Cisco Secure Firewall Threat Defense/Firepower ホットフィックス リリースノート

初版：2017 年 9 月 21 日

最終更新：2021 年 12 月 21 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

第 1 章 ホットフィックスについて 1

ホットフィックスのダウンロード 1

ホットフィックスのインストール 2

ホットフィックス成功の確認 4

無応答または失敗したホットフィックス 4

ホットフィックスのアンインストール 4

トラフィック フローとインスペクション 4

サポートが必要な場合 5

第 2 章 利用可能なホットフィックス 7

Management Center ハードウェアの BIOS およびファームウェアのホットフィックス 8

バージョン 7.2.x のホットフィックス 9

バージョン 7.1.x のホットフィックス 10

バージョン 7.0.x のホットフィックス 12

バージョン 6.7.x のホットフィックス 13

バージョン 6.6.x のホットフィックス 17

バージョン 6.5.0 のホットフィックス 20

バージョン 6.4.0 のホットフィックス 23

バージョン 6.3.0 のホットフィックス 26

バージョン 6.2.3 のホットフィックス 29

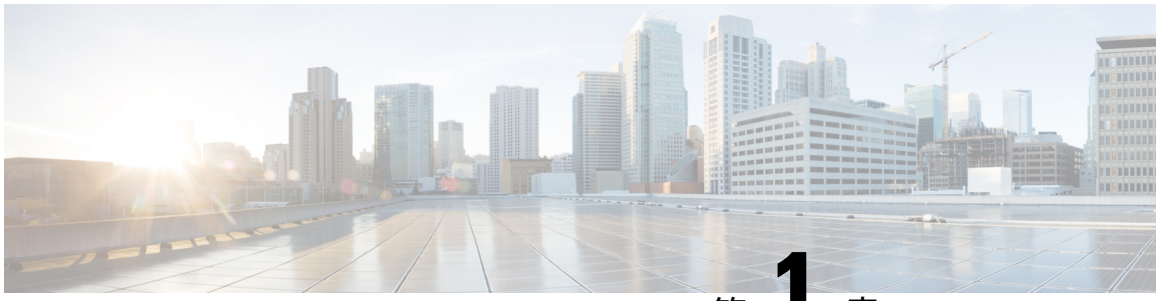
バージョン 6.2.2 のホットフィックス 34

バージョン 6.2.0 のホットフィックス 36

バージョン 6.1.0 のホットフィックス 40

バージョン 6.0.1 のホットフィックス 43

バージョン 6.0.0 のホットフィックス 44
バージョン 5.4.x のホットフィックス 45



第 1 章

ホットフィックスについて

ホットフィックスは、特定の緊急の問題に対処するマイナーな更新プログラムです。

- ホットフィックスのダウンロード （1 ページ）
- ホットフィックスのインストール （2 ページ）
- ホットフィックス成功の確認 （4 ページ）
- 無応答または失敗したホットフィックス （4 ページ）
- ホットフィックスのアンインストール （4 ページ）
- トラフィック フローとインスペクション （4 ページ）
- サポートが必要な場合 （5 ページ）

ホットフィックスのダウンロード

シスコ サポートおよびダウンロードサイト（https://software.cisco.com/download/home）からホットフィックスをダウンロードします。

ホットフィックスを見つけるには、モデルを選択または検索し、現在のバージョンに対するソフトウェアのダウンロードページを参照します。使用可能なホットフィックスがアップグレードおよびインストール パッケージとともに一覧表示されます。パッチレベルのダウンロードページでホットフィックスが見つからない場合（特に同じホットフィックスが他のパッチに適用される場合）は、ホットフィックスが適用される他のダウンロードページ（特に最初のバージョンと最新のバージョン）を参照してください。

ファミリまたはシリーズのすべてのモデルに同じホットフィックスパッケージを使用します。ほとんどのホットフィックスパッケージでは、次の命名スキームが使用されます。

- *Platform*_Hotfix_*letter-version-build*.sh.REL.tar（バージョン 6.2.2+）
- *Platform*_Hotfix_*letter-version-build*.sh（バージョン 5.4 ～ 6.2.0）

