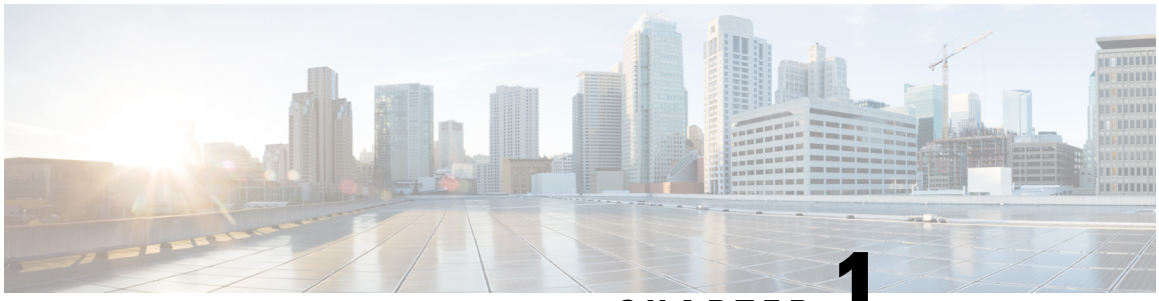
Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes

First Published: 2017-09-21

Last Modified: 2022-08-10

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

CONTENTS



CHAPTER 1

About Hotfixes

Hotfixes are minor updates that address particular, urgent issues.

Downloading Hotfixes

Download hotfixes from the Cisco Support & Download site: https://software.cisco.com/download/home.

To find a hotfix, select or search for your model, then browse to the software download page for your current version. Available hotfixes are listed along with upgrade and installation packages. If you cannot find a hotfix on the download page for your patch level—especially if that same hotfix applies to other patches—look on other download pages where the hotfix applies, especially the first version and the last version.

You use the same hotfix package for all models in a family or series. Most hotfix packages use the following naming scheme:

- *Platform*_Hotfix_*letter-version-build*.sh.REL.tar (Version 6.2.2+)
- *Platform*_Hotfix_*letter-version-build*.sh (Version 5.4 through 6.2.0)

Do not untar signed (.tar) packages.

Tip In management center and ASDM deployments where your appliance has internet access, you can easily obtain hotfixes directly from Cisco. On the management center, select **System** > **Updates**, then click **Download Updates**. With ASDM, select **Configuration** > **ASA FirePOWER Configuration** > **Updates**, then click **Download Updates**.

Installing Hotfixes

You install hotfixes the same way you install patches. For instructions, see one of the following guides.

Note For CDO + device manager deployments, use device manager to install threat defense hotfixes. You cannot use CDO.

Management Center

Table 1: Instructions for Management Center

Version	Guide
7.2+	Under Upgrade Guides, the *Upgrade the Management Center* chapter in the *Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center* for your version.
7.1	Upgrade the FMC in the *Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1*
7.0 or earlier	Upgrade Firepower Management Centers in the *Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*

Threat Defense

Table 2: Instructions for Threat Defense with Management Center

Version	Guide
7.2+	Under Upgrade Guides, the *Upgrade Threat Defense* chapter in the *Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center* for your version.
7.1	Upgrade FTD in the *Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1*
7.0 or earlier	Upgrade Firepower Threat Defense in the *Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*

Table 3: Instructions for Threat Defense with Device Manager

Version	Guide
7.2+	Under Upgrade Guides, the *Upgrade Threat Defense* chapter in the *Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager* for your version.
7.1	Upgrade FTD in the *Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1*

Version	Guide
7.0	System Management in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 7.0*
6.7	System Management in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.7*
6.6	System Management in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.6*
6.5	System Management in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.5*
6.4	System Management in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4*
6.3	System Management in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.3*
6.2.3	System Management in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.2.3*
6.2.2	System Management in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.2.2*
6.2	System Management in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.2*
6.1	System Management in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.1*

NGIPS

Table 4: Instructions for NGIPS Devices

Version	Platform	Guide
Any	Firepower 7000/8000 series	Upgrade Firepower 7000/8000 Series and NGIPSv in the *Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*
Any	ASA FirePOWER with FMC	Upgrade ASA with FirePOWER Services in the *Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*
Any	ASA FirePOWER with ASDM	Upgrade the ASA FIrePOWER Module in the *Cisco ASA Upgrade Guide*

Verifying Hotfix Success

Applying a hotfix does not update the software version or build. To verify that a hotfix installed successfully, access the Linux shell (also called expert mode) and run the following command:

```
cat /etc/sf/patch_history
```

The system lists all successful upgrades, patches, hotfixes, and pre-install packages since the software was first installed.

Unresponsive or Unsuccessful Hotfixes

Do not make or deploy configuration changes while you are installing a hotfix. Even if the system appears inactive, do not manually reboot, shut down, or restart a hotfix in progress. You could place the system in an unusable state and require a reimage. Do not install the same hotfix more than once on a single appliance. If you encounter issues with a hotfix, including a failed hotfix or unresponsive appliance, contact Cisco TAC.

Uninstalling Hotfixes

Do not attempt to uninstall a hotfix. Instead, contact Cisco TAC.

Traffic Flow and Inspection

Device hotfixes can affect traffic flow and inspection, especially if the hotfix reboots the device, or if you need to deploy configuration changes.

Device type, deployment type (standalone, high availability, clustered), and interface configurations determine the nature of the interruptions. We *strongly* recommend installing hotfixes in a maintenance window or at a time when any interruption will have the least impact on your deployment.

For specifics on traffic flow and inspection, see the Cisco Secure Firewall Threat Defense Release Notes for your version.

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.

