deployment on FP 8130 is not seen                       |
| <a href="#">CSCvt73407</a> | TACACS Fallback authorization fails for Username enable_15 on ASA device.                         |
| <a href="#">CSCvt75760</a> | Traceback/Page-fault in Clientless WebVPN due to HTTP cleanup                                     |
| <a href="#">CSCvt80126</a> | ASA traceback and reload for the CLI "show asp table socket 18421590 det"                         |
| <a href="#">CSCvt80134</a> | WebVPN rewriter fails to parse data from SAP Netweaver.                                           |
| <a href="#">CSCvt80172</a> | Supervisor software needs to be upgraded to address CVE-2017-11610                                |
| <a href="#">CSCvt83133</a> | Unable to access anyconnect webvpn portal from google chrome using group-url                      |
| <a href="#">CSCvt90330</a> | ASA traceback and reload with thread name coa_task                                                |
| <a href="#">CSCvt91521</a> | Crypto accelerator bias setting should be included in show tech                                   |
| <a href="#">CSCvt92647</a> | Connectivity over the state link configured with IPv6 addresses is lost after upgrading the ASA   |
| <a href="#">CSCvt98599</a> | IKEv2 Call Admission Statistics "Active SAs" counter out of sync with the real number of sessions |
| <a href="#">CSCvt99020</a> | Cisco Firepower Managment Center Software Stored Cross-Site Scripting Vulnerability               |
| <a href="#">CSCvt99137</a> | With huge FTP traffic in cluster, the SEC_FLOW messages are in a retransmit loop                  |
| <a href="#">CSCvu00112</a> | tsd0 not reset when ssh quota limit is hit in ci_cons_shell                                       |
| <a href="#">CSCvu03107</a> | AnyConnect statistics is doubled in both %ASA-4-113019 and RADIUS accounting                      |
| <a href="#">CSCvu03562</a> | Device loses ssh connectivity when username and password is entered                               |
| <a href="#">CSCvu03675</a> | FPR2100: ASA console may hang & become unresponsive in low memory conditions                      |
| <a href="#">CSCvu05180</a> | aaa-server configuration missing on the FTD after a Remote Access VPN policy deployment           |

| Bug ID                     | Headline                                                                                          |
|----------------------------|---------------------------------------------------------------------------------------------------|
| <a href="#">CSCvu06767</a> | Lina cores on multi-instance causing a boot loop on both logical-devices                          |
| <a href="#">CSCvu07602</a> | FPR-41x5: 'clear crypto accelerator load-balance' will cause a traceback and reload               |
| <a href="#">CSCvu07880</a> | ASA on QP platforms display wrong core dump filesystem space (50 GB)                              |
| <a href="#">CSCvu12039</a> | Cluster data unit might fail to synchronize SCTP configuration from the control unit after bootup |
| <a href="#">CSCvu12045</a> | Deployment fails for NGIPS with error "System (/etc/rc.d/init.d/netif-speed eth0) Failed"         |
| <a href="#">CSCvu12248</a> | ASA-FPWR 1010 traceback and reload when users connect using AnyConnect VPN                        |
| <a href="#">CSCvu16423</a> | ASA 9.12(2) - Multiple tracebacks due to Unicorn Proxy Thread                                     |
| <a href="#">CSCvu17924</a> | FTD failover units traceback and reload on DATAPATH                                               |
| <a href="#">CSCvu17965</a> | ASA generated a traceback and reloaded when changing the port value of a manual nat rule          |
| <a href="#">CSCvu20007</a> | Config_XML_Response from LINA is not in the correct format,Lina reporting as No memory available. |
| <a href="#">CSCvu20666</a> | Few FPR 2100 series External Authentication RADIUS not taking configuration                       |
| <a href="#">CSCvu26296</a> | ASA interface ACL dropping snmp control-plane traffic from ASA                                    |
| <a href="#">CSCvu26561</a> | WebVPN SSO Gives Unexpected Results when Integrated with Kerberos                                 |
| <a href="#">CSCvu29184</a> | Cisco Firepower Threat Defense Software Command File Overwrite Vulnerability                      |
| <a href="#">CSCvu29395</a> | Traceback observed while performing master role change with active IGMP joins                     |
| <a href="#">CSCvu29660</a> | Block exhaustion snapshot not created when available blocks goes to zero                          |
| <a href="#">CSCvu32698</a> | ASA Crashes in SNMP while joining the cluster when key config-key password-encryption" is present |
| <a href="#">CSCvu33992</a> | traceback: ASA reloaded lina_sigcrash+1394                                                        |
| <a href="#">CSCvu34413</a> | SSH keys lost in ASA after reload                                                                 |
| <a href="#">CSCvu40213</a> | ASA traceback in Thread Name kerberos_recv                                                        |
| <a href="#">CSCvu40324</a> | ASA traceback and reload with Flow lookup calling traceback                                       |
| <a href="#">CSCvu40398</a> | ASAv reload due to FIPS SELF-TEST FAILURE after enabling FIPS                                     |
| <a href="#">CSCvu43924</a> | GIADDR of DHCP Discover packet is changed to the ip address of dhcp-network-scope                 |
| <a href="#">CSCvu45748</a> | ASA traceback in threadname 'ppp_timer_thread'                                                    |
| <a href="#">CSCvu45822</a> | ASA experienced a traceback and reloaded                                                          |