署名付きの（.tar）パッケージは解凍しないでください。

ヒント　使用中のアプライアンスでインターネットにアクセス可能な Management Center 展開および ASDM 展開では、シスコから直接ホットフィックスを簡単に取得できます。Management Center で、**[System]** > **[Updates]**を選択して [Download Update] をクリックします。ASDM で、**[Configuration]** > **[ASA FirePOWER Configuration]** > **[Updates]** を選択し、[Download Updates] をクリックします。

ホットフィックスのインストール

ホットフィックスは、パッチをインストールするのと同じ方法でインストールします。手順については、次のいずれかのガイドを参照してください。

（注）　CDO と Device Manager の展開では、Device Manager を使用して Threat Defense ホットフィックスをインストールしてください。CDO は使用できません。

Management Center

表 *1 : Management Center* のホットフィックス

現在の Management Center のバージョン	ガイド
クラウド提供型の管理センター（バージョンなし）	なし。更新はシスコが行います。
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』内の「Upgrade the Management Center」。
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1』内の「Upgrade the FMC」。
7.0 以前	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0内の「Upgrade Firepower Management Centers」。

Threat Defense

表 *2 : Management Center* を使用した *Threat Defense* のホットフィックス

現在の Management Center のバージョン	ガイド
クラウド提供型の管理センター（バージョンなし）	最新のリリースバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』内の「Upgrade Threat Defense」。
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』内の「Upgrade Threat Defense」。
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1』内の「Upgrade FTD」。
7.0 以前	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0の「Upgrade Firepower Threat Defense」。

表 *3 : Device Manager* を使用した *Threat Defense* のホットフィックス

現在の Threat Defense のバージョン	ガイド
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager』内の「Upgrade Threat Defense」。
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1』内の「Upgrade FTD」。
7.0 以前	『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』内の「System Management」。
バージョン 6.4 以降、CDO 使用	Device Manager を使用して Threat Defense ホットフィックスをインストールします。CDO は使用できません。

NGIPS

表 *4 : NGIPS* デバイスのホットフィックス

現在のマネージャバージョン	プラットフォーム	ガイド
任意	Firepower 7000/8000 シリーズ	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0の「Upgrade Firepower 7000/8000 Series and NGIPSv」。

現在のマネージャバージョン	プラットフォーム	ガイド
任意	FMC を搭載した ASA FirePOWER	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0の「Upgrade ASA with FirePOWER Services」。
任意	ASDM を使用した ASA FirePOWER	Cisco Secure Firewall ASA Upgrade Guideの「Upgrade the ASA FirePOWER Module」。

ホットフィックス成功の確認

ホットフィックスを適用しても、ソフトウェアのバージョンまたはビルドは更新されません。ホットフィックスが正常にインストールされたことを確認するには、Linux シェル（エキスパートモードとも呼ばれる）にアクセスして、次のコマンドを実行します。

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

ソフトウェアが新規にインストールされると、システムは、正常なアップグレード、パッチ、ホットフィックス、およびインストール前のパッケージをすべて一覧表示します。

無応答または失敗したホットフィックス

ホットフィックスのインストール中は、構成の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のホットフィックスを手動でリブート、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。1 つのアプライアンスに対して同じホットフィックスを複数回インストールしないでください。ホットフィックスに失敗する、アプライアンスが応答しないなど、ホットフィックスで問題が発生した場合には Cisco TAC にお問い合わせください。

ホットフィックスのアンインストール

ホットフィックスをアンインストールしようとしないでください。代わりに、Cisco TAC にお問い合わせください。

トラフィック フローとインスペクション

デバイスのホットフィックスは、トラフィックフローとインスペクションに影響を与える可能性があります。ホットフィックスによってデバイスが再起動された場合、または構成の変更を展開する必要がある場合は特に注意が必要です。

