



Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes

First Published: 2017-09-21

Last Modified: 2024-05-01

Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes

Hotfixes are minor updates that address particular, urgent issues.

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.

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 1700, 2700, 4700	7.4	BIOS Update Hotfix EZ	C225M6.4.3.2c.0	52.20.0-4523	4.3(2.240009)
FMC 1600, 2600, 4600	7.4	BIOS Update Hotfix EZ	C220M5.4.3.2a.0	51.10.0-3612	4.3(2.240009)
	7.3				
	7.2				
	7.0				
FMC 1600, 2600, 4600	7.1	BIOS Update Hotfix EN	C220M5.4.2.3b.0	51.10.0-3612	4.2(3b)
	6.7				
	6.6				
	6.4				

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

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

Table 2: Version 7.4.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EZ	7.4.0 7.4.x 7.4.x.x	Management Center (all hardware models): Cisco_Secure_FW_Mgmt_Center_Hotfix_EZ_BIOSUPDATE-7.4.99.99-6 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 1 .

Version 7.3.x Hotfixes

Table 3: Version 7.3.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EZ	7.3.0 7.3.x 7.3.x.x	Management Center (all hardware models): Cisco_Secure_FW_Mgmt_Center_Hotfix_EZ_BIOSUPDATE-7.3.99.99-6 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 1 .

Version 7.2.x Hotfixes

Table 4: Version 7.2.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EZ	7.2.0 7.2.x 7.2.x.x	Management Center (all hardware models): Cisco_Secure_FW_Mgmt_Center_Hotfix_EZ_BIOSUPDATE-7.2.99.99-6shREL.tar 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 1 .

Hotfix	Versions	Platforms	Resolves
Hotfix BJ	7.2.5	Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_BJ-7.2.5.1-1 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_BJ-7.2.5.1-1 Secure Firewall 3100 series: Cisco_FTD_SSP_FP3K_Hotfix_BJ-7.2.5.1-1 Firepower 4100/9300 Cisco_FTD_SSP_Hotfix_BJ-7.2.5.1-1 ISA 3000: Cisco_FTD_Hotfix_BJ-7.2.5.1-1 Threat Defense Virtual: Cisco_FTD_Hotfix_BJ-7.2.5.1-1	CSCwh23100 : Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability CSCwh45108 : Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
Hotfix AW	7.2.4	Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_AW-7.2.4.1-1 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_AW-7.2.4.1-1 Secure Firewall 3100 series: Cisco_FTD_SSP_FP3K_Hotfix_AW-7.2.4.1-1 Firepower 4100/9300 Cisco_FTD_SSP_Hotfix_AW-7.2.4.1-1 ISA 3000: Cisco_FTD_Hotfix_AW-7.2.4.1-1 Threat Defense Virtual: 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: Cisco_Secure_FW_Mgmt_Center_Hotfix_AN-7.2.4.1-2 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

Table 5: Version 7.1.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EN	7.1.0 7.1.x 7.1.x.x	FMC (all hardware models): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_710_EN-11 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 1 .
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_P-7.1.0.2-2 ISA 3000: Cisco_FTD_Hotfix_P-7.1.0.2-2 FTDv: Cisco_FTD_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	Versions	Platforms	Resolves
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

Table 6: Version 7.0.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EZ	7.0.0 7.0.x 7.0.x.x	Management Center (1600, 2600, 4600): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EZ-5 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 1 .
Hotfix EN	7.0.0 7.0.x 7.0.x.x	Management Center (1000, 2500, 4500): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EN-11 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 1 .

Hotfix	Versions	Platforms	Resolves
Hotfix EI	7.0.6	Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_EI-7.0.6.1-3 Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_EI-7.0.6.1-3 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_EI-7.0.6.1-3 ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_EI-7.0.6.1-3 FTDv: Cisco_FTD_Hotfix_EI-7.0.6.1-3	CSCwh23100 : Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability CSCwh45108 : Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
Hotfix DC	7.0.5	FMC: 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 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 <i>not</i> 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

Version 6.7.x Hotfixes

Table 7: Version 6.7.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EN	6.7.0 6.7.x 6.7.x.x	FMC (all hardware models): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_670_EN-11 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 1 .