| Bug ID                     | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvu48886</a> | FTD deployment failure when removing non-default "crypto ikev2 limit max-in-negotiation-sa"        |
| <a href="#">CSCvu49625</a> | [PKI] Standard Based IKEv2 Certificate Auth session does second userfromcert lookup unnecessarily  |
| <a href="#">CSCvu55469</a> | FTD - Connection idle timeout doesn't reset                                                        |
| <a href="#">CSCvu55843</a> | ASA traceback after TACACS authorized user made configuration changes                              |
| <a href="#">CSCvu61704</a> | ASA high CPU with intel_82576_check_link_thread impacting on overall unit performance              |
| <a href="#">CSCvu65688</a> | IKEv2 CAC "Active SAs" counter out of sync with the real number of sessions despite CSCvt98599     |
| <a href="#">CSCvu68529</a> | Embryonic connections limit does not work consistently                                             |
| <a href="#">CSCvu70931</a> | Cluster / aaa-server key missing after "no key config-key" is entered                              |
| <a href="#">CSCvu72094</a> | ASA traceback and reload on thread name DATAPATH                                                   |
| <a href="#">CSCvu73207</a> | DSCP values not preserved in DTLS packets towards AnyConnect users                                 |
| <a href="#">CSCvu77095</a> | ASA unable to delete ACEs with remarks and display error "Specified remark does not exist"         |
| <a href="#">CSCvu78721</a> | Cannot change (modify) interface speed after upgrade                                               |
| <a href="#">CSCvu89110</a> | ASA: Block new conns even when the "logging permit-hostdown" is set & TCP syslog is down           |
| <a href="#">CSCvu90727</a> | Native VPN client with EAP-TLS authentication fails to connect to ASA                              |
| <a href="#">CSCvu91097</a> | Cisco Firepower Management Center Software Policy Vulnerability                                    |
| <a href="#">CSCvu91792</a> | SNMP IfInDiscards OIDs for Internal-Data 0/0 and 0/1 may return incorrect values                   |
| <a href="#">CSCvu98222</a> | FTD Lina engine may traceback in datapath after enabling SSL decryption policy                     |
| <a href="#">CSCvv04584</a> | Multicast traffic is being dropped with the resson no-mcast-intrf                                  |
| <a href="#">CSCvv07721</a> | FirePOWER: System>Users>User Roles Pages is blank on Firepower 7000 and Firepower 8000 series      |
| <a href="#">CSCvv07864</a> | Multicast EIGRP traffic not seen on internal FTD interface                                         |
| <a href="#">CSCvv08244</a> | Firepower module may block trusted HTTPS connections matching 'Do not decrypt' SSL decryption rule |
| <a href="#">CSCvv08684</a> | Cluster site-specific MAC addresses not rewritten by flow-offload                                  |
| <a href="#">CSCvv09396</a> | Stale VPN routes for L2TP, after the session was terminated                                        |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvv10778</a> | Traceback in threadname DATAPATH (5585) or Lina (2100) after upgrade to 9.12.4                       |
| <a href="#">CSCvv12127</a> | Series 3 policy deploy can fail when adding a large number of IPV4 source and destination AC rules.  |
| <a href="#">CSCvv12857</a> | ASA gets frozen after crypto engine failure                                                          |
| <a href="#">CSCvv15572</a> | ASA traceback observed when "config-url" is entered while creating new context                       |
| <a href="#">CSCvv16082</a> | stress/low memory: assert: mh->mh_mem_pool > MEMPOOL_UNDEFINED && mh->mh_mem_pool < MEMPOOL_MAX_TYPE |
| <a href="#">CSCvv19230</a> | ASAv Anyconnect users unexpectedly disconnect with reason: Idle Timeout                              |
| <a href="#">CSCvv20450</a> | FMC 6.4 to 6.7 upgrade fails "Error running script 500_rpms/110_generate_dbaccess.sh"                |
| <a href="#">CSCvv23370</a> | Observed traceback in FPR2130 while running webVPN, SNMP related traffic.                            |
| <a href="#">CSCvv25394</a> | After upgrade ASA swapped names for disks, disk0 became disk1 and vice versa.                        |
| <a href="#">CSCvv25839</a> | reCAPTCHA is not working when SSL decryption is enable.                                              |
| <a href="#">CSCvv28997</a> | ASA Traceback and reload on thread name Crypto CA                                                    |
| <a href="#">CSCvv29687</a> | Rate-limit syslogs 780001/780002 by default on ASA                                                   |
| <a href="#">CSCvv30172</a> | Intermittently after reboot, ADI can't join KCD                                                      |
| <a href="#">CSCvv31334</a> | Lina traceback and reload seen on trying to switch peer on KP HA with 6.6.1-63                       |
| <a href="#">CSCvv31629</a> | Intermittently embedded ping reply over GRE drops on FTD cluster if traffic passes asymmetrically.   |
| <a href="#">CSCvv32333</a> | ASA still doesn't allow to poll internal-data0/0 counters via SNMP in multiple mode                  |
| <a href="#">CSCvv32425</a> | ASA traceback when running show asp table classify domain permit                                     |
| <a href="#">CSCvv34003</a> | 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           |
| <a href="#">CSCvv34140</a> | ASA IKEv2 VTI - Failed to request SPI from CTM as responder                                          |
| <a href="#">CSCvv36518</a> | ASA: Extended downtime after reload after CSCUw51499 fix                                             |
| <a href="#">CSCvv36725</a> | ASA logging rate-limit 1 5 message ... limits to 1 message in 10 seconds instead of 5                |
| <a href="#">CSCvv37629</a> | Malformed SIP packets leads to 4k block hold-up till SIP conn timeout causing probable traffic issue |
| <a href="#">CSCvv40223</a> | Error parsing flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.cdb, when trying to modify/read the user-db     |
| <a href="#">CSCvv41453</a> | Removing static ipv6 route from management-only route table affects data traffic                     |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvv43484</a> | ASA stops processing RIP packets after system upgrade                                                |
| <a href="#">CSCvv44270</a> | ASAv5 reloads without traceback.                                                                     |
| <a href="#">CSCvv48942</a> | Snmpwalk showing traffic counter as 0 for failover interface                                         |
| <a href="#">CSCvv49698</a> | ASA Anyconnect url-redirect not working for ipv6                                                     |
| <a href="#">CSCvv49800</a> | ASA/FTD: HA switchover doesn't happen with graceful reboot of firepower chassis                      |
| <a href="#">CSCvv50338</a> | Traceback Cluster unit on snpi_nat_xlate_destroy+2508                                                |
| <a href="#">CSCvv53696</a> | ASA/FTD traceback and reload during AAA or CoA task of Anyconnect user                               |
| <a href="#">CSCvv56644</a> | Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS             |
| <a href="#">CSCvv57590</a> | ASA: ACL compilation takes more time on standby                                                      |
| <a href="#">CSCvv57842</a> | WebSSL clientless user accounts being locked out on 1st bad password                                 |
| <a href="#">CSCvv58332</a> | ASA/FTD is reading BGP MP_REACH_NLRI attribute's next-hop bytes in reverse order                     |
| <a href="#">CSCvv58605</a> | ASA traceback and reload in thread:Crypto CA,mem corruption by unvirtualized pki global table in MTX |
| <a href="#">CSCvv59036</a> | Static routes deleted from the FMC without user deleting it.                                         |
| <a href="#">CSCvv59676</a> | Snort2: Implement aggressive pruning for certificate cache for TLS to free up memory                 |
| <a href="#">CSCvv62305</a> | ASA traceback and reload in fover_parse when attempting to join the failover pair.                   |
| <a href="#">CSCvv63412</a> | ASA dropping all traffic with reason "No route to host" when tmatch compilation is ongoing           |
| <a href="#">CSCvv65184</a> | Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS             |
| <a href="#">CSCvv66005</a> | ASA traceback and reload on inspect esmtp                                                            |
| <a href="#">CSCvv66920</a> | Inner flow: U-turn GRE flows trigger incorrect connection flow creation                              |
| <a href="#">CSCvv67500</a> | ASA 9.12 random traceback and reload in DATAPATH                                                     |
| <a href="#">CSCvv70984</a> | ASA traceback while modifying the bookmark SSL Ciphers configuration                                 |
| <a href="#">CSCvv72466</a> | OSPF network commands go missing in the startup-config after upgrading the ASA                       |
| <a href="#">CSCvv73017</a> | Traceback due to fover and ssh thread                                                                |
| <a href="#">CSCvv79897</a> | Block "sensor restart" command for FTD units to prevent Lina crash and system reboot event           |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvv86926</a> | Unexpected traceback and reload on FTD creating a Core file                                          |
| <a href="#">CSCvv87232</a> | ASA: High number of CPU hog in igb_saleen_io_sfp_mod_poll_thread process                             |
| <a href="#">CSCvv87496</a> | ASA cluster members 2048 block depletion due to "VPN packet redirect on peer"                        |
| <a href="#">CSCvv88017</a> | ASA: EasyVPN HW Client triggers duplicate phase 2 rekey causing disconnections across the tunnel     |
| <a href="#">CSCvv90181</a> | No deployment failure reason in transcript if 'show running-config' is running during deployment     |
| <a href="#">CSCvv90720</a> | ASA/FTD: Mac address-table flap seen on connected switch after a HA switchover                       |
| <a href="#">CSCvv94701</a> | ASA keeps reloading with "octnic_hm_thread". After the reload, it takes very long time to recover.   |
| <a href="#">CSCvv97877</a> | Secondary unit not able to join the cluster                                                          |
| <a href="#">CSCvw01028</a> | 7K/8K devices experience unresponsiveness if upgraded to 6.4.0.[9,10,11] from release prior to 6.4.0 |
| <a href="#">CSCvw05393</a> | Certificate validation syslog is not generated on OCSP revocation check                              |
| <a href="#">CSCvw06195</a> | ASA traceback cp_midpath_process_thread                                                              |
| <a href="#">CSCvw07000</a> | Snort busy drops with PDTS Tx queue stuck                                                            |
| <a href="#">CSCvw12008</a> | ASA traceback and reload while executing "show tech-support" command                                 |
| <a href="#">CSCvw12100</a> | ASA stale VPN Context seen for site to site and AnyConnect sessions                                  |
| <a href="#">CSCvw19272</a> | Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability                 |
| <a href="#">CSCvw21844</a> | FTD traceback and reload on DATAPATH thread when processing encapsulated flows                       |
| <a href="#">CSCvw22881</a> | radius_rcv_auth can shoot up control plane CPU to 100%.                                              |
| <a href="#">CSCvw22986</a> | Secondary unit stuck in Bulk sync infinitely due to interface of Primary stuck in init state         |
| <a href="#">CSCvw23199</a> | ASA/FTD Traceback and reload in Thread Name: Logger                                                  |
| <a href="#">CSCvw24164</a> | heartbeat false positives                                                                            |
| <a href="#">CSCvw24556</a> | TCP File transfer (Big File) not properly closed when Flow offload is enabled                        |
| <a href="#">CSCvw24700</a> | FPR2100 ASA running 9.12.4.7 fails to boot with ERROR: FIPS Self-Test failure, fipsPostGFSboxKat     |
| <a href="#">CSCvw26171</a> | ASA syslog traceback while strncpy NULL string passed from SSL library                               |
| <a href="#">CSCvw26331</a> | ASA traceback and reload on Thread Name: ci/console                                                  |