デバイスのタイプ、展開のタイプ（スタンドアロン、高可用性、クラスタ化）、およびインターフェイスの構成によって中断の性質が決まります。ホットフィックスのインストールは、保守期間中に行うか、中断による展開環境への影響が最も小さい時点で行うことを強くお勧めします。

トラフィックフローとインスペクションの詳細については、お使いのバージョンの『Cisco Secure Firewall Threat Defense リリースノート』を参照してください。

サポートが必要な場合

オンラインリソース

シスコは、ドキュメント、ソフトウェア、ツールのダウンロードのほか、バグを照会したり、サービスリクエストをオープンしたりするための次のオンラインリソースを提供しています。これらのリソースは、Cisco ソフトウェアをインストールして設定したり、技術的問題を解決したりするために使用してください。

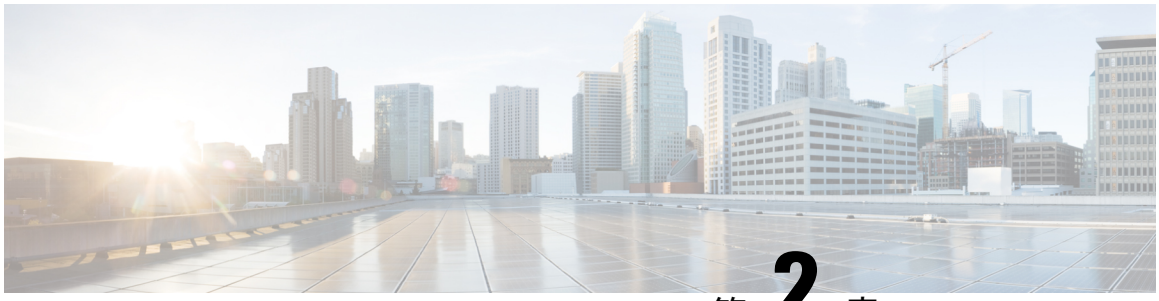
- マニュアル：http://www.cisco.com/go/ftd-docs
- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

シスコ サポートおよびダウンロード サイトの大部分のツールにアクセスする際は、Cisco.com のユーザー ID およびパスワードが必要です。

シスコへのお問い合わせ

上記のオンライン リソースを使用して問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域）：Cisco Worldwide Support の連絡先



第 2 章

利用可能なホットフィックス

これらのリリース ノートでは、公開されているホットフィックスのページをダウンロードするクイックリンクを提供しています。

（注） クイックリンクによっては特定のモデルのダウンロードページにアクセスできない場合があります。ただし、アプライアンスが同じファミリまたはシリーズである限り、ホットフィックスを安全にダウンロードして適用することができます。絶対に確実にしたい場合は、特定のモデルのページを参照してください。

- Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）
- バージョン 7.2.x のホットフィックス （9 ページ）
- バージョン 7.1.x のホットフィックス （10 ページ）
- バージョン 7.0.x のホットフィックス （12 ページ）
- バージョン 6.7.x のホットフィックス （13 ページ）
- バージョン 6.6.x のホットフィックス （17 ページ）
- バージョン 6.5.0 のホットフィックス （20 ページ）
- バージョン 6.4.0 のホットフィックス （23 ページ）
- バージョン 6.3.0 のホットフィックス （26 ページ）
- バージョン 6.2.3 のホットフィックス （29 ページ）
- バージョン 6.2.2 のホットフィックス （34 ページ）
- バージョン 6.2.0 のホットフィックス （36 ページ）
- バージョン 6.1.0 のホットフィックス （40 ページ）
- バージョン 6.0.1 のホットフィックス （43 ページ）
- バージョン 6.0.0 のホットフィックス （44 ページ）
- バージョン 5.4.x のホットフィックス （45 ページ）

Management Center ハードウェアの BIOS およびファームウェアのホットフィックス

Management Center ハードウェアの BIOS および RAID コントローラファームウェアのアップデートを提供します。Management Center が要件を満たしていない場合は、適切なホットフィックスを適用してください。使いの Management Center モデルとバージョンがリストになく、更新が必要だと思われる場合は、Cisco TAC までお問い合わせください。