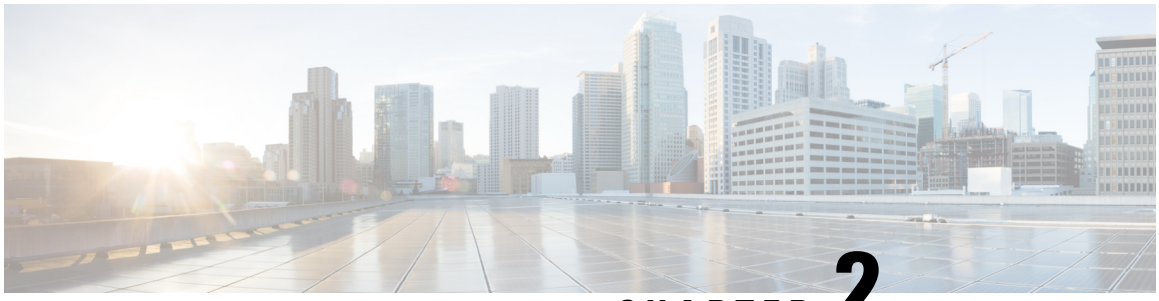
- Documentation: http://www.cisco.com/go/ftd-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

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

Available Hotfixes

These release notes provide quicklinks to download pages for publicly available hotfixes.

Note Some quicklinks may not go to the download page for your *specific* model. However, as long as the appliance is in the same family or series, you can safely download and apply the hotfix. If you want to be absolutely sure, browse to the page for your specific model.

BIOS and Firmware Hotfixes for Management Center Hardware

We provide updates for BIOS and RAID controller firmware on management center hardware. If your management center does not meet the requirements, apply the appropriate hotfix. If your management center model and version are not listed and you think you need to update, contact Cisco TAC.

Table 5: BIOS and Firmware Minimum Requirements

Platform	Version	BIOS	RAID Controller Firmware	CIMC Firmware	Hotfix
FMC 1600, 2600, 4600	6.3.0 to 7.0	C220M5.4.1.3i.0	51.10.0-3612	4.1(3d)	BIOS Update Hotfix EL
FMC 1000, 2500, 4500	6.2.3 to 7.0	C220M4.4.1.2c.0	24.12.1-0456	4.1(2g)	BIOS Update Hotfix EL
FMC 2000, 4000	6.2.3 to 6.6	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS Update Hotfix EI
FMC 750, 1500, 3500	6.2.3 to 6.4	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS Update Hotfix EI

Hotfixing is the only way to update the BIOS and RAID controller firmware. Upgrading the software does not accomplish this task, nor does reimaging to a later version. If the management center is already up to date, the hotfix has no effect.

Tip These hotfixes also update the CIMC firmware; for resolved issues see Release Notes for Cisco UCS Rack Server Software. Note that in general, we do not support changing configurations on the management center using CIMC. However, to enable logging of invalid CIMC usernames, apply the latest hotfix, then follow the instructions in the *Viewing Faults and Logs* chapter in the Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Version 4.0 or later.

For quicklinks to the Cisco Support & Download site, see the tables below.

Note The management center web interface may display these hotfixes with a version that is different from (usually later than) the current software version. This is expected behavior and the hotfixes are safe to apply.

Determining BIOS and Firmware Versions

To determine the current versions on the management center, run these commands from the Linux shell/expert mode:

- BIOS: **sudo dmidecode -t bios -q**
- RAID controller firmware (FMC 4500): **sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"**
- RAID controller firmware (all other models): **sudo storcli /c0 show | grep "FW Package"**

Version 7.1.x Hotfixes

This table provides quicklinks to download pages for publicly available Version 7.1.x hotfixes.

Table 6: Version 7.1.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix Q	7.1.0.2	Secure Firewall 3100 series: Cisco_FTD_SSP_FP3K_Hotfix_Q-7.1.0.3-2	CSCwb88651: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability CSCwc28334: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
Hotfix P	7.1.0.1	Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_P-7.1.0.2-2 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_P-7.1.0.2-2 Firepower 4100/9300 Cisco_FTD_SSP_Hotfix_Hotfix_P-7.1.0.2-2 ISA 3000: Cisco_FTD_Hotfix_Hotfix_P-7.1.0.2-2 FTDv: Cisco_FTD_Hotfix_Hotfix_P-7.1.0.2-2	CSCwb88651: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability CSCwc28334: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
Hotfix A	7.1.0	Firepower 1000 series with FDM: Cisco_FTD_SSP_FP1K_Hotfix_A-7.1.0.1-7 Firepower 2100 series with FDM: Cisco_FTD_SSP_FP2K_Hotfix_A-7.1.0.1-7 Firepower 4100/9300 with FDM: Cisco_FTD_SSP_Hotfix_A-7.1.0.1-7 ISA 3000 with FDM: Cisco_FTD_Hotfix_A-7.1.0.1-7 FTDv with FDM: Cisco_FTD_Hotfix_A-7.1.0.1-7 **Note** Apply this hotfix to FDM and FDM/CDO-managed devices. FMC-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability

Version 7.0.x Hotfixes

This table provides quicklinks to download pages for publicly available Version 7.0.x hotfixes.

Table 7: Version 7.0.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix S	7.0.1	Firepower 1000 series with FDM: Cisco_FTD_SSP_FP1K_Hotfix_S-7.0.1.1-10 Firepower 2100 series with FDM: Cisco_FTD_SSP_FP2K_Hotfix_S-7.0.1.1-10 Firepower 4100/9300 with FDM: Cisco_FTD_SSP_Hotfix_S-7.0.1.1-10 ASA 5500-X series and ISA 3000 with FDM: Cisco_FTD_Hotfix_S-7.0.1.1-10 FTDv with FDM: Cisco_FTD_Hotfix_S-7.0.1.1-10 **Note** This hotfix was originally released as build 9 on 2021-12-19. It was rereleased as build 10 on 2021-12-21. If you installed the earlier build, you do *not* have to install the later build. Apply this hotfix to FDM and FDM/CDO-managed devices. FMC-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability CSCwa55039: Firepower Threat Defense Hotfix S for 7.0.1 cause system failing when ran twice
Hotfix EL	7.0.0 7.0.x 7.0.x.x	FMC (all hardware models): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EL-7 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.