| Bug ID                     | Headline                                                                                       |
|----------------------------|------------------------------------------------------------------------------------------------|
| <a href="#">CSCvw26544</a> | Cisco ASA and FTD Software SIP Denial of Service Vulnerability                                 |
| <a href="#">CSCvw27301</a> | IKEv2 with EAP, MOBIKE status fails to be processed.                                           |
| <a href="#">CSCvw28894</a> | SFDataCorrelator slow startup and vuln remap due to duplicate entries in vuln tables           |
| <a href="#">CSCvw31254</a> | User with shell set to /bin/false on 8350 sensor causes deployment failure                     |
| <a href="#">CSCvw31569</a> | Director/Backup flows are left behind and traffic related to this flow is blackholed           |
| <a href="#">CSCvw32518</a> | ASASM traceback and reload after upgrade up to 9.12(4)4 and higher                             |
| <a href="#">CSCvw33987</a> | ASAv/2100 Smart License failure post upgrade                                                   |
| <a href="#">CSCvw36662</a> | TACACS+ ASCII password change request not handled properly                                     |
| <a href="#">CSCvw37259</a> | VPN syslogs are generated at a rate of 600/s until device goes into a hang state               |
| <a href="#">CSCvw41728</a> | Unable to configure syslog via CLI on FTD                                                      |
| <a href="#">CSCvw42999</a> | 9.10.1.11 ASA on FPR2110 traceback and reloads randomly                                        |
| <a href="#">CSCvw43486</a> | ASA/FTD Traceback and reload during PBR configuration change                                   |
| <a href="#">CSCvw43534</a> | A Null pointer dereference vulnerability exists in Mozilla Network S ...                       |
| <a href="#">CSCvw43543</a> | The inflateMark function in inflate.c in zlib 1.2.8 might allow cont ...                       |
| <a href="#">CSCvw43586</a> | A vulnerability was found in gnutls versions from 3.5.8 before 3.6.7 ...                       |
| <a href="#">CSCvw43615</a> | An issue was discovered in GnuTLS before 3.6.15. A server can trigge ...                       |
| <a href="#">CSCvw44122</a> | ASA: "class-default" class-map redirecting non-DNS traffic to DNS inspection engine            |
| <a href="#">CSCvw46702</a> | FTD Cluster secondary units fail to join cluster due to application configuration sync timeout |
| <a href="#">CSCvw47321</a> | IPSec transport mode traffic corruption for inbound traffic for some FPR platforms             |
| <a href="#">CSCvw48517</a> | DAP stopped working after upgrading the ASA to 9.13(1)13                                       |
| <a href="#">CSCvw49531</a> | Applications are being misclassified after VDB upgrade.                                        |
| <a href="#">CSCvw51462</a> | IPv4 Default Tunneled Route Rejected                                                           |
| <a href="#">CSCvw51950</a> | FPR 4K: SSL trust-point removed from new active ASA after manual Failover                      |
| <a href="#">CSCvw51985</a> | ASA: AnyConnect sessions cannot be resumed due to ipv6 DACL failure                            |
| <a href="#">CSCvw52098</a> | Upgrade to 6.4.0.11 fails at 800_post/901_reapply_sensor_policy.pl on standby 2120             |
| <a href="#">CSCvw52609</a> | Cisco ASA and FTD Software Web Services Buffer Overflow Denial of Service Vulnerability        |

| Bug ID                     | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvw53255</a> | FTD/ASA HA: Standby Unit FXOS is still able to forward traffic even after failover due to traceback |
| <a href="#">CSCvw53427</a> | ASA Fails to process HTTP POST with SAML assertion containing multiple query parameters             |
| <a href="#">CSCvw53796</a> | Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerability                         |
| <a href="#">CSCvw53884</a> | M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service           |
| <a href="#">CSCvw54640</a> | FPR-4150 - ASA traceback and reload with thread name DATAPATH                                       |
| <a href="#">CSCvw54802</a> | Revocation check fails to move to none after ocsf check fails due to server being unavailable       |
| <a href="#">CSCvw58414</a> | Name of anyconnect custom attribute of type dynamic-split-exclude-domains is changed after reload   |
| <a href="#">CSCvw58865</a> | sftunnel TLS handshake should not include NewSessionTicket                                          |
| <a href="#">CSCvw59035</a> | Connection issues to directly connected IP from FTD BVI address                                     |
| <a href="#">CSCvw60177</a> | Standby/Secondary cluster unit might crash in Thread Name: fover_parse and "cluster config sync"    |
| <a href="#">CSCvw62526</a> | ASA traceback and reload on engineering ASA build - 9.12.3.237                                      |
| <a href="#">CSCvw62820</a> | memcached 1.5.6 or higher update                                                                    |
| <a href="#">CSCvw63862</a> | ASA: Random L2TP users cannot access resources due to stale ACL filter entries                      |
| <a href="#">CSCvw71766</a> | ASA traceback and reload in Thread: Ikev2 Daemon                                                    |
| <a href="#">CSCvw74495</a> | Application detection fails for FTP service when an unsuccessful login is encountered.              |
| <a href="#">CSCvw74940</a> | ASA traceback in IKE Daemon and reload                                                              |
| <a href="#">CSCvw79208</a> | Incorrect URL normalization when "http://" substring is at a latter stage in the input string       |
| <a href="#">CSCvw79294</a> | sftunnel logging huge number of logs to messages file                                               |
| <a href="#">CSCvw81322</a> | FTD running multi-instance mode gets snort GID 3 rules disabled after SRU install and deploy        |
| <a href="#">CSCvw81897</a> | ASA: OpenSSL Vulnerability CVE-2020-1971                                                            |
| <a href="#">CSCvw82629</a> | ASA Tracebacks when making "configuration session" changes regarding an ACL.                        |
| <a href="#">CSCvw83572</a> | BVI HTTP/SSH access is not working in versions 9.14.1.30 or above                                   |
| <a href="#">CSCvw84339</a> | Managed device backup fails, for FTD, if hostname exceeds 30 characters                             |

| Bug ID                     | Headline                                                                                        |
|----------------------------|-------------------------------------------------------------------------------------------------|
| <a href="#">CSCvw85377</a> | URL is not updated in the access policy URL filtering rule                                      |
| <a href="#">CSCvw87788</a> | ASA traceback and reload webvpn thread                                                          |
| <a href="#">CSCvw89365</a> | ASA/FTD may traceback and reload during certificate changes.                                    |
| <a href="#">CSCvw93272</a> | Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability                   |
| <a href="#">CSCvw93282</a> | Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability                   |
| <a href="#">CSCvw93513</a> | Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability                   |
| <a href="#">CSCvw95301</a> | ASA traceback and reload with Thread name: ssh when capture was removed                         |
| <a href="#">CSCvw96295</a> | Unable to add Route Tracking to static route in FMC 6.4.0.10                                    |
| <a href="#">CSCvw96488</a> | Traceback in inspect_h323_ras+1810                                                              |
| <a href="#">CSCvw97821</a> | ASA: VPN traffic does not pass if no dACL is provided in CoA                                    |
| <a href="#">CSCvw98840</a> | ASA: dACL with no IPv6 entries is not applied to v6 traffic after CoA                           |
| <a href="#">CSCvx01381</a> | FMC GUI year drop-down list for Manual Time set up only listing until 2020                      |
| <a href="#">CSCvx02869</a> | Traceback in Thread Name: Lic TMR                                                               |
| <a href="#">CSCvx03764</a> | Offload rewrite data needs to be fixed for identity nat traffic and clustering environment      |
| <a href="#">CSCvx04057</a> | When SGT name is unresolved and used in ACE, line is not being ignored/inactive                 |
| <a href="#">CSCvx04643</a> | ASA reload is removing 'content-security-policy' config                                         |
| <a href="#">CSCvx05381</a> | Cisco ASA and FTD Software Command Injection Vulnerability                                      |
| <a href="#">CSCvx05956</a> | High snort cpu usage while copying navl attribute                                               |
| <a href="#">CSCvx08734</a> | ASA: default IPv6/IPv4 route tunneled does not work                                             |
| <a href="#">CSCvx11295</a> | ASA may traceback and reload on thread Crypto CA                                                |
| <a href="#">CSCvx11460</a> | Firepower 2110 silently dropping traffic with TFC enabled on the remote end                     |
| <a href="#">CSCvx13694</a> | ASA/FTD traceback in Thread Name: PTHREAD-4432                                                  |
| <a href="#">CSCvx15040</a> | DHCP Proxy Offer is getting drop on the ASA/FTD                                                 |
| <a href="#">CSCvx16202</a> | self referenced object pushed from FMC results in lina crash with error - loop in grp hierarchy |
| <a href="#">CSCvx17664</a> | ASA may traceback and reload in Thread Name 'webvpn_task'                                       |
| <a href="#">CSCvx17785</a> | Crash seen consistently by adding/removing acl & entering into route-map command                |
| <a href="#">CSCvx20352</a> | Snort PDTS buffer corruption during upgrade or heavy traffic load                               |