表 *5: BIOS* およびファームウェアの最小要件

プラットフォーム	バージョン	BIOS	RAID コントローラのファームウェア	CIMC ファームウェア	ホットフィックス
FMC 1600、2600、4600	6.3.0 ～ 7.0	C220M5.4.1.3i.0	51.10.0-3612	4.1（3d）	BIOS のアップデート ホットフィックス EL
FMC 1000、2500、4500	6.2.3 ～ 7.0	C220M4.4.1.2c.0	24.12.1-0456	4.1(2g)	BIOS のアップデート ホットフィックス EL
FMC 2000、4000	6.2.3 ～ 6.6	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS のアップデート ホットフィックス EI
FMC 750、1500、3500	6.2.3 ～ 6.4	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS のアップデート ホットフィックス EI

ホットフィックスは、BIOS および RAID コントローラファームウェアを更新する唯一の方法です。ソフトウェアをアップグレードしても、このタスクは実行されず、新しいバージョンに再イメージ化されません。Management Center がすでに最新の状態である場合、ホットフィックスは効果がありません。

ヒント これらのホットフィックスにより、CIMC ファームウェアも更新されます。解決された問題については、Cisco UCS ラックサーバソフトウェアのリリースノートを参照してください。一般に、CIMC の使用での設定の変更はサポートされていないことに注意してください。Management Centerただし、無効な CIMC ユーザー名のロギングを有効にするには、最新のホットフィックスを適用してから、『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide』バージョン 4.0 以降の「*Viewing Faults and Logs*」の章の手順に従ってください。

シスコ サポートおよびダウンロード サイト へのクイックリンクについては、次の表を参照してください。

（注） Management Center Web インターフェイスは、現在のソフトウェアバージョンとは異なる（通常はそれ以降の）バージョンでこれらのホットフィックスを表示する場合があります。これは予想される動作であり、このホットフィックスは適用しても安全です。

BIOS およびファームウェアバージョンの確認

Management Center での現在のバージョンを確認するには、Linux シェル/エキスパートモードで次のコマンドを実行します。

- BIOS: **sudo dmidecode -t bios -q**
- RAID コントローラファームウェア（FMC 4500）： **sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"**
- RAID コントローラファームウェア（他のすべてのモデル）： **sudo storcli /c0 show | grep "FW Package"**

バージョン 7.2.x のホットフィックス

この表には、公開されているバージョン 7.2.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 *6*：バージョン *7.2.x* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス AW	7.2.4	FirePOWER 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_AW-7.2.4.1-1 FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_AW-7.2.4.1-1 Secure Firewall 3100 シリーズ： 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 FTDv： Cisco_FTD_Hotfix_AW-7.2.4.1-1	CSCwf71606：リロード時に Cisco ASA および FTD ACL がインストールされない
ホットフィックス AN	7.2.4-165	Management Center： Cisco_Secure_FW_Mgmt_Center_Hotfix_AN-7.2.4.1-2 （注） このホットフィックスは、バージョン 7.2.4-165 にのみ適用します。この問題を修正するバージョン 7.2.4-169 には適用しないでください。	CSCwf28592：一部の特定のシナリオでは、オブジェクトオプティマイザによって、デバイスに不適切なルールが展開される可能性がある

バージョン 7.1.x のホットフィックス

この表には、公開されているバージョン 7.1.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 7: バージョン 7.1.x のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス Q	7.1.0.2	Secure Firewall 3100 シリーズ： Cisco_FTD_SSP_FP3K_Hotfix_Q-7.1.0.3-2	CSCwb88651 : Cisco ASA および FTD ソフトウェアの RSA 秘密キーリークの脆弱性 CSCwb28334 : Cisco ASA および FTD ソフトウェアの RSA 秘密キーリークの脆弱性
ホットフィックス P	7.1.0.1	FirePOWER 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_P-7.1.0.2-2 FirePOWER 2100 シリーズ： 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 および FTD ソフトウェアの RSA 秘密キーリークの脆弱性 CSCwb28334 : Cisco ASA および FTD ソフトウェアの RSA 秘密キーリークの脆弱性
ホットフィックス A	7.1.0	FDM を使用した Firepower 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_A-7.1.0.1-7 FDM を使用した Firepower 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_A-7.1.0.1-7 FDM を使用した Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_A-7.1.0.1-7 FDM を使用した ISA 3000： Cisco_FTD_Hotfix_A-7.1.0.1-7 FDM を使用した FTDv： Cisco_FTD_Hotfix_A-7.1.0.1-7 （注） FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。	CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性