Version 6.7.x Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.7.x hotfixes.

Table 8: Version 6.7.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix AA	6.7.0.3	Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_AA-6.7.0.4-2 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_AA-6.7.0.4-2 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_AA-6.7.0.4-2 ASA 5500-X series and ISA 3000: Cisco_FTD_Hotfix_AA-6.7.0.4-2 FTDv: Cisco_FTD_Hotfix_AA-6.7.0.4-2	

Hotfix	Versions	Platforms	Resolves
			CSCvw94160: CIAM: openssl CVE-2020-1971 CSCvx64478: Unwanted console output during SAML transactions CSCvz70595: Traceback observed on ASA while handling SAML handler CSCvz76966: Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DNS DoS CSCvz81480: IV in the outbound pkt is not updated on Nitrox V platforms when GCM is used for IPsec CSCvz84850: ASA/FTD traceback and reload caused by "timer services" function CSCvz85683: Wrong syslog message format for 414004 CSCvz85913: ASN.1 strings are represented internally within OpenSSL as an ASN1_STR for CISCO-SSL-1.0.2 CSCvz89545: SSL VPN performance degraded and significant stability issues after upgrade CSCvz92016: ASA Privilege Escalation with valid user in AD CSCwa04461: Cisco ASA Software and FTD Software Remote Access SSL VPN Denial of Service CSCwa14485: Cisco Firepower Threat Defense Software Denial of Service Vulnerability CSCwa15185: ASA/FTD: remove unwanted process call from LUA CSCwa33898: Cisco Adaptive Security Appliance Software Clientless SSL VPN Heap Overflow Vulnerability CSCwa36678: Random FTD reloads with the traceback during

Hotfix	Versions	Platforms	Resolves
			deployment from FMC CSCwa65389: ASA traceback and reload in Unicorn Admin Handler when change interface configuration via ASDM
Hotfix Y	6.7.0.2	Firepower 1000 series with FDM: Cisco_FTD_SSP_FP1K_Hotfix_Y-6.7.0.3-7 Firepower 2100 series with FDM: Cisco_FTD_SSP_FP2K_Hotfix_Y-6.7.0.3-7 Firepower 4100/9300 with FDM: Cisco_FTD_SSP_Hotfix_Y-6.7.0.3-7 ASA 5500-X series and ISA 3000 with FDM: Cisco_FTD_Hotfix_Y-6.7.0.3-7 FTDv with FDM: Cisco_FTD_Hotfix_Y-6.7.0.3-7 **Note** Apply this hotfix to FDM and FDM/CDO-managed devices. FMC-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability
Hotfix EL	6.7.0 6.7.x.x	FMC (all hardware models): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_670_EL-7 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.
Hotfix C	6.7.0 6.7.x.x	ISA 3000 with FTD: Cisco_FTD_Hotfix_C-6.7.0.999-2	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service

Version 6.6.x Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.6.x hotfixes.

Table 9: Version 6.6.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix DE	6.6.5 6.6.5.1	FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_DE-6.6.5.2-8 Firepower 1000 series with FDM: Cisco_FTD_SSP_FP1K_Hotfix_DE-6.6.5.2-8 Firepower 2100 series with FDM: Cisco_FTD_SSP_FP2K_Hotfix_DE-6.6.5.2-8 Firepower 4100/9300 with FDM: Cisco_FTD_SSP_Hotfix_DE-6.6.5.2-8 ASA 5500-X series and ISA 3000 with FDM: Cisco_FTD_Hotfix_DE-6.6.5.2-8 FTDv with FDM: Cisco_FTD_Hotfix_DE-6.6.5.2-8 ASA FirePOWER with ASDM: Cisco_Network_Sensor_Hotfix_DE-6.6.5.2-8 **Note** Apply this hotfix to the FMC and to FDM, FDM/CDO, and ASDM managed devices only. FMC-managed devices are covered by the FMC hotfix.	CSCwa70008: Expired certs cause Security Intel. and malware file preclassification signature updates to fail
Hotfix DA	6.6.5.1	Firepower 1000 series with FDM: Cisco_FTD_SSP_FP1K_Hotfix_DA-6.6.5.2-4 Firepower 2100 series with FDM Cisco_FTD_SSP_FP2K_Hotfix_DA-6.6.5.2-4 Firepower 4100/9300 with FDM: Cisco_FTD_SSP_Hotfix_DA-6.6.5.2-4 ASA 5500-X series and ISA 3000 with FDM: Cisco_FTD_Hotfix_DA-6.6.5.2-4 FTDv with FDM: Cisco_FTD_Hotfix_DA-6.6.5.2-4 **Note** Apply this hotfix to FDM and FDM/CDO-managed devices. FMC-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix EL	6.6.0 6.6.x 6.6.x.x	FMC 1000, 1600, 2500, 2600, 4500, 4600: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EL-7 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.
Hotfix EI	6.6.0 6.6.x 6.6.x.x	FMC 2000, 4000: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EI-15 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.
Hotfix AB	6.6.1	ISA 3000 with FTD: Cisco_FTD_Hotfix_AB-6.6.1.999-1	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
Hotfix N	6.6.0 6.6.0.x	ISA 3000 with FTD: Cisco_FTD_Hotfix_N-6.6.0.999-1	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service

Version 6.5.0 Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.5.0 hotfixes.

Table 10: Version 6.5.0 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EL	6.5.0 6.5.0.x	FMC 1000, 1600, 2500, 2600, 4500, 4600: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_650_EL-7 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.