| Bug ID                     | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvx26286</a> | IPV6 address was marked as duplicate on both units and ipv6 Traffic was stopped after the failover. |
| <a href="#">CSCvx26808</a> | FTD traceback and reload on process lina on FPR2100 series                                          |
| <a href="#">CSCvx27430</a> | ASA: Unable to import PAC file if FIPS is enabled.                                                  |
| <a href="#">CSCvx29771</a> | Firewall CPU can increase after a bulk routing update with flow offload                             |
| <a href="#">CSCvx30314</a> | ASA 9.15.1.7 traceback and reload in ssl midpath                                                    |
| <a href="#">CSCvx41171</a> | Concurrent modification of ACL configuration breaks output of "show running-config" completely      |
| <a href="#">CSCvx42197</a> | ASA EIGRP route stuck after neighbour disconnected                                                  |
| <a href="#">CSCvx44401</a> | FTD/ASA traceback in Thread Name : Unicorn Proxy Thread                                             |
| <a href="#">CSCvx48490</a> | SSL Decrypted https flow EOF events showing 'Initiator/Responder' Packets as 0                      |
| <a href="#">CSCvx50366</a> | Traceback in Thread Name: fover_health_monitoring_thread                                            |
| <a href="#">CSCvx51860</a> | Failed lookups due to license check when the sensor URL lookup is enabled in 6.4.0.x                |
| <a href="#">CSCvx52122</a> | ASA traceback and reload in SNMP Notify Thread while deleting transparent context                   |
| <a href="#">CSCvx59120</a> | COA Received before data tunnel comes up results in tear down of parent session                     |
| <a href="#">CSCvx71434</a> | ASA/FTD Traceback and reload in Thread Name: pix_startup_thread due to asa_run_ttyS0 script         |
| <a href="#">CSCvx74035</a> | ASA traceback and reload after run "clear configure all" with multiple ACLs and objects configured  |
| <a href="#">CSCvy09252</a> | 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 57: Resolved Bugs in Version 6.4.0.11*

| Bug ID                     | Headline                                                         |
|----------------------------|------------------------------------------------------------------|
| <a href="#">CSCvv59788</a> | Lina traceback on 21xx following upgrade from 6.4.0.8 to 6.4.0.9 |
| <a href="#">CSCvw42241</a> | CRL command missing on FP1k                                      |

## Resolved Bugs in Version 6.4.0.10

Table last updated: 2020-12-08

**Table 58: Resolved Bugs in Version 6.4.0.10**

| Bug ID                     | Headline                                                                                              |
|----------------------------|-------------------------------------------------------------------------------------------------------|
| <a href="#">CSCuw95798</a> | Cisco Firepower Management Center Software Cross-Site Scripting Vulnerabilities                       |
| <a href="#">CSCuz24872</a> | Original Client IP does not populate for dropped events when inline normalization enabled             |
| <a href="#">CSCvh19161</a> | ASA/FTD traceback and reload in Thread Name: SXP CORE                                                 |
| <a href="#">CSCvi46896</a> | FeedDownloader should not update status to Downloading after download is complete                     |
| <a href="#">CSCvj93609</a> | ASA traceback on spin_lock_release_actual                                                             |
| <a href="#">CSCvm69545</a> | Multiple Cisco Products SNORT HTTP Detection Engine File Policy Bypass Vulnerability                  |
| <a href="#">CSCvn27043</a> | Hostscan: LastSuccessfulInstallParams can not be detected by Hostscan                                 |
| <a href="#">CSCvn78076</a> | Firepower: Misleading stats w.r.t "Memory Usage" being displayed under System->Monitoring->Statistics |
| <a href="#">CSCvo26597</a> | CLI Banner not seen on FTD                                                                            |
| <a href="#">CSCvo59683</a> | Large number of stale Objects in EOAttributes table results in high CPU/backup failure                |
| <a href="#">CSCvp45786</a> | Not able to upload the STIX or Flat File Manually under Threat Intelligence Director                  |
| <a href="#">CSCvp56719</a> | Cisco FMC and FTD Software sftunnel Pass the Hash Vulnerability                                       |
| <a href="#">CSCvp56744</a> | Cisco FMC and FTD Software Directory Traversal Vulnerability                                          |
| <a href="#">CSCvp76950</a> | FTD Traceback and Reload on Lina thread for thread_logger                                             |
| <a href="#">CSCvp99327</a> | FMC UI Unresponsive After Attempt To Register Smart License With Smart Satellite                      |
| <a href="#">CSCvq04619</a> | FTD ftd_sftunnel core is generated after upgrading from 6.4.0                                         |
| <a href="#">CSCvq11282</a> | Cisco Firepower Management Center Software Denial of Service Vulnerability                            |
| <a href="#">CSCvq20707</a> | Snort rendering block verdict for rules with action of alert.                                         |
| <a href="#">CSCvq43920</a> | Cisco Firepower Threat Defense Software Hidden Commands Vulnerability                                 |
| <a href="#">CSCvq46587</a> | After failover, Active unit tcp sessions are not removed when timeout reached                         |
| <a href="#">CSCvq53902</a> | Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities                       |
| <a href="#">CSCvq63653</a> | FTD may crash when processing fragmented packets                                                      |
| <a href="#">CSCvq95694</a> | Memory leak SSL_ALLOC [ERROR] ssl_alloc.c:113:ssl_alloc_destroy()                                     |