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

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 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

Table 8: Version 6.6.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EN	6.6.0 6.6.x 6.6.x.x	FMC (1000, 1600, 2500, 2600, 4500, 4600): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EN-11 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 1 .
Hotfix EB	6.6.7.1	FMC/FMCv: 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	Versions	Platforms	Resolves
Hotfix DE	6.6.5 6.6.5.1	<p>FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_DE-6.6.5.2-8</p> <p>Firepower 1000 series with FDM: Cisco_FTD_SSP_FP1K_Hotfix_DE-6.6.5.2-8</p> <p>Firepower 2100 series with FDM: Cisco_FTD_SSP_FP2K_Hotfix_DE-6.6.5.2-8</p> <p>Firepower 4100/9300 with FDM: Cisco_FTD_SSP_Hotfix_DE-6.6.5.2-8</p> <p>ASA 5500-X series and ISA 3000 with FDM: Cisco_FTD_Hotfix_DE-6.6.5.2-8</p> <p>FTDv with FDM: Cisco_FTD_Hotfix_DE-6.6.5.2-8</p> <p>ASA FirePOWER with ASDM: Cisco_Network_Sensor_Hotfix_DE-6.6.5.2-8</p> <p>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.</p>	CSCwa70008 : Expired certs cause Security Intel. and malware file preclassification signature updates to fail
Hotfix DA	6.6.5.1	<p>Firepower 1000 series with FDM: Cisco_FTD_SSP_FP1K_Hotfix_DA-6.6.5.2-4</p> <p>Firepower 2100 series with FDM Cisco_FTD_SSP_FP2K_Hotfix_DA-6.6.5.2-4</p> <p>Firepower 4100/9300 with FDM: Cisco_FTD_SSP_Hotfix_DA-6.6.5.2-4</p> <p>ASA 5500-X series and ISA 3000 with FDM: Cisco_FTD_Hotfix_DA-6.6.5.2-4</p> <p>FTDv with FDM: Cisco_FTD_Hotfix_DA-6.6.5.2-4</p> <p>Note Apply this hotfix to FDM and FDM/CDO-managed devices. FMC-managed devices are not vulnerable to this exploit.</p>	CSCwa46963 : Security: CVE-2021-44228 -> Log4j 2 Vulnerability

Hotfix	Versions	Platforms	Resolves
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 1 .
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 6.4.0 Hotfixes

Table 9: Version 6.4.0 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EN	6.4.0 6.4.x 6.4.x.x	FMC (1000, 1600, 2500, 2600, 4500, 4600): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EN-11 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 1 .
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	Versions	Platforms	Resolves
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 1 .
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 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	Versions	Platforms	Resolves
Hotfix AY	6.4.0.8	<p>Firepower 1000 series: Cisco_FTD_SSP_FP1K_Hotfix_AY-6.4.0.9-3</p> <p>Firepower 2100 series: Cisco_FTD_SSP_FP2K_Hotfix_AY-6.4.0.9-3</p> <p>Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_AY-6.4.0.9-3</p> <p>ASA 5500-X series and ISA 3000 with FTD: Cisco_FTD_Hotfix_AY-6.4.0.9-3</p> <p>FTDv: Cisco_FTD_Hotfix_AY-6.4.0.9-3</p> <p>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.</p>	<p>CSCvp49481, CSCvp93468: Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability</p> <p>CSCvs10748: Cisco Adaptive Security Appliance and Firepower Threat Defense Denial of Service Vuln</p> <p>CSCvo80853: Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability</p> <p>CSCvs50459: Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability</p> <p>CSCvr86783: Standby FDM lost connectivity after forming HA</p> <p>CSCvr92168: ASA/FTD Slow memory leak in OSPF process when processing OSPF Hellos</p> <p>CSCvt15163: Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability</p> <p>CSCvq89361: Cisco Firepower 1000 Series SSL/TLS Denial of Service Vulnerability</p> <p>CSCvu20521: OSPF is not forming after HF installation</p>
Hotfix U	6.4.0.5 and 6.4.0.6	<p>FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_U-6.4.0.7-2</p>	CSCvr95287 : Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability
Hotfix T	6.4.0 6.4.0.1 to 6.4.0.4	<p>FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_T-6.4.0.5-1</p>	CSCvr95287 : Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability
Hotfix AA	6.4.0.4 to 6.4.0.7	<p>FMC/FMCv: Cisco_Firepower_Mgmt_Center_Hotfix_AA-6.4.0.8-4</p> <p>Note You must also update to VDB 329+ and deploy configuration changes. You can do this before or after you apply the hotfix.</p>	Resolves issues with application identification.