Hotfix	Versions	Platforms	Resolves
Hotfix EI	6.5.0 6.5.0.x	FMC 2000, 4000: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_650_EI-15 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.
Hotfix T	6.5.0 6.5.0.x	ISA 3000 with FTD: Cisco_FTD_Hotfix_T-6.5.0.999-1	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
Hotfix O	6.5.0.4	Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_O-6.5.0.5-3 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_O-6.5.0.5-3 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_O-6.5.0.5-3 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_O-6.5.0.5-3 FTDv: Cisco_FTD_Hotfix_O-6.5.0.5-3	CSCvt03598: Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix H	6.5.0.4	Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_H-6.5.0.5-2 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_H-6.5.0.5-2 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_H-6.5.0.5-2 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_H-6.5.0.5-2 FTDv: Cisco_FTD_Hotfix_H-6.5.0.5-2	CSCvp93468: Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability CSCvr92168: ASA/FTD Slow memory leak in OSPF process when processing OSPF Hellos CSCvs10748: Cisco Adaptive Security Appliance and Firepower Threat Defense Denial of Service Vuln CSCvs50459: Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability CSCvt15163: Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability CSCvu20521: OSPF is not forming after HF installation
Hotfix D	6.5.0.2	Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_D-6.5.0.3-3 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_D-6.5.0.3-3 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_D-6.5.0.3-3 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_D-6.5.0.3-3 FTDv: Cisco_FTD_Hotfix_D-6.5.0.3-3	CSCvs55990: Deployment failure with SI DNS configured on FTD managed locally / FDM
Hotfix B	6.5.0 6.5.0.1 and 6.5.0.2	FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_B-6.5.0.3-3 **Note** You must also update to VDB 329+ and deploy configuration changes. You can do this before or after you apply the hotfix.	Resolves issues with application identification.
Hotfix C	6.5.0.1	FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_C-6.5.0.2-2	CSCvr52109: FTD has hitcounts on access-lists but traffic is not hitting Access Policy rules

Version 6.4.0 Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.4.0 hotfixes.

Table 11: Version 6.4.0 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EP	6.4.0.13	Firepower 1000 series with FDM: Cisco_FTD_SSP_FP1K_Hotfix_EP-6.4.0.14-9 Firepower 2100 series with FDM: Cisco_FTD_SSP_FP2K_Hotfix_EP-6.4.0.14-9 ASA 5500-X series and ISA 3000 with FDM: Cisco_FTD_Hotfix_EP-6.4.0.14-9 FTDv with FDM: Cisco_FTD_Hotfix_EP-6.4.0.14-9 **Note** Apply this hotfix to FDM and FDM/CDO-managed devices. FMC-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability
Hotfix EL	6.4.0 6.4.0.x	FMC 1000, 1600, 2500, 2600, 4500, 4600: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EL-7 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.
Hotfix EI	6.4.0 6.4.0.x	FMC 750, 1500, 2000, 3500, 4000: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EI-15 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.
Hotfix DV	6.4.0 6.4.0.x	ISA 3000 with FTD: Cisco_FTD_Hotfix_DV-6.4.0.999-1	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service

Hotfix	Versions	Platforms	Resolves
Hotfix BM	6.4.0.9	Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_BM-6.4.0.10-2 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_BM-6.4.0.10-2 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_BM-6.4.0.10-2 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_BM-6.4.0.10-2 FTDv: Cisco_FTD_Hotfix_BM-6.4.0.10-2	CSCvt03598: Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability
Hotfix AY	6.4.0.8	Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_AY-6.4.0.9-3 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_AY-6.4.0.9-3 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_AY-6.4.0.9-3 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_AY-6.4.0.9-3 FTDv: Cisco_FTD_Hotfix_AY-6.4.0.9-3 **Note** We recommend you patch to Version 6.4.0.9+ instead of applying this hotfix. If you cannot patch, note that this hotfix was originally released as build 2 on 2020-05-06, and was rereleased on 2020-05-15 as build 3. If you installed the earlier build, install the new one also. You do not have to uninstall.	CSCvp49481, CSCvp93468: Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability CSCvs10748: Cisco Adaptive Security Appliance and Firepower Threat Defense Denial of Service Vuln CSCvo80853: Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability CSCvs50459: Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability CSCvr86783: Standby FDM lost connectivity after forming HA CSCvr92168: ASA/FTD Slow memory leak in OSPF process when processing OSPF Hellos CSCvt15163: Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability CSCvq89361: Cisco Firepower 1000 Series SSL/TLS Denial of Service Vulnerability CSCvu20521: OSPF is not forming after HF installation

Hotfix	Versions	Platforms	Resolves
Hotfix U	6.4.0.5 and 6.4.0.6	FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_U-6.4.0.7-2	CSCvr95287: Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability
Hotfix T	6.4.0 6.4.0.1 to 6.4.0.4	FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_T-6.4.0.5-1	CSCvr95287: Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability
Hotfix AA	6.4.0.4 to 6.4.0.7	FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_AA-6.4.0.8-4 **Note** You must also update to VDB 329+ and deploy configuration changes. You can do this before or after you apply the hotfix.	Resolves issues with application identification.
Hotfix X	6.4.0.6	FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_X-6.4.0.7-2	CSCvr52109: FTD has hitcounts on access-lists but traffic is not hitting Access Policy rules
Hotfix F	6.4.0.2	FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_F-6.4.0.3-2 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_F-6.4.0.3-2 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_F-6.4.0.3-2 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_F-6.4.0.3-2 FTDv (VMware, FVM): Cisco_FTD_Hotfix_F-6.4.0.3-2	CSCvq34224: Firepower Primary Detection Engine process terminated after Manager upgrade

Version 6.3.0 Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.3.0 hotfixes.

