# Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes

**First Published:** 2017-09-21

**Last Modified:** 2024-04-29

# Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes

Hotfixes are minor updates that address particular, urgent issues.

**Note** This document provides quicklinks to download pages for publicly available hotfixes. 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.

## Available Hotfixes

### 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 1: BIOS and Firmware Minimum Requirements***

| Platform | Version | Hotfix | BIOS | RAID Controller Firmware | CIMC Firmware |
|---|---|---|---|---|---|
| FMC 1600, 2600, 4600 | 7.0 | BIOS Update Hotfix EZ | C220M5.4.3.2a.0 | 51.10.0-3612 | 4.3(2.240009) |
| | 7.1<br>6.7<br>6.6<br>6.4 | BIOS Update Hotfix EN | C220M5.4.2.3b.0 | 51.10.0-3612 | 4.2(3b) |

| Platform | Version | Hotfix | BIOS | RAID Controller Firmware | CIMC Firmware |
|---|---|---|---|---|---|
| FMC 1000, 2500, 4500 | 7.0<br>6.7<br>6.6<br>6.4 | BIOS Update Hotfix EN | C220M5.4.2.3b.0 | 51.10.0-3612 | 4.2(3b) |
| | 6.2.3 | BIOS Update Hotfix EL | C220M4.4.1.2c.0 | 24.12.1-0456 | 4.1(2g) |
| FMC 2000, 4000 | 6.6<br>6.4<br>6.2.3 | BIOS Update Hotfix EI | C220M3.3.0.4e.0 | 23.33.1-0060 | 3.0(4s) |
| FMC 750, 1500, 3500 | 6.4<br>6.2.3 | BIOS Update Hotfix EI | C220M3.3.0.4e.0 | 23.33.1-0060 | 3.0(4s) |

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.

**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 7.4.x Hotfixes

There are no publicly available hotfixes for Version 7.4.x.

## Version 7.3.x Hotfixes

*Table 2: Version 7.3.x Hotfixes*

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix EN | 7.3.0<br>7.3.x<br>7.3.x.x | Management Center (all hardware models):<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_730_EN-11<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |

## Version 7.2.x Hotfixes

This table provides quicklinks to download pages for publicly available Version 7.2.x hotfixes.

*Table 3: Version 7.2.x Hotfixes*

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix EN | 7.2.0<br>7.2.x<br>7.2.x.x | Management Center (all hardware models):<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_720_EN-11<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |
| Hotfix BJ | 7.2.5 | Firepower 1000 series:<br>Cisco_FTD_SSP_FP1K_Hotfix_BJ-7.2.5.1-1<br>Firepower 2100 series:<br>Cisco_FTD_SSP_FP2K_Hotfix_BJ-7.2.5.1-1<br>Secure Firewall 3100 series:<br>Cisco_FTD_SSP_FP3K_Hotfix_BJ-7.2.5.1-1<br>Firepower 4100/9300<br>Cisco_FTD_SSP_Hotfix_BJ-7.2.5.1-1<br>ISA 3000:<br>Cisco_FTD_Hotfix_BJ-7.2.5.1-1<br>Threat Defense Virtual:<br>Cisco_FTD_Hotfix_BJ-7.2.5.1-1 | CSCwh23100: Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability<br>CSCwh45108: Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability |

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix AW | 7.2.4 | Firepower 1000 series:<br>Cisco_FTD_SSP_FP1K_Hotfix_AW-7.2.4.1-1<br>Firepower 2100 series:<br>Cisco_FTD_SSP_FP2K_Hotfix_AW-7.2.4.1-1<br>Secure Firewall 3100 series:<br>Cisco_FTD_SSP_FP3K_Hotfix_AW-7.2.4.1-1<br>Firepower 4100/9300<br>Cisco_FTD_SSP_Hotfix_AW-7.2.4.1-1<br>ISA 3000:<br>Cisco_FTD_Hotfix_AW-7.2.4.1-1<br>Threat Defense Virtual:<br>Cisco_FTD_Hotfix_AW-7.2.4.1-1 | CSCwf71606: Cisco ASA and FTD ACLs Not Installed upon Reload |
| Hotfix AN | 7.2.4-165 | Management Center:<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_AN-7.2.4.1-2<br>**Note** Apply this hotfix to Version 7.2.4-165 only. Do not apply to Version 7.2.4-169, which fixes this issue. | CSCwf28592: In some specific scenarios, object optimizer can cause incorrect rules to be deployed to the device |