Hotfix	Versions	Platforms	Resolves
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 6.2.3 Hotfixes

Table 10: 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 1 .

Hotfix	Versions	Platforms	Resolves
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 1 .
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	Versions	Platforms	Resolves
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	<p>CSCvr55825: Cisco ASA and FTD Software Path Traversal Vulnerability</p> <p>CSCvp49481, CSCvp93468: Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability</p> <p>CSCvp16945, CSCvp16949: Cisco ASA Software and FTD Software MGCP Denial of Service Vulnerabilities</p> <p>CSCvo62077: Cisco Firepower Threat Defense Software VPN System Logging Denial of Service Vulnerability</p> <p>CSCvs10748: Cisco Adaptive Security Appliance and Firepower Threat Defense Denial of Service Vuln</p> <p>CSCvs50459: Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability</p> <p>CSCvo80853: Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability</p> <p>CSCvr07419: Cisco ASA and FTD Software IPv6 DNS Denial of Service Vulnerability</p> <p>CSCvt15163: Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability</p>

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.

Applying Hotfixes

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 that in management center deployments, use the guide for the version of management center (not threat defense) that you are currently running. In device manager deployments, use the device manager guide even if you usually use CDO; you cannot use CDO to hotfix threat defense.

Table 11: Upgrade Guides for Management Center

Current Management Center Version	Guide
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version: <i>Upgrade Management Center</i>
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1: <i>Upgrade the FMC</i>
7.0 or earlier	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0: <i>Upgrade Firepower Management Centers</i>

Table 12: Upgrade Guides for Threat Defense with Management Center

Current Management Center Version	Guide
Cloud-delivered Firewall Management Center	Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version: <i>Upgrade Threat Defense</i>
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1: <i>Upgrade FTD</i>
7.0 or earlier	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0: <i>Upgrade Firepower Threat Defense</i>

Table 13: Upgrade Guides for Threat Defense with Device Manager

Current Threat Defense Version	Guide
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager for your version: <i>Upgrade Threat Defense</i>
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1: <i>Upgrade FTD</i>
7.0 or earlier	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for your version: <i>System Management</i>

Table 14: Upgrade Guides for NGIPS

Platform	Current Manager Version	Guide
Firepower 7000/8000 series with management center	6.0.0–7.0.x	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0: Upgrade Firepower 7000/8000 Series and NGIPSv
NGIPSv with management center	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0: Upgrade Firepower 7000/8000 Series and NGIPSv
	7.2.6–7.2.x 7.4.1–7.4.x	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version: <i>Upgrade Older ASA FirePOWER and NGIPSv Devices</i>
ASA FirePOWER with management center	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0: Upgrade ASA with FirePOWER Services
	7.2.6–7.2.x 7.4.1–7.4.x	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version: <i>Upgrade Older ASA FirePOWER and NGIPSv Devices</i>
ASA FirePOWER with ASDM	Any	Cisco Secure Firewall ASA Upgrade Guide: Upgrade the ASA FirePOWER Module

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 (linked above).

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](#)

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)

© 2017–2024 Cisco Systems, Inc. All rights reserved.