| Bug ID                     | Headline                                                                                         |
|----------------------------|--------------------------------------------------------------------------------------------------|
| <a href="#">CSCvr27584</a> | Estreamer process queries wrong database for rna_policy_rules table and causes excessive logging |
| <a href="#">CSCvr46901</a> | Analysis Connection Events doesn't show and report all the events in UI                          |
| <a href="#">CSCvr49229</a> | FMC high CPU utilization in sfmbsservice                                                         |
| <a href="#">CSCvr51955</a> | Estreamer should terminate a connection when not receiving ACKs for a long time                  |
| <a href="#">CSCvr53058</a> | Cisco Firepower Threat Defense Software TCP Intercept Bypass Vulnerability                       |
| <a href="#">CSCvr55741</a> | FMC shows policies out of date after successful deploy                                           |
| <a href="#">CSCvr57051</a> | Policy deployment failed with error "Can't use an undefined value as a HASH reference "          |
| <a href="#">CSCvr63851</a> | SSH via External Auth to NGIPS succeeds then closes immediately                                  |
| <a href="#">CSCvr66798</a> | DNS Application Detector sometimes fails to detect DNS traffic                                   |
| <a href="#">CSCvr76029</a> | FTD-HA: after restoring FTD-HA backup file, snort process will be down                           |
| <a href="#">CSCvr76044</a> | FTD Snort Rule Profiling does not work consistently - log folder is missing                      |
| <a href="#">CSCvr79974</a> | Configuration might not replicated if packet loss on the failover Link                           |
| <a href="#">CSCvr86016</a> | FMC connections to v3.sds.cisco.com are bypassing proxy                                          |
| <a href="#">CSCvr94406</a> | Cannot download TAXII feeds in Intelligence Sources v6.2.3 -> v6.4.0.4 on either HTTP or HTTPS   |
| <a href="#">CSCvr99222</a> | NTP configuration is not synchronized to LINA on Multi Instance                                  |
| <a href="#">CSCvs01422</a> | Lina traceback when changing device mode of FTD                                                  |
| <a href="#">CSCvs05066</a> | Snort file mempool corruption leads to performance degradation and process failure.              |
| <a href="#">CSCvs09533</a> | FP2100: Traceback and reload when processing traffic through more than two inline sets           |
| <a href="#">CSCvs10748</a> | Cisco ASA Software and FTD Software Web Services Denial of Service Vulnerability                 |
| <a href="#">CSCvs21705</a> | admin user is not authorized to access the device routing configuration inside the domain.       |
| <a href="#">CSCvs24215</a> | Firepower Device Manager (FDM) option to disable SSL rekey is not reflected on the config        |
| <a href="#">CSCvs28290</a> | Cisco Firepower Threat Defense Software SSL Input Validation Denial of Service Vulnerability     |
| <a href="#">CSCvs39253</a> | Firepower 7000 & 8000 cannot send emails on version 6.4                                          |
| <a href="#">CSCvs41883</a> | Deployment fails after upgrading to 6.4.0.x if ND policy refs are missing                        |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvs49104</a> | Network Discovery Policy rules are ignored if it uses network groups                                 |
| <a href="#">CSCvs50137</a> | Same Security Zone used in ACP rule is Not pushed to NGFW rules                                      |
| <a href="#">CSCvs50931</a> | Policy deployment fails subsequent to SRU                                                            |
| <a href="#">CSCvs56802</a> | Cisco Firepower 2100 Series SSL/TLS Inspection Denial of Service Vulnerability                       |
| <a href="#">CSCvs56888</a> | Cisco Firepower Threat Defense Software TCP Flood Denial of Service Vulnerability                    |
| <a href="#">CSCvs64510</a> | Deployment failure with message (Can't call method "binip" on unblessed reference)                   |
| <a href="#">CSCvs71766</a> | Cisco Firepower Management Center Software Open Redirect Vulnerability                               |
| <a href="#">CSCvs74452</a> | SFDataCorrelator and Snort process cores repeatedly while loading malware seed file                  |
| <a href="#">CSCvs74586</a> | Firepower FTD transparent does not decode non-ip packets                                             |
| <a href="#">CSCvs77334</a> | FTD failover due to error "Inspection engine in other unit has failed due to snort and disk failure" |
| <a href="#">CSCvs82829</a> | Calls fail once anyconnect configuration is added to the site to site VPN tunnel                     |
| <a href="#">CSCvs87168</a> | SNORT Fatal Error due to out of range interface ID                                                   |
| <a href="#">CSCvs91270</a> | Inspect Interruption - Error in deployment page.                                                     |
| <a href="#">CSCvt00113</a> | ASA/FTD traceback and reload due to memory leak in SNMP community string                             |
| <a href="#">CSCvt01763</a> | Application classification is not retried if a flow is marked brute force failed.                    |
| <a href="#">CSCvt02409</a> | Cisco Firepower Threat Defense Software Inline Pair/Passive Mode DoS Vulnerability                   |
| <a href="#">CSCvt03598</a> | Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability              |
| <a href="#">CSCvt03794</a> | Policy deployment failure after SRU update on FTD with passive zone                                  |
| <a href="#">CSCvt04377</a> | When vlan encapsulation is exceeded decoding errors are depleting disk space.                        |
| <a href="#">CSCvt04535</a> | Allow 30-seconds of NFE microengine missing heartbeat faults before engaging error recovery          |
| <a href="#">CSCvt04560</a> | SCTP heartbeats failing across the firewall in Cluster deployment.                                   |
| <a href="#">CSCvt09940</a> | Cisco Firepower 4110 ICMP Flood Denial of Service Vulnerability                                      |
| <a href="#">CSCvt13445</a> | Cisco ASA and FTD Software FTP Inspection Bypass Vulnerability                                       |
| <a href="#">CSCvt16642</a> | FMC not sending some audit messages to remote syslog server                                          |
| <a href="#">CSCvt18028</a> | Cisco ASA and FTD WebVPN CRLF Injection Vulnerability                                                |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvt20709</a> | Wrong direction in SSL-injected RESET causes it to exit through wrong interface, causing MAC flap    |
| <a href="#">CSCvt24328</a> | FTD: Traceback and reload related to lina_host_file_open_raw function                                |
| <a href="#">CSCvt26067</a> | Active FTP fails when secondary interface is used on FTD                                             |
| <a href="#">CSCvt28182</a> | sctp-state-bypass is not getting invoked for inline FTD                                              |
| <a href="#">CSCvt35053</a> | Cisco Firepower Management Center Software Cross-Site Scripting Vulnerabilities                      |
| <a href="#">CSCvt35233</a> | Excessive logging from the daq modules process_snort_verdict verdict blacklist                       |
| <a href="#">CSCvt35897</a> | Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS Vuln            |
| <a href="#">CSCvt39135</a> | snort instances CPU spikes to >90% at low non-SSL traffic with SSL policy applied                    |
| <a href="#">CSCvt39349</a> | Registration of device should be allowed as long as deploy status = DEPLOYED or FAILED               |
| <a href="#">CSCvt41333</a> | Dynamic RRI route is not destroyed when IKEv2 tunnel goes down                                       |
| <a href="#">CSCvt45863</a> | Crypto ring stalls when the length in the ip header doesn't match the packet length                  |
| <a href="#">CSCvt48941</a> | FTD Standby unit does not join HA due to "HA state progression failed due to APP SYNC timeout"       |
| <a href="#">CSCvt50263</a> | FMC Unable to fetch VPN troubleshooting logs from WM Model devices                                   |
| <a href="#">CSCvt50946</a> | Stuck uauth entry rejects AnyConnect user connections despite fix of CSCvi42008                      |
| <a href="#">CSCvt52782</a> | ASA traceback Thread name - webvpn_task                                                              |
| <a href="#">CSCvt54267</a> | Cisco Firepower Management Center Software Denial of Service Vulnerability                           |
| <a href="#">CSCvt59015</a> | KP IOQ driver. Add defensive parameter and state checks.                                             |
| <a href="#">CSCvt59253</a> | ASA 9.13.1.7 traceback and reload while processing hostscan data (process name LINA )                |
| <a href="#">CSCvt60190</a> | Cisco ASA and FTD Web Services File Upload Denial of Service Vulnerability                           |
| <a href="#">CSCvt61370</a> | Events may stop coming from a device due to a communication deadlock                                 |
| <a href="#">CSCvt63556</a> | Local User Password not updating in 6.4.0.9                                                          |
| <a href="#">CSCvt64270</a> | ASA is sending failover interface check control packets with a wrong destination mac address         |
| <a href="#">CSCvt64642</a> | FMC -Deployment Failure- Anyconnect - "Certificate Map" using "DC (Domain Component)" to match cert. |