## Version 7.1.x Hotfixes

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

***Table 4: Version 7.1.x Hotfixes***

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix EN | 7.1.0<br>7.1.x<br>7.1.x.x | FMC (all hardware models):<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_710_EN-11<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |
| Hotfix Q | 7.1.0.2 | Secure Firewall 3100 series:<br>Cisco_FTD_SSP_FP3K_Hotfix_Q-7.1.0.3-2 | CSCwb88651: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability<br>CSCwc28334: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability |

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix P | 7.1.0.1 | Firepower 1000 series:<br>Cisco_FTD_SSP_FP1K_Hotfix_P-7.1.0.2-2<br>Firepower 2100 series:<br>Cisco_FTD_SSP_FP2K_Hotfix_P-7.1.0.2-2<br>Firepower 4100/9300<br>Cisco_FTD_SSP_Hotfix_P-7.1.0.2-2<br>ISA 3000:<br>Cisco_FTD_Hotfix_P-7.1.0.2-2<br>FTDv:<br>Cisco_FTD_Hotfix_P-7.1.0.2-2 | CSCwb88651: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability<br>CSCwc28334: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability |
| Hotfix A | 7.1.0 | Firepower 1000 series with FDM:<br>Cisco_FTD_SSP_FP1K_Hotfix_A-7.1.0.1-7<br>Firepower 2100 series with FDM:<br>Cisco_FTD_SSP_FP2K_Hotfix_A-7.1.0.1-7<br>Firepower 4100/9300 with FDM:<br>Cisco_FTD_SSP_Hotfix_A-7.1.0.1-7<br>ISA 3000 with FDM:<br>Cisco_FTD_Hotfix_A-7.1.0.1-7<br>FTDv with FDM:<br>Cisco_FTD_Hotfix_A-7.1.0.1-7<br>**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 5: Version 7.0.x Hotfixes*

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix EZ | 7.0.0<br>7.0.x<br>7.0.x.x | Management Center (1600, 2600, 4600):<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EZ-5<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |
| Hotfix EN | 7.0.0<br>7.0.x<br>7.0.x.x | Management Center (1000, 2500, 4500):<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EN-11<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |
| Hotfix EI | 7.0.6 | Firepower 1000 series:<br>Cisco_FTD_SSP_FP1K_Hotfix_EI-7.0.6.1-3<br>Firepower 2100 series:<br>Cisco_FTD_SSP_FP2K_Hotfix_EI-7.0.6.1-3<br>Firepower 4100/9300:<br>Cisco_FTD_SSP_Hotfix_EI-7.0.6.1-3<br>ASA 5500-X series and ISA 3000 with FTD:<br>Cisco_FTD_Hotfix_EI-7.0.6.1-3<br>FTDv:<br>Cisco_FTD_Hotfix_EI-7.0.6.1-3 | CSCwh23100: Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability<br>CSCwh45108: Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability |
| Hotfix DC | 7.0.5 | FMC:<br>Cisco_Firepower_Mgmt_Center_Hotfix_DC-7.0.5.1-5 | CSCwd88641: Deployment changes to push VDB package based on Device model and snort engine |

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix S | 7.0.1 | Firepower 1000 series with FDM:<br>Cisco_FTD_SSP_FP1K_Hotfix_S-7.0.1.1-10<br>Firepower 2100 series with FDM:<br>Cisco_FTD_SSP_FP2K_Hotfix_S-7.0.1.1-10<br>Firepower 4100/9300 with FDM:<br>Cisco_FTD_SSP_Hotfix_S-7.0.1.1-10<br>ASA 5500-X series and ISA 3000 with FDM:<br>Cisco_FTD_Hotfix_S-7.0.1.1-10<br>FTDv with FDM:<br>Cisco_FTD_Hotfix_S-7.0.1.1-10<br>**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.<br>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<br>CSCwa55039: Firepower Threat Defense Hotfix S for 7.0.1 cause system failing when ran twice |

## Version 6.7.x Hotfixes

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

***Table 6: Version 6.7.x Hotfixes***

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix EN | 6.7.0<br>6.7.x<br>6.7.x.x | FMC (all hardware models):<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_670_EN-11<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |

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

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

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| | | | deployment from FMC<br>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:<br>Cisco_FTD_SSP_FP1K_Hotfix_Y-6.7.0.3-7<br>Firepower 2100 series with FDM:<br>Cisco_FTD_SSP_FP2K_Hotfix_Y-6.7.0.3-7<br>Firepower 4100/9300 with FDM:<br>Cisco_FTD_SSP_Hotfix_Y-6.7.0.3-7<br>ASA 5500-X series and ISA 3000 with FDM:<br>Cisco_FTD_Hotfix_Y-6.7.0.3-7<br>FTDv with FDM:<br>Cisco_FTD_Hotfix_Y-6.7.0.3-7<br>**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 C | 6.7.0<br>6.7.x.x | ISA 3000 with FTD:<br>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 7: Version 6.6.x Hotfixes***

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix EN | 6.6.0<br>6.6.x<br>6.6.x.x | FMC (1000, 1600, 2500, 2600, 4500, 4600):<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EN-11<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix EB | 6.6.7.1 | FMC/FMCv:<br>Cisco_Firepower_Mgmt_Center_Hotfix_EB-6.6.7.2-4 | CSCwd88641: Deployment changes to push VDB package based on Device model and snort engine |
| Hotfix DE | 6.6.5<br>6.6.5.1 | FMC/FMCv:<br>Cisco_Firepower_Mgmt_Center_Hotfix_DE-6.6.5.2-8<br>Firepower 1000 series with FDM:<br>Cisco_FTD_SSP_FP1K_Hotfix_DE-6.6.5.2-8<br>Firepower 2100 series with FDM:<br>Cisco_FTD_SSP_FP2K_Hotfix_DE-6.6.5.2-8<br>Firepower 4100/9300 with FDM:<br>Cisco_FTD_SSP_Hotfix_DE-6.6.5.2-8<br>ASA 5500-X series and ISA 3000 with FDM:<br>Cisco_FTD_Hotfix_DE-6.6.5.2-8<br>FTDv with FDM:<br>Cisco_FTD_Hotfix_DE-6.6.5.2-8<br>ASA FirePOWER with ASDM:<br>Cisco_Network_Sensor_Hotfix_DE-6.6.5.2-8<br>**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:<br>Cisco_FTD_SSP_FP1K_Hotfix_DA-6.6.5.2-4<br>Firepower 2100 series with FDM<br>Cisco_FTD_SSP_FP2K_Hotfix_DA-6.6.5.2-4<br>Firepower 4100/9300 with FDM:<br>Cisco_FTD_SSP_Hotfix_DA-6.6.5.2-4<br>ASA 5500-X series and ISA 3000 with FDM:<br>Cisco_FTD_Hotfix_DA-6.6.5.2-4<br>FTDv with FDM:<br>Cisco_FTD_Hotfix_DA-6.6.5.2-4<br>**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 EI | 6.6.0<br>6.6.x<br>6.6.x.x | FMC 2000, 4000:<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EI-15<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |
| Hotfix AB | 6.6.1 | ISA 3000 with FTD:<br>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<br>6.6.0.x | ISA 3000 with FTD:<br>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 6.4.0 Hotfixes

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

***Table 8: Version 6.4.0 Hotfixes***

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix EN | 6.4.0<br>6.4.x<br>6.4.x.x | FMC (1000, 1600, 2500, 2600, 4500, 4600):<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EN-11<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |
| Hotfix EP | 6.4.0.13 | Firepower 1000 series with FDM:<br>Cisco_FTD_SSP_FP1K_Hotfix_EP-6.4.0.14-9<br>Firepower 2100 series with FDM:<br>Cisco_FTD_SSP_FP2K_Hotfix_EP-6.4.0.14-9<br>ASA 5500-X series and ISA 3000 with FDM:<br>Cisco_FTD_Hotfix_EP-6.4.0.14-9<br>FTDv with FDM:<br>Cisco_FTD_Hotfix_EP-6.4.0.14-9<br>**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 EI | 6.4.0<br>6.4.0.x | FMC 750, 1500, 2000, 3500, 4000:<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EI-15<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |
| Hotfix DV | 6.4.0<br>6.4.0.x | ISA 3000 with FTD:<br>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 BM | 6.4.0.9 | Firepower 1000 series:<br>Cisco_FTD_SSP_FP1K_Hotfix_BM-6.4.0.10-2<br>Firepower 2100 series:<br>Cisco_FTD_SSP_FP2K_Hotfix_BM-6.4.0.10-2<br>Firepower 4100/9300:<br>Cisco_FTD_SSP_Hotfix_BM-6.4.0.10-2<br>ASA 5500-X series and ISA 3000 with FTD:<br>Cisco_FTD_Hotfix_BM-6.4.0.10-2<br>FTDv:<br>Cisco_FTD_Hotfix_BM-6.4.0.10-2 | CSCvt03598: Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability |

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix AY | 6.4.0.8 | Firepower 1000 series:<br>Cisco_FTD_SSP_FP1K_Hotfix_AY-6.4.0.9-3<br>Firepower 2100 series:<br>Cisco_FTD_SSP_FP2K_Hotfix_AY-6.4.0.9-3<br>Firepower 4100/9300:<br>Cisco_FTD_SSP_Hotfix_AY-6.4.0.9-3<br>ASA 5500-X series and ISA 3000 with FTD:<br>Cisco_FTD_Hotfix_AY-6.4.0.9-3<br>FTDv:<br>Cisco_FTD_Hotfix_AY-6.4.0.9-3<br>**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<br>CSCvs10748: Cisco Adaptive Security Appliance and Firepower Threat Defense Denial of Service Vuln<br>CSCvo80853: Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability<br>CSCvs50459: Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability<br>CSCvr86783: Standby FDM lost connectivity after forming HA<br>CSCvr92168: ASA/FTD Slow memory leak in OSPF process when processing OSPF Hellos<br>CSCvt15163: Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability<br>CSCvq89361: Cisco Firepower 1000 Series SSL/TLS Denial of Service Vulnerability<br>CSCvu20521: OSPF is not forming after HF installation |
| Hotfix U | 6.4.0.5 and 6.4.0.6 | FMC/FMCv:<br>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<br>6.4.0.1 to 6.4.0.4 | FMC/FMCv:<br>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:<br>Cisco_Firepower_Mgmt_Center_Hotfix_AA-6.4.0.8-4<br>**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 | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix X | 6.4.0.6 | FMC/FMCv:<br>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:<br>Cisco_Firepower_Mgmt_Center_Hotfix_F-6.4.0.3-2<br>Firepower 2100 series:<br>Cisco_FTD_SSP_FP2K_Hotfix_F-6.4.0.3-2<br>Firepower 4100/9300:<br>Cisco_FTD_SSP_Hotfix_F-6.4.0.3-2<br>ASA 5500-X series and ISA 3000 with FTD:<br>Cisco_FTD_Hotfix_F-6.4.0.3-2<br>FTDv (VMware, FVM):<br>Cisco_FTD_Hotfix_F-6.4.0.3-2 | CSCvq34224: Firepower Primary Detection Engine process terminated after Manager upgrade |

## Version 6.2.3 Hotfixes

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

***Table 9: Version 6.2.3 Hotfixes***

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix EM | 6.2.3.17 | Firepower 2100 series with FDM:<br>Cisco_FTD_SSP_FP2K_Hotfix_EM-6.2.3.18-13<br>ASA 5500-X series and ISA 3000 with FDM:<br>Cisco_FTD_Hotfix_EM-6.2.3.18-13<br>FTDv with FDM:<br>Cisco_FTD_Hotfix_EM-6.2.3.18-13<br>**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<br>6.2.3.x | FMC 1000, 2500, 4500:<br>Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EL-7<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix EI | 6.2.3<br>6.2.3.x | FMC 750, 1500, 2000, 3500, 4000:<br>Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EI-15<br>**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.<br>See BIOS and Firmware Hotfixes for Management Center Hardware, on page 1. |
| Hotfix EH | 6.2.3<br>6.2.3.x | ASA 5506-X series with FTD:<br>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 | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix DT | 6.2.3.15 | Firepower 2100 series:<br>Cisco_FTD_SSP_FP2K_Hotfix_DT-6.2.3.16-3<br>Firepower 4100/9300:<br>Cisco_FTD_SSP_Hotfix_DT-6.2.3.16-3<br>ASA 5500-X series and ISA 3000 with FTD:<br>Cisco_FTD_Hotfix_DT-6.2.3.16-3<br>FTDv:<br>Cisco_FTD_Hotfix_DT-6.2.3.16-3 | CSCvr55825: Cisco ASA and FTD Software Path Traversal Vulnerability<br>CSCvp49481, CSCvp93468: Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability<br>CSCvp16945, CSCvp16949: Cisco ASA Software and FTD Software MGCP Denial of Service Vulnerabilities<br>CSCvo62077: Cisco Firepower Threat Defense Software VPN System Logging Denial of Service Vulnerability<br>CSCvs10748: Cisco Adaptive Security Appliance and Firepower Threat Defense Denial of Service Vuln<br>CSCvs50459: Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability<br>CSCvo80853: Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability<br>CSCvr07419: Cisco ASA and FTD Software IPv6 DNS Denial of Service Vulnerability<br>CSCvt15163: Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability |

| Hotfix | Versions | Platforms | Resolves |
|---|---|---|---|
| Hotfix DW | 6.2.3.15 | Firepower 2100 series:<br>Cisco_FTD_SSP_FP2K_Hotfix_DW-6.2.3.16-6<br>Firepower 4100/9300:<br>Cisco_FTD_SSP_Hotfix_DW-6.2.3.16-6<br>ASA 5500-X series and ISA 3000 with FTD:<br>Cisco_FTD_Hotfix_DW-6.2.3.16-6<br>FTDv:<br>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<br>CSCvs84713: Cannot SSH to the device after upgrading FTD on ASA55XX/ISA 3000/FTDv to 6.2.3.15 build 38<br>CSCvs95725: Virtual FTD Running on 6.2.3.15 blocks SSH request and loses connection with the FMC |
| Hotfix DO | 6.2.3<br>6.2.3.1 to 6.2.3.15 | FMC/FMCv:<br>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:<br>Sourcefire_3D_Defense_Center_S3_Hotfix_DQ-6.2.3.16-2<br>**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:<br>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:<br>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<br>6.2.3.x | FMC/FMCv:<br>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<br>6.2.3.1 to 6.2.3.3 | FMC/FMCv:<br>Sourcefire_3D_Defense_Center_S3_Hotfix_H-6.2.3.999-5<br>Firepower 7000/8000 series:<br>Sourcefire_3D_Device_S3_Hotfix_H-6.2.3.999-5<br>ASA FirePOWER:<br>Cisco_Network_Sensor_Hotfix_H-6.2.3.999-5<br>NGIPSv:<br>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<br>6.2.3.1 to 6.2.3.3 | Firepower 2100 series:<br>Cisco_FTD_SSP_FP2K_Hotfix_G-6.2.3.999-6<br>Firepower 4100/9300:<br>Cisco_FTD_SSP_Hotfix_G-6.2.3.999-6<br>ASA 5500-X series with FTD:<br>Cisco_FTD_Hotfix_G-6.2.3.999-6<br>FTDv (VMware, KVM, AWS):<br>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:<br>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:<br>Cisco_FTD_SSP_FP2K_Hotfix_A-6.2.3.1-10<br>Firepower 4100/9300:<br>Cisco_FTD_SSP_Hotfix_A-6.2.3.1-10<br>ASA 5500-X series with FTD:<br>Cisco_FTD_Hotfix_A-6.2.3.1-10<br>FTDv (VMware, KVM, AWS):<br>Cisco_FTD_Hotfix_A-6.2.3.1-10 | CSCvg65072: ASA, Threat Defense, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability.<br>CSCvi16029: ASA Web Interface Authentication Bypass. |

## 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 naming scheme: *Platform*_Hotfix_*letter-version-build*.sh.REL.tar. Do not untar signed (.tar) packages.

## 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 10: Hotfixing Management Center*

| Current Management Center Version | Guide |
|---|---|
| Cloud-delivered management center (no version) | None. We take care of updates. |
| 7.2+ | *Upgrade the Management Center* 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 11: Hotfixing Threat Defense with Management Center*

| Current Management Center Version | Guide |
|---|---|
| Cloud-delivered management center (no version) | *Upgrade Threat Defense* in the latest released version of the Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center. |
| 7.2+ | *Upgrade Threat Defense* 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 12: Hotfixing Threat Defense with Device Manager*

| Current Threat Defense Version | Guide |
|---|---|
| 7.2+ | *Upgrade Threat Defense* 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. |
| 7.0 or earlier | *System Management* in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for your version. |

| Current Threat Defense Version | Guide |
|---|---|
| Version 6.4+, with CDO | Use device manager to install threat defense hotfixes. You cannot use CDO. |

### NGIPS

*Table 13: Hotfixing NGIPS Devices*

| Current Manager 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 Secure Firewall 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. Install 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 appropriate upgrade guide.

*Table 14: Upgrade Guides*

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

# 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