Table 12: Version 6.3.0 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EL	6.3.0 6.3.0.x	FMC 1000, 1600, 2500, 2600, 4500, 4600: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_630_EL-7 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.
Hotfix EI	6.3.0 6.3.0.x	FMC 750, 1500, 2000, 3500, 4000: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_630_EI-15 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.
Hotfix AZ	6.3.0 6.3.0.x	ISA 3000 with FTD: Cisco_FTD_Hotfix_AZ-6.3.0.999-1	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
Hotfix AV	6.3.0.5	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_ AV-6.3.0.6-3 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_ AV-6.3.0.6-3 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_AV-6.3.0.6-3 FTDv: Cisco_FTD_Hotfix_AV-6.3.0.6-3	CSCvt03598: Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix AO	6.3.0.5	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_ AO-6.3.0.6-2 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_ AO-6.3.0.6-2 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_AO-6.3.0.6-2 FTDv: Cisco_FTD_Hotfix_AO-6.3.0.6-2	CSCvp93468: Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability CSCvo80853: Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability CSCvr07419 CSCvs50459: Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability CSCvs10748: Cisco Adaptive Security Appliance and Firepower Threat Defense Denial of Service Vuln CSCvp49481: Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability CSCvt15163: Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability CSCvr55825: Cisco ASA and FTD Software Path Traversal Vulnerability
Hotfix AI	6.3.0 6.3.0.1 to 6.3.0.5	FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_AI-6.3.0.6-2	CSCvr95287: Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability
Hotfix AK	6.3.0.5	FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_AK-6.3.0.6-2 **Note** You must also update to VDB 329+ and deploy configuration changes. You can do this before or after you apply the hotfix.	Resolves issues with application identification.
Hotfix AA	6.3.0.3	ASA 5508-X and ASA 5516-X with FTD: Cisco_FTD_Hotfix_AA-6.3.0.4-2	CSCvp36425: Cisco ASA & FTD Software Cryptographic TLS and SSL Driver Denial of Service Vulnerability
Hotfix W	6.3.0.3	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_W-6.3.0.4-4	CSCvn77248: Cisco Secure Boot Hardware Tampering Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix B	6.3.0	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_B-6.3.0.1-1 **Note** Do not apply this hotfix if you have configured multiple instances (multiple logical devices on one security module).	CSCvo02577: Buffer exhaustion with SSL HW decryption

Version 6.2.3 Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.2.3 hotfixes.

Table 13: Version 6.2.3 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EM	6.2.3.17	Firepower 2100 series with FDM: Cisco_FTD_SSP_FP2K_Hotfix_EM-6.2.3.18-13 ASA 5500-X series and ISA 3000 with FDM: Cisco_FTD_Hotfix_EM-6.2.3.18-13 FTDv with FDM: Cisco_FTD_Hotfix_EM-6.2.3.18-13 **Note** Apply this hotfix to FDM and FDM/CDO-managed devices. FMC-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability
Hotfix EL	6.2.3 6.2.3.x	FMC 1000, 2500, 4500: Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EL-7 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.
Hotfix EI	6.2.3 6.2.3.x	FMC 750, 1500, 2000, 3500, 4000: Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EI-15 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these management center models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for Management Center Hardware, on page 7.

Hotfix	Versions	Platforms	Resolves
Hotfix EH	6.2.3 6.2.3.x	ASA 5506-X series with FTD: Cisco_FTD_Hotfix_EH-6.2.3.999-6	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
Hotfix DT	6.2.3.15	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_DT-6.2.3.16-3 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_DT-6.2.3.16-3 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_DT-6.2.3.16-3 FTDv: Cisco_FTD_Hotfix_DT-6.2.3.16-3	CSCvr55825: Cisco ASA and FTD Software Path Traversal Vulnerability CSCvp49481, CSCvp93468: Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability CSCvp16945, CSCvp16949: Cisco ASA Software and FTD Software MGCP Denial of Service Vulnerabilities CSCvo62077: Cisco Firepower Threat Defense Software VPN System Logging Denial of Service Vulnerability CSCvs10748: Cisco Adaptive Security Appliance and Firepower Threat Defense Denial of Service Vuln CSCvs50459: Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability CSCvo80853: Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability CSCvr07419: Cisco ASA and FTD Software IPv6 DNS Denial of Service Vulnerability CSCvt15163: Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix DW	6.2.3.15	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_DW-6.2.3.16-6 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_DW-6.2.3.16-6 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_DW-6.2.3.16-6 FTDv: Cisco_FTD_Hotfix_DW-6.2.3.16-6	CSCvs84578: Upgrading FTD on 4100/9300 Platform to 6.2.3.15 break SSHD, preventing FTD instance from booting up CSCvs84713: Cannot SSH to the device after upgrading FTD on ASA55XX/ISA 3000/FTDv to 6.2.3.15 build 38 CSCvs95725: Virtual FTD Running on 6.2.3.15 blocks SSH request and loses connection with the FMC
Hotfix DO	6.2.3 6.2.3.1 to 6.2.3.15	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_DO-6.2.3.16-3	CSCvr95287: Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability
Hotfix DQ	6.2.3.15	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_DQ-6.2.3.16-2 **Note** You must also update to VDB 329+ and deploy configuration changes. You can do this before or after you apply the hotfix.	Resolves issues with application identification.
Hotfix CY	6.2.3.14	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_CY-6.2.3.15-2	CSCvq34224: Firepower Primary Detection Engine process terminated after Manager upgrade
Hotfix CK	6.2.3.12	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_CK-6.2.3.13-1	CSCvn77248: Cisco Secure Boot Hardware Tampering Vulnerability
Hotfix Local Malware Cert	6.2.3 6.2.3.x	FMC/FMCv: Hotfix_Local_Malware_Cert-6.2.3.999-4	CSCvm81052: local malware detection updates not downloading to FMC due to invalid certificate chain.
Hotfix H	6.2.3 6.2.3.1 to 6.2.3.3	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_H-6.2.3.999-5 Firepower 7000/8000 series: Sourcefire_3D_Device_S3_Hotfix_H-6.2.3.999-5 ASA FirePOWER: Cisco_Network_Sensor_Hotfix_H-6.2.3.999-5 NGIPSv: Sourcefire_3D_Device_VMware_Hotfix_H-6.2.3.999-5	CSCvj07038: Firepower devices need to trust Threat Grid certificate.