| Bug ID                     | Headline                                                                                        |
|----------------------------|-------------------------------------------------------------------------------------------------|
| <a href="#">CSCvt66136</a> | 6.4.0.9 upgrade from 6.4.0 with CC mode causes httpsd.conf to have an incorrect config          |
| <a href="#">CSCvt66351</a> | NetFlow reporting impossibly large flow bytes                                                   |
| <a href="#">CSCvt66875</a> | AppId caches proxy IP instead of tunneled IP for ultrasurf                                      |
| <a href="#">CSCvt68131</a> | FTD traceback and reload on thread "IKEv2 Mgd Timer Thread"                                     |
| <a href="#">CSCvt70322</a> | Cisco ASA Software and FTD Software Web Services Denial of Service Vulnerability                |
| <a href="#">CSCvt73806</a> | FTD traceback and reload on FP2120 LINA Active Box. VPN                                         |
| <a href="#">CSCvt73808</a> | Handling for longer header length messages going from DAQ to Oct driver                         |
| <a href="#">CSCvt75241</a> | Redistribution of VPN advertised static routes fail after reloading the FTD on FPR2100          |
| <a href="#">CSCvt78068</a> | Time sync do not work correctly for FTD on FP1000/1100 series platform                          |
| <a href="#">CSCvt79777</a> | duplicate ip addresses in sfiproxy.conf                                                         |
| <a href="#">CSCvt81628</a> | False positives for ultrasurf                                                                   |
| <a href="#">CSCvt83121</a> | Cisco ASA and FTD Software OSPFv2 Link-Local Signaling Denial of Service Vulnerability          |
| <a href="#">CSCvt86188</a> | SNMP traps can't be generated via diagnostic interface                                          |
| <a href="#">CSCvt93142</a> | ASA should allow null sequence encoding in certificates for client authentication.              |
| <a href="#">CSCvt95517</a> | Certificate mapping for AnyConnect on FTD stops working.                                        |
| <a href="#">CSCvu01039</a> | Traceback: Modifying FTD inline-set tap-mode configuration with active traffic                  |
| <a href="#">CSCvu08013</a> | DTLS v1.2 and AES-GCM cipher when used drops a particular size packet frequently.               |
| <a href="#">CSCvu08422</a> | Cisco Firepower Threat Defense Software Multi-Instance Container Escape Vulnerability           |
| <a href="#">CSCvu12684</a> | HKT - Failover time increases with upgrade to 9.8.4.15                                          |
| <a href="#">CSCvu15801</a> | Cisco ASA and FTD Software SIP Denial of Service Vulnerability                                  |
| <a href="#">CSCvu25030</a> | FTD 6.4.0.8 traceback & reload on thread name : CP processing                                   |
| <a href="#">CSCvu30134</a> | High unmanaged disk usage on /ngfw due to logrotate and missing /var/spool/cron/root directory. |
| <a href="#">CSCvu38795</a> | FTD firewall unit cannot join the cluster after a traceback due to invalid interface GOID entry |
| <a href="#">CSCvu42434</a> | ASA: High CPU due to stuck running SSH sessions / Unable to SSH to ASA                          |
| <a href="#">CSCvu43355</a> | FTD Lina traceback in datapath due to double free                                               |

| Bug ID                     | Headline                                                                                       |
|----------------------------|------------------------------------------------------------------------------------------------|
| <a href="#">CSCvu44910</a> | Cisco ASA Software and FTD Software Web Services Cross-Site Scripting Vulnerability            |
| <a href="#">CSCvu46685</a> | Cisco ASA and FTD Software SSL/TLS Session Denial of Service Vulnerability                     |
| <a href="#">CSCvu47925</a> | Cisco ASA and FTD IP Fragment Memory Leak Vulnerability                                        |
| <a href="#">CSCvu48285</a> | ASA configured with TACACS REST API: /cli api fail with "Command authorization failed" message |
| <a href="#">CSCvu53258</a> | FMC pushes certificate map incorrectly to lina                                                 |
| <a href="#">CSCvu57834</a> | syslog-ng process utilizing 100% CPU                                                           |
| <a href="#">CSCvu59817</a> | Cisco ASA and FTD Software SSL VPN Direct Memory Access Denial of Service Vulnerability        |
| <a href="#">CSCvu60923</a> | Editing the IP in a Radius Server Group object results in unintended values for the IP address |
| <a href="#">CSCvu63458</a> | FPR2100: Show crash output on show tech does not display outputs from most recent tracebacks   |
| <a href="#">CSCvu66119</a> | URL rules are incorrectly promoted on series 3 resulting in traffic matching the wrong rule.   |
| <a href="#">CSCvu70529</a> | Binary rules (SO rules) are not loaded when snort reloads                                      |
| <a href="#">CSCvu72658</a> | AnyConnect Connected Client IPs Not Advertised into OSPF Intermittently                        |
| <a href="#">CSCvu75581</a> | Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities                  |
| <a href="#">CSCvu75594</a> | FTD: Traceback and reload when changing capture buffer options on a already applied capture    |
| <a href="#">CSCvu75615</a> | Cisco ASA Software and FTD Software WebVPN Portal Access Rule Bypass Vulnerability             |
| <a href="#">CSCvu80370</a> | Cisco Firepower Threat Defense Software SNMP Denial of Service Vulnerability                   |
| <a href="#">CSCvu82743</a> | Encoded Rule Plugin SID: value, GID: 3 not registered properly. Disabling this rule            |
| <a href="#">CSCvu83178</a> | Dynamic routing protocols summary route not being replicated to standby                        |
| <a href="#">CSCvu83309</a> | Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities                  |
| <a href="#">CSCvu91105</a> | High unmanaged disk usage on /ngfw due to large process_stdout.log file                        |
| <a href="#">CSCvu98197</a> | HTTPS connections matching 'Do not decrypt' SSL decryption rule may be blocked                 |
| <a href="#">CSCvv09944</a> | Lina Traceback during FTD deployment when WCCP config is being pushed                          |
| <a href="#">CSCvv13835</a> | Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities                  |

| Bug ID                     | Headline                                                                                        |
|----------------------------|-------------------------------------------------------------------------------------------------|
| <a href="#">CSCvv13993</a> | Cisco Firepower 1000 Series Bleichenbacher Attack Vulnerability                                 |
| <a href="#">CSCvv16245</a> | Cisco Firepower Management Center Software Common Access Card Authentication Bypass Vuln        |
| <a href="#">CSCvv33712</a> | Cisco ASA Software Web-Based Management Interface Reflected Cross-Site Scripting Vulnerabi      |
| <a href="#">CSCvv40916</a> | 3 min delay caused by AbstractBaseDeploymentValidationHandler.validatePreApply during deploy.   |
| <a href="#">CSCvv44051</a> | Cluster unit traceback on snp_cluster_forward_and_free_packet due to GRE/IPiniP passenger flows |
| <a href="#">CSCvv50107</a> | FTD Traceback and reload while trying to switch peer on HA                                      |
| <a href="#">CSCvv52591</a> | DMA memory leak in ctm_hw_malloc_from_pool causing management and VPN connections to fail       |
| <a href="#">CSCvv58604</a> | Reset not sent when traffic matches AC-policy configured with block/reset and SSL inspection    |
| <a href="#">CSCvv70096</a> | Snort 2: Memory Leak in SSL Decrypt & Resign Processing                                         |
| <a href="#">CSCvv77910</a> | FQDN rules do not work on 1k platforms                                                          |
| <a href="#">CSCvv98534</a> | Failed upgrade does not create audit messages in syslog                                         |
| <a href="#">CSCvw48033</a> | 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 59: Resolved Bugs in Version 6.4.0.9**

| Bug ID                     | Headline                                                                             |
|----------------------------|--------------------------------------------------------------------------------------|
| <a href="#">CSCvi34123</a> | ENHancement: Cannot add DNS lists that contain _ at the beginning of the list.       |
| <a href="#">CSCvj00997</a> | "show open-network-ports" not showing the proper infomration on FP4100 Series        |
| <a href="#">CSCvm77115</a> | Lina Traceback due to invalid TSC values                                             |
| <a href="#">CSCvo31790</a> | Cisco Firepower Threat Defense Software Management Interface DoS Vulnerability       |
| <a href="#">CSCvo76866</a> | Traceback on 2100 - watchdog                                                         |
| <a href="#">CSCvo80853</a> | Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability |

| Bug ID                     | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvp57643</a> | FTD/ASA - Cluster/HA - Master/Active unit does not update all the route changes to Slaves/Standby  |
| <a href="#">CSCvp63814</a> | FTD - Inner Flow: Carrier id flow lookup enhancement                                               |
| <a href="#">CSCvp90847</a> | Refresh Root CAs that SSL uses for resigning in FTD/FMC                                            |
| <a href="#">CSCvp93468</a> | Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability                  |
| <a href="#">CSCvp99930</a> | deployment failure with sftunnel exception while primary active.                                   |
| <a href="#">CSCvq09357</a> | Unrestricted File Upload in FMC -Backup Management - Upload Backup                                 |
| <a href="#">CSCvq10500</a> | captures of both CLISH and LINA doesn't work with IPv6 address                                     |
| <a href="#">CSCvq24258</a> | Increase number of worker for mojo-server on large appliances                                      |
| <a href="#">CSCvq35440</a> | Upgrade Enhancements to STRAP verification for anyconnect - Cisco VPN session replay vulnerability |
| <a href="#">CSCvq38889</a> | slib memory manager : mempool mutex vs spinlock selection                                          |
| <a href="#">CSCvq39344</a> | Firepower managed devices may stop responding to SNMPv3 GET/WALK requests                          |
| <a href="#">CSCvq61601</a> | OpenSSL vulnerability CVE-2019-1559 on FTD                                                         |
| <a href="#">CSCvq71351</a> | FMC:Page stuck when editing inline sets                                                            |
| <a href="#">CSCvq79913</a> | ICMP error packets being dropped for Null pds_info                                                 |
| <a href="#">CSCvq89361</a> | Cisco Firepower 1000 Series SSL/TLS Denial of Service Vulnerability                                |
| <a href="#">CSCvq89794</a> | FDM - user downloads not working with LDAPS                                                        |
| <a href="#">CSCvq93572</a> | Unable to add user on FTD using external authentication                                            |
| <a href="#">CSCvq93669</a> | Cisco Firepower Threat Defense Software SSL/TLS URL Category Bypass Vulnerability                  |
| <a href="#">CSCvq96495</a> | Console connection for FPR2100 is disconnected randomly about 20 minutes.                          |
| <a href="#">CSCvr07460</a> | ASA traceback and reload related to crypto PKI operation                                           |
| <a href="#">CSCvr09468</a> | ASA traceback and reload for the CLI "Show nat pool"                                               |
| <a href="#">CSCvr13278</a> | PPPoE session not coming up after reload.                                                          |
| <a href="#">CSCvr17735</a> | SFDataCorrelator high CPU during SI update                                                         |
| <a href="#">CSCvr19922</a> | Cluster: BGP route may go in out of sync in some scenarios                                         |
| <a href="#">CSCvr20449</a> | Policy deployment is reported as successful on the FMC but it is actually failed                   |
| <a href="#">CSCvr20893</a> | FTD in HA pair crashes in ids_event_proce process after policy deployment                          |

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvr21803</a> | Mac address flap on switch with wrong packet injected on ingress FTD interface                       |
| <a href="#">CSCvr30694</a> | FMC : FMC detect HA Sync Failed                                                                      |
| <a href="#">CSCvr33586</a> | FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded                              |
| <a href="#">CSCvr35125</a> | Packet loss over failover link triggers Split-Brain                                                  |
| <a href="#">CSCvr39556</a> | Segfault in libclamav.so (in the context of SFDataCorrelator)                                        |
| <a href="#">CSCvr42344</a> | Traceback on snp_policy_based_route_lookup when deleting a rule from access-list configured for PBR  |
| <a href="#">CSCvr49833</a> | Cisco Firepower 2100 Series Security Appliances ARP Denial of Service Vulnerability                  |
| <a href="#">CSCvr51998</a> | ASA Static route disappearing from asp table after learning default route via BGP                    |
| <a href="#">CSCvr54250</a> | Many user_ip_map files even though no realm is configured                                            |
| <a href="#">CSCvr54980</a> | FPR2100: Power doesn't turn off after turned off the power button on back of chassis                 |
| <a href="#">CSCvr56031</a> | FTD/LINA Traceback and reload observed in thread name: cli_xml_server                                |
| <a href="#">CSCvr72665</a> | FMC upgrading to 6.3/6.4 shouldn't remove existing deprecated flexconfig                             |
| <a href="#">CSCvr73115</a> | Initial FTD Deploy After Policy Import causes Unused Objects which bloat policy size                 |
| <a href="#">CSCvr78166</a> | Deployment failed on FTD with reason "failed to retrieve running configuration"                      |
| <a href="#">CSCvr79008</a> | Session processing delay from FMC wastefully querying all Directory Servers normalizing bad username |
| <a href="#">CSCvr86213</a> | CD is required to ignore Cluster-Msg-Delivery-Confirmation in Cluster Node Release Lina State        |
| <a href="#">CSCvr90768</a> | FTD: Deployment through slow links may fail                                                          |
| <a href="#">CSCvr90965</a> | FTDv Deployment in Azure causes unrecoverable traceback state due to no dns domain-lookup any"       |
| <a href="#">CSCvr92168</a> | Cisco ASA and Cisco FTD Software OSPF Packets Processing Memory Leak Vulnerability                   |
| <a href="#">CSCvr92327</a> | ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'                                       |
| <a href="#">CSCvr92617</a> | NPE in SecurityIntelligenceEoConvertor causes Lucene indexing failure                                |
| <a href="#">CSCvr93978</a> | ASA traceback and reload on Thread DATAPATH-0-2064                                                   |
| <a href="#">CSCvr96527</a> | FMC existing rule error while adding new rule                                                        |
| <a href="#">CSCvs00023</a> | port manager crashes with "shutdown" command from clish CLI                                          |

| Bug ID                     | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvs01422</a> | Lina traceback when changing device mode of FTD                                                     |
| <a href="#">CSCvs03023</a> | Clustering module needs to skip the hardware clock update to avoid the timeout error and clock jump |
| <a href="#">CSCvs04067</a> | Not able to access FMC devices with Chrome on Mac after upgrade to Catalina.                        |
| <a href="#">CSCvs06043</a> | TunnelClient for CSM_CCMservice on ngfwManager not reading ACK sent from CSM_CCM service on FMC     |
| <a href="#">CSCvs07668</a> | FTD traceback and reload on thread DATAPATH-1-15076 when SIP inspection is enabled                  |
| <a href="#">CSCvs07982</a> | ASA TRACEBACK: sctpProcessNextSegment - SCTP_INIT_CHUNK                                             |
| <a href="#">CSCvs10443</a> | 6.5 CloudEvent code writes config files in a way that 6.4 code does not understand                  |
| <a href="#">CSCvs10526</a> | Throttle SSE Attempts on FTDs                                                                       |
| <a href="#">CSCvs12288</a> | Snort unexpectedly exits with SSL policy enabled and debug_policy_all                               |
| <a href="#">CSCvs15276</a> | ERROR: entry for ::/0 exists when configuring ipv6 icmp                                             |
| <a href="#">CSCvs15972</a> | Network Performance Degradation when SSL policy is enabled                                          |
| <a href="#">CSCvs19968</a> | Fix consoled from getting stuck and causing HA FTD policy deployment errors.                        |
| <a href="#">CSCvs22503</a> | eStreamer repeatedly exits after "Failed to deserialize policy event"                               |
| <a href="#">CSCvs23750</a> | 6.4.0.4 FMC WebUI cannot create a Series-3 stack (Cannot select primary device)                     |
| <a href="#">CSCvs25607</a> | addition of netmap_num to constraints causes performance degradation                                |
| <a href="#">CSCvs28094</a> | Receiving error 403 when editing User Preferences on FP8000 sensors                                 |
| <a href="#">CSCvs28580</a> | Traceback when processing SSL traffic under heavy load                                              |
| <a href="#">CSCvs29405</a> | Snort handles traffic as Tagged, when CMD field does not exist in Frame                             |
| <a href="#">CSCvs32303</a> | SNMP polling fails on Standby FMC as the snmpd process is in Waiting state                          |
| <a href="#">CSCvs33416</a> | Upgrade kernel to cpe:2.3:o:linux:linux_kernel:4.14.158:                                            |
| <a href="#">CSCvs34844</a> | pm process becomes randomly deadlocked when communicating with hardware.                            |
| <a href="#">CSCvs34854</a> | FMC generates referred interfaces cli delta after access-list cli delta                             |
| <a href="#">CSCvs37013</a> | Prevent octeon_init from getting stuck and causing HA FTD policy deployment errors.                 |
| <a href="#">CSCvs39388</a> | FTD not sending system syslog messages in CC mode                                                   |
| <a href="#">CSCvs40531</a> | AnyConnect 4.8 is not working on the FPR1000 series                                                 |
| <a href="#">CSCvs45111</a> | WR6 and WR8 commit id update in CCM layer(sprint 75)                                                |