Hotfix	Versions	Platforms	Resolves
Hotfix G	6.2.3 6.2.3.1 to 6.2.3.3	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_G-6.2.3.999-6 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_G-6.2.3.999-6 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_G-6.2.3.999-6 FTDv (VMware, KVM, AWS): Cisco_FTD_Hotfix_G-6.2.3.999-6	CSCvj07038: Firepower devices need to trust Threat Grid certificate.
Hotfix T	6.2.3.1 to 6.2.3.3	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_T-6.2.3.4-4	CSCvk06176: SSEConnector is not coming up because of Wrong Executable.
Hotfix A	6.2.3	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_A-6.2.3.1-10 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_A-6.2.3.1-10 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_A-6.2.3.1-10 FTDv (VMware, KVM, AWS): Cisco_FTD_Hotfix_A-6.2.3.1-10	CSCvg65072: ASA, Threat Defense, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability. CSCvi16029: ASA Web Interface Authentication Bypass.

Version 6.2.2 Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.2.2 hotfixes.

Table 14: Version 6.2.2 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix CB	6.2.2.5	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_CB-6.2.2.6-2	CSCvn77248: Cisco Secure Boot Hardware Tampering Vulnerability
Hotfix BY	6.2.2 6.2.2.x	FMC (all hardware models): Sourcefire_3D_Defense_Center_S3_Hotfix_BY-6.2.2.999-1	Updates the RAID controller firmware.

Hotfix	Versions	Platforms	Resolves
Hotfix Local Malware Cert	6.2.2 6.2.2.x	FMC/FMCv: Hotfix_Local_Malware_Cert-6.2.2.999-4 **Note** After you upgrade to Version 6.2.3, you must apply a new Local Malware Cert hotfix.	CSCvm81052: local malware detection updates not downloading to FMC due to invalid certificate chain.
Hotfix BZ	6.2.2.4	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_BZ-6.2.2.5-4 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_BZ-6.2.2.5-4 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_BZ-6.2.2.5-4 FTDv (VMware, KVM, AWS): Cisco_FTD_Hotfix_BZ-6.2.2.5-4	CSCvm43975: Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability.
Hotfix BN	6.2.2 6.2.2.1 to 6.2.2.4	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_BN-6.2.2.999-5 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_BN-6.2.2.999-5 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_BN-6.2.2.999-5 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_BN-6.2.2.999-5 FTDv (VMware, KVM, AWS): Cisco_FTD_Hotfix_BN-6.2.2.999-5 Firepower 7000/8000 series: Sourcefire_3D_Device_S3_Hotfix_BN-6.2.2.999-5 ASA FirePOWER: Cisco_Network_Sensor_Hotfix_BN-6.2.2.999-5 NGIPSv: Sourcefire_3D_Device_VMware_Hotfix_BN-6.2.2.999-5	CSCvj07038: Firepower devices need to trust Threat Grid certificate.
Hotfix BS	6.2.2.4	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_BS-6.2.2.5-3	CSCvk17382: Snort exiting unexpectedly while processing rule evaluation.

Hotfix	Versions	Platforms	Resolves
Hotfix BD	6.2.2.2	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_BD-6.2.2.3-4 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_BD-6.2.2.3-4 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_BD-6.2.2.3-4 FTDv (VMware, KVM, AWS): Cisco_FTD_Hotfix_BD-6.2.2.3-4	CSCvi16029, CSCvg65072: ASA, Threat Defense, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability. CSCvi16029: ASA Web Interface Authentication Bypass.
Hotfix AO	6.2.2.1	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_AO-6.2.2.2-1 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_AO-6.2.2.2-1 FTDv: Cisco_FTD_Hotfix_AO-6.2.2.2-1 **Note** Hotfix AO replaces Hotfix AB. If you installed Hotfix AB, you must install Hotfix AO.	CSCvg35618: Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability. CSCvh79732, CSCvh81737, CSCvh81870: Cisco Adaptive Security Appliance Denial of Service Vulnerability.
Hotfix AN	6.2.2.1	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_AN-6.2.2.2-4 **Note** Hotfix AN replaces Hotfix AC. If you installed Hotfix AC, you must install Hotfix AN.	CSCvg35618: Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability. CSCvh79732, CSCvh81737, CSCvh81870: Cisco Adaptive Security Appliance Denial of Service Vulnerability.
Hotfix Z	6.2.2 6.2.2.1	FTDv: Cisco_FTD_Hotfix_Z-6.2.2.2-7	CSCvg68914: segfault while processing TCP traffic (StreamQueue).
Hotfix D	6.2.2	Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_D-6.2.2.1-4	CSCvg06695: FP2100 Threat Defense pair reporting failed status due to Detect service module failure.

Version 6.2.0 Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.2.0 hotfixes.

Table 15: Version 6.2.0 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix Local Malware Cert	6.2.0 6.2.0.x	FMC/FMCv: Hotfix_Local_Malware_Cert-6.2.0.999-1 **Note** After you upgrade to Version 6.2.2 or 6.2.3, you must apply a new Local Malware Cert hotfix.	CSCvm81052: local malware detection updates not downloading to FMC due to invalid certificate chain.
Hotfix CE	6.2.0.6	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_CE-6.2.0.7-1 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_CE-6.2.0.7-1 FTDv: Cisco_FTD_Hotfix_CE-6.2.0.7-1	CSCvm43975: Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability.
Hotfix BX	6.2.0 6.2.0.1 to 6.2.0.5	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_BX-6.2.0.999-5 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_BX-6.2.0.999-5 FTDv: Cisco_FTD_Hotfix_BX-6.2.0.999-5	CSCvj07038: Firepower devices need to trust Threat Grid certificate.
Hotfix BW	6.2.0 6.2.0.1 to 6.2.0.5	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_BW-6.2.0.999-6 Firepower 7000/8000 series: Sourcefire_3D_Device_S3_Hotfix_BW-6.2.0.999-6 ASA FirePOWER: Cisco_Network_Sensor_Hotfix_BW-6.2.0.999-6 NGIPSv: Sourcefire_3D_Device_Virtual64_VMware_Hotfix_BW-6.2.0.999-6	CSCvj07038: Firepower devices need to trust Threat Grid certificate.
Hotfix BN	6.2.0.4	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_BN-6.2.0.5-3 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_BN-6.2.0.5-3 FTDv: Cisco_FTD_Hotfix_BN-6.2.0.5-3	CSCvg35618: Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability. CSCvh79732, CSCvh81737, CSCvh81870: Cisco Adaptive Security Appliance Denial of Service Vulnerability.