| Bug ID                     | Headline                                                                                       |
|----------------------------|------------------------------------------------------------------------------------------------|
| <a href="#">CSCvs47201</a> | GET ALL for devicerecords we get "isPartOfContainer": false for devices part of HA and cluster |
| <a href="#">CSCvs47252</a> | ASA traceback and reload when running command "clear capture /"                                |
| <a href="#">CSCvs50459</a> | Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability      |
| <a href="#">CSCvs50952</a> | Upgrade of 6.4.0.4-34 to 6.4.0.6 is deleting Static Route                                      |
| <a href="#">CSCvs59056</a> | ASA/FTD Tunneled Static Routes are Ignored by Suboptimal Lookup if Float-Conn is Enabled       |
| <a href="#">CSCvs61392</a> | On firepower devices, hardware rules are not updated after successful policy deployment        |
| <a href="#">CSCvs79023</a> | ASA/FTD Traceback in Thread Name: DATAPATH due to DNS inspection                               |
| <a href="#">CSCvs80157</a> | ASA Traceback Thread Name: IKE Daemon                                                          |
| <a href="#">CSCvs80536</a> | FP41xx incorrect interface applied in ASA capture                                              |
| <a href="#">CSCvs91389</a> | FTD Traceback Lina process                                                                     |
| <a href="#">CSCvs91869</a> | FPR-1000 Series Random Number Generation Error                                                 |
| <a href="#">CSCvs98634</a> | catalina.<date>.log files can consume all disk space in their partition                        |
| <a href="#">CSCvt01397</a> | Deployment is marked as success although LINA config was not pushed                            |
| <a href="#">CSCvt10097</a> | logs about SF_Egress_Zone/SF_Ingress_Zone is empty even though security zones have interfaces  |
| <a href="#">CSCvt15163</a> | Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability                   |
| <a href="#">CSCvt21041</a> | FTD Traceback in thread 'ctm_ipsec_display_msg'                                                |
| <a href="#">CSCvt33785</a> | IPSec SAs are not being created for random VPN peers                                           |
| <a href="#">CSCvt46830</a> | FPR2100 'show crypto accelerator statistics' counters do not track symmetric crypto            |
| <a href="#">CSCvt79988</a> | Policy deployment failure due to snmp configuration after upgrading FMC to 6.6                 |
| <a href="#">CSCvt93177</a> | 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 60: Resolved Bugs in Version 6.4.0.8*

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

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

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

## Resolved Bugs in Version 6.4.0.7

Table last updated: 2020-02-20

**Table 61: Resolved Bugs in Version 6.4.0.7**

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

| Bug ID                     | Headline                                |
|----------------------------|-----------------------------------------|
| <a href="#">CSCvs32023</a> | 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 62: Resolved Bugs in Version 6.4.0.6**

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

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

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvq70775</a> | FPR2100 FTD Standby unit leaking 9K blocks                                                           |
| <a href="#">CSCvq71217</a> | High Disk Utilization due to mysql-server.err failing to rotate after CSCvn30118                     |
| <a href="#">CSCvq75743</a> | ASA:BGP recursive route lookup for destination 3 hop away is failing.                                |
| <a href="#">CSCvq76533</a> | F_RNA_EVENT_LIMIT for MC4000 should be 20 million                                                    |
| <a href="#">CSCvq77547</a> | Connections fail to replicate in failover due to failover descriptor mis-match on port-channels      |
| <a href="#">CSCvq80318</a> | ASA generates incorrect error message about PCI cfg space when enumerating Internal-Data0/1          |
| <a href="#">CSCvq81516</a> | VPN events between 12 and 1 PM UTC are not displayed on the FMC                                      |
| <a href="#">CSCvq83168</a> | DNS lookup using mgmt VRF not possible because FMC doesn't allow interface after server address      |
| <a href="#">CSCvq87703</a> | Active device is not reporting correct peer state.                                                   |
| <a href="#">CSCvq91645</a> | Flow Offload Hashing Change of Behavior                                                              |
| <a href="#">CSCvq92126</a> | ASA traceback in Thread IPsec Message Handler                                                        |
| <a href="#">CSCvq94729</a> | Deployment rollback causes momentary traffic drop when error in a LINA ONLY section of delta cli     |
| <a href="#">CSCvr00892</a> | where clause not working for external data base access                                               |
| <a href="#">CSCvr07421</a> | 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 63: Resolved Bugs in Version 6.4.0.5**

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

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCVq32681</a> | Fail to Wire configuration disabled for multiple interface-pair inline-sets during FTD upgrades      |
| <a href="#">CSCVq39083</a> | Security Intelligence does not drop HTTPS connections to blacklisted URLs when SSL policy is enabled |
| <a href="#">CSCVq41936</a> | Must disable and then re-enable SNMP in FMC UI after adding new user                                 |
| <a href="#">CSCVq44594</a> | Flooding of logs with message "Unknown HPQ rule key"                                                 |
| <a href="#">CSCVq46804</a> | Unable to login with AD username containing upper case RADIUS                                        |
| <a href="#">CSCVq46918</a> | SNMPv3 User(s) deleted after upgrade                                                                 |
| <a href="#">CSCVq54242</a> | Warning "There is an empty group in the source networks" in SSL policy                               |
| <a href="#">CSCVq56138</a> | User login fails into FMC GUI for LDAP user if the password contains SPACE in the string             |
| <a href="#">CSCVq56462</a> | File policy not inspecting some malware document (.doc) and Adobe flash (.swf) files.                |
| <a href="#">CSCVq65092</a> | Slow device related REST API calls                                                                   |
| <a href="#">CSCVq66217</a> | FMT   MTU value not within the permissible range                                                     |
| <a href="#">CSCvr23858</a> | 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 64: Resolved Bugs in Version 6.4.0.4**

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

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

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

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

| Bug ID                     | Headline                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvq25912</a> | Correlation rule alerting is not working in 6.4.0                                                    |
| <a href="#">CSCvq26794</a> | GTP response messages with non existent cause are getting dropped with error message TID is 0        |
| <a href="#">CSCvq27010</a> | Memory leak observed when ASA-SFR dataplane communication flaps                                      |
| <a href="#">CSCvq37902</a> | TID fails to add source as a URL - Flat file                                                         |
| <a href="#">CSCvq39828</a> | SFDC crashes inserting into packet_log table after upgrading to 6.4.0                                |
| <a href="#">CSCvq50314</a> | Failed SSH Login attempts not being exported via syslog                                              |
| <a href="#">CSCvq57710</a> | Firepower Primary Detection Engine process might terminated after Manager upgrade                    |
| <a href="#">CSCvq61651</a> | URL DB download failure alerts on FMC; new URL DB updates not taking effect on FMC/FDM               |
| <a href="#">CSCvq86553</a> | Traffic not matching expected ACP rule after updating to 6.4.0                                       |
| <a href="#">CSCvq97301</a> | 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 65: Resolved Bugs in Version 6.4.0.3**

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

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

## Version 6.4.0.2 Resolved Issues

Table last updated: 2020-04-16

**Table 66: Version 6.4.0.2 Resolved Issues**

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

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

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

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

## Resolved Bugs in Version 6.4.0.1

Table last updated: 2019-05-15

**Table 67: Resolved Bugs in Version 6.4.0.1**

| Bug ID                     | Headline                                                                                       |
|----------------------------|------------------------------------------------------------------------------------------------|
| <a href="#">CSCvh51853</a> | Random packet drops by session preprocessor                                                    |
| <a href="#">CSCvp59960</a> | 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 68: Resolved Bugs in Version 6.4.0**

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

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

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

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

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

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