Hotfix	Versions	Platforms	Resolves
Hotfix BH	6.2.0.3	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_BH-6.2.0.4-1	CSCvg32885: Unable to edit or Deployment missing some of the access control rules after upgraded to 6.2.0.3.
Hotfix AQ	6.2.0.2	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_AQ-6.2.0.3-3	CSCve82386: Configuring an IP pool for a diagnostic port channel interface on an Threat Defense cluster fails.
Hotfix U	6.2.0.1	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_U-6.2.0.2-1	CSCve44987: eStreamer service sends corrupt messages and spams log files with Not connected.
Hotfix S	6.2.0.1	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_S-6.2.0.2-1	CSCve35816: SFDataCorrelator segfault due to null pointer dereference in handle_host_address_changes().
Hotfix N	6.2.0	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_N-6.2.0.1-1 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_N-6.2.0.1-1 FTDv: Cisco_FTD_Hotfix_N-6.2.0.1-1	CSCve02069: Cisco Firepower Detection Engine SSL Decryption Memory Consumption Denial of Service Vulnerability.
Hotfix G	6.2.0	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_G-6.2.0.1-4	CSCvd27278: UIMP fails importing all users if any user in the import list has been deleted.
Hotfix F	6.2.0	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_F-6.2.0.1-3 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_F-6.2.0.1-3 FTDv: Cisco_FTD_Hotfix_F-6.2.0.1-3	CSCvc96586: 9K Blocks counters has issues which stops the traffic punted to snort, stating snort busy.
Hotfix B	6.2.0	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_B-6.2.0.1-2	CSCvc57533: Policy Deployment may fail due to delta splitting logic fail.

Hotfix	Versions	Platforms	Resolves
Hotfix AM	6.2.0.2	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_AM-6.2.0.3-3 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_AM-6.2.0.3-3 FTDv: Cisco_FTD_Hotfix_AM-6.2.0.3-3	CSCve04326: Standby should have use CCL to forward traffic instead of blackholing when egress interface is down.
Hotfix AG	6.2.0 6.2.0.1	ASA 5500-X series with FTD: Cisco_FTD_Hotfix_AG-6.2.0.2-3	CSCve95026: ids_event_alertercauses high CPU on Threat Defense device when UUID is missing from EOAttributes.
Hotfix AC	6.2.0.2	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_AC-6.2.0.3-2 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_AC-6.2.0.3-2 FTDv: Cisco_FTD_Hotfix_AC-6.2.0.3-2	CSCve71661: Firepower Threat Defense - Multicast and BPDU traffic dropped due to dst-l2_lookup-fail.
Hotfix AU	6.2.0 6.2.0.1 to 6.2.0.3	FMC 1000, 2500, 4500: Sourcefire_3D_Defense_Center_S3_Hotfix_AU-6.2.0.4-1	CSCvf77493: Management interfaces are missing on Firepower Management Center 4500, 2500, or 1000.
Hotfix A	6.2.0	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_A-6.2.0.1-10 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_A-6.2.0.1-10 ASA FirePOWER with ASDM: Cisco_Network_Sensor_Hotfix_A-6.2.0.1-10	CSCvc88603: All policies using GeoLocation are Blocking traffic.

Version 6.1.0 Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.1.0 hotfixes.

Table 16: Version 6.1.0 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix ES	6.1.0 6.1.0.1 to 6.1.0.7	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_ES-6.1.0.8-2	CSCvr95287: Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability
Hotfix Local Malware Cert	6.1.0 6.1.0.x	FMC/FMCv: Hotfix_Local_Malware_Cert-6.1.0.999-1.sh **Note** After you upgrade to Version 6.2.0 or 6.2.3, you must apply a new Local Malware Cert hotfix.	CSCvm81052: local malware detection updates not downloading to FMC due to invalid certificate chain.
Hotfix EM	6.1.0 6.1.0.1 to 6.1.0.5	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_EM-6.1.0.999-49 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_EM-6.1.0.999-51 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_EM-6.1.0.999-51 FTDv: Cisco_FTD_Hotfix_EM-6.1.0.999-51	CSCvj07038: Firepower devices need to trust Threat Grid certificate.
Hotfix ER	6.1.0.7	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_ER-6.1.0.8-1.sh ASA 5500-X series with FTD: Cisco_FTD_Hotfix_ER-6.1.0.8-1.sh FTDv: Cisco_FTD_Hotfix_ER-6.1.0.8-1.sh	CSCvm43975: Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability.
Hotfix EI	6.1.0.6	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_EI-6.1.0.7-2 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_EI-6.1.0.7-2 FTDv: Cisco_FTD_Hotfix_EI-6.1.0.7-2 **Note** Hotfix EI replaces Hotfix DZ. If you installed Hotfix DZ, you must also install Hotfix EI.	CSCvg35618: Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability. CSCvh95456, CSCvh23085: Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities. CSCvh79732: Cisco Adaptive Security Appliance Denial of Service Vulnerability. CSCvi16029: Cisco Adaptive Security Appliance WebVPN Denial of Service Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix CF	6.1.0.1 6.1.0.2	Firepower 4100/9300 Cisco_FTD_SSP_Hotfix_CF-6.1.0.3-3 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_CF-6.1.0.3-3 FTDv: Cisco_FTD_Hotfix_CF-6.1.0.3-3	CSCvd78303: Firepower Threat Defense device running Version 6.1.0.1 or Version 6.1.0.2 stopped passing traffic after 213 days of uptime and experienced a range of issues from limited connectivity to a traffic outage.
Hotfix DH	6.1.0.5	Firepower 8000 series: Sourcefire_3D_Device_S3_Hotfix_DH-6.1.0.6-48	CSCvf66660: If you update clustered Firepower 8000 Series stacks configured in a high availability environment to Version 6.1.0.5, the peers experience continuous failover.
Hotfix DQ	6.1.0.5	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_DQ-6.1.0.6-1	CSCve82410: If you deploy an intrusion policy configured to block TCP, UDP, ICMP, or IP scanning, the Firepower Management Center detects the port scan but does not block it when it should.
Hotfix AJ	6.1.0 6.1.0.1	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_AJ-6.1.0.2-1	CSCvb96776: Re-establishing high-availability synchronization failed after successfully updating an Firepower Management Center high-availability pair from Version 6.1.0 or later to Version 6.2.0 failed.
Hotfix AZ	6.1.0.2	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_AZ-6.1.0.3-1	CSCvd10943: If you deployed an access control policy containing at least two access control rules referencing the same intrusion policy but with different variable sets from a Firepower Management Center running Version 6.1.0.2, deployment failed.
Hotfix AI	6.1.0	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_AI-6.1.0.2-3	CSCvc49789: An optimization component attempted to connect to the wrong database and caused system issues, such as high CPU use and general performance degradation.

Hotfix	Versions	Platforms	Resolves
Hotfix AF	6.1.0	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_AF-6.1.0.2-1 Firepower 7000/8000 series Sourcefire_3D_Device_S3_Hotfix_AF-6.1.0.2-1 ASA FirePOWER: Cisco_Network_Sensor_Hotfix_AF-6.1.0.2-1 NGIPSv: Sourcefire_3D_Device_Virtual64_VMware_Hotfix_AF-6.1.0.2-1	CSCvc26880: If a Firepower 8350 device or AMP8350 device produced an unusually large stream of messages on the serial port console or, if you enabled it, the Lights-out Management (LOM) console, the device became unresponsive.

Version 6.0.1 Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.0.1 hotfixes.

Table 17: Version 6.01 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix BH	6.0.1.4	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_BH-6.0.1.5-1 ASA 5500-X series with FTD: Cisco_FTD_Hotfix_BH-6.0.1.5-1 FTDv: Cisco_FTD_Hotfix_BH-6.0.1.5-1	CSCvg35618: Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability. CSCvh79732, CSCvh81870: Cisco Adaptive Security Appliance Denial of Service Vulnerability.
Hotfix Local Malware Cert	6.0.1 6.0.1.x	FMC/FMCv: Hotfix_Local_Malware_Cert-6.0.1.999-1 **Note** After you upgrade to Version 6.1, you must apply a new Local Malware Cert hotfix.	CSCvm81052: local malware detection updates not downloading to FMC due to invalid certificate chain.
Hotfix AU	6.0.1.1	Firepower 7000/8000 series: Sourcefire_3D_Device_S3_Hotfix_AU-6.0.1.3-1	CSCvc26880: In some cases, Series 3 devices produced unusually large streams of messages on the serial port console or, if you enabled it, the Lights-out Management (LOM) console and the device become unresponsive.

Version 6.0.0 Hotfixes

This table provides quicklinks to download pages for publicly available Version 6.0.0 hotfixes.

Table 18: Version 6.0.0 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix Local Malware Cert	6.0.0 6.0.0.1	FMC/FMCv: Hotfix_Local_Malware_Cert-6.0.0.999-1 **Note** After you upgrade to Version 6.0.1, you must apply a new Local Malware Cert hotfix.	CSCvm81052: local malware detection updates not downloading to FMC due to invalid certificate chain.
Hotfix O	6.0.0.1	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_O-6.0.0.999-1 ASA FirePOWER with ASDM: Cisco_Network_Sensor_Hotfix_O-6.0.0.0.999-1	CSCuy99274: If you deployed access control rules from either a Firepower Management Center or local management to an ASA Firepower module managed configured with security zones, the system incorrectly deployed the control rules out of order and incoming traffic triggered rules that would not have triggered in the desired configuration.
Hotfix K	6.0.0.1	FMC/FMCv: Sourcefire_3D_Defense_Center_S3_Hotfix_K-6.0.0.2-3	CSCuy60529: New shared object rules are not pushed down to sensor after SRU update.

Version 5.4.x Hotfixes

This table provides quicklinks to download pages for publicly available Version 5.4.x hotfixes.

Table 19: Version 5.4.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix CX	5.4.1.8	ASA FirePOWER (ASA 5506-X series, 5508-X, 5516-X, ISA 3000): Cisco_Network_Sensor_Hotfix_CX-5.4.1.9-1	CSCuv11738: Configuring a system policy to use remote NTP server to synchronize time to a system with a registered ASA FirePOWER modules running a version older than Version 5.4 and experiencing a leap second may cause the system may use a high amount of CPU.

Hotfix	Versions	Platforms	Resolves
Hotfix DK	5.4.0.9	Firepower 7000/8000 series: Sourcefire_3D_Device_S3_Hotfix_DK-5.4.0.10-1 ASA FirePOWER (ASA 5515-X, 5525-X, 5545-X, 5555-X): Cisco_Network_Sensor_Hotfix-5.4.0.10-1 NGIPSv: Sourcefire_3D_Device_Virtual64_VMware_Hotfix-5.4.0.10-1	CSCvb26230: Excessive logging causes disk space issues, performance degradation, and limited storage.