バージョン 7.0.x のホットフィックス

この表には、公開されているバージョン 7.0.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 *8* : バージョン *7.0.x* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス DC	7.0.5	FMC： Cisco_Firepower_Mgmt_Center_Hotfix_DC-7.0.5.1-5	CSCwd88641：デバイスモデルと snort エンジンに基づいて VDB パッケージをプッシュするための展開の変更
ホットフィックス S	7.0.1	FDM を使用した Firepower 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_S-7.0.1.1-10 FDM を使用した Firepower 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_S-7.0.1.1-10 FDM を使用した Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_S-7.0.1.1-10 FDM を使用した ASA 5500-X シリーズおよび ISA 3000： Cisco_FTD_Hotfix_S-7.0.1.1-10 FDM を使用した FTDv： Cisco_FTD_Hotfix_S-7.0.1.1-10 （注） このホットフィックスは、2021 年 12 月 19 日にビルド 9 として最初にリリースされました。2021 年 12 月 21 日にビルド 10 として再リリースされました。前のビルドをインストールした場合は、後のビルドをインストールする必要はありません。 FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。	CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性 CSCwa55039 : 7.0.1 用の Firepower Threat Defense ホットフィックス S を 2 回実行するとシステムが失敗する

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス EL	7.0.0 7.0.x 7.0.x.x	FMC（すべてのハードウェアモデル）： Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EL-7 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、およびRAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。

バージョン 6.7.x のホットフィックス

この表には、公開されているバージョン 6.7.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 *9*：バージョン *6.7.x* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス AA	6.7.0.3	FirePOWER 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_AA-6.7.0.4-2 FirePOWER 2100 シリーズ： 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 シリーズおよび ISA 3000： Cisco_FTD_Hotfix_AA-6.7.0.4-2 FTDv： Cisco_FTD_Hotfix_AA-6.7.0.4-2	

ホットフィックス	バージョン	プラットフォーム	解決済み
			CSCvw94160：CIAM：OpenSSL CVE-2020-1971 CSCvx64478：SAML トランザクション中に不要なコンソール出力がある CSCvz70595：SAML ハンドラの処理中に ASA でトレースバックが観察される CSCvz76966：Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアのドメインネームシステム（DNS）DoS の脆弱性 CSCvz81480：IPsec で GCM が使用されている場合、アウトバウンドパケットの IV が Nitrox V プラットフォームで更新されない CSCvz84850：「タイマーサービス」機能により、ASA および FTD のトレースバックとリロードが発生する CSCvz85683：414004 に関する間違った syslog メッセージ形式 CSCvz85913：ASN.1 文字列が、CISCO-SSL-1.0.2 の ASN1_STR として OpenSSL 内で内部的に表される CSCvz89545：アップグレード後の SSL VPN のパフォーマンスの低下と重大な安定性に関する問題 CSCvz92016：AD の有効なユーザーによる ASA 特権昇格 CSCwa04461：Cisco ASA ソフトウェアおよび FTD ソフトウェア リモート アクセスの SSL VPN サービス拒否 CSCwa14485：Cisco Firepower

ホットフィックス	バージョン	プラットフォーム	解決済み
			Threat Defense ソフトウェアで確認されたサービス拒否攻撃に対する脆弱性 CSCwa15185：ASA/FTD：LUA から不要なプロセス呼び出しを削除 CSCwa33898：Cisco 適応型セキュリティアプライアンスのソフトウェア クライアントレス SSL VPN ヒープオーバーフローの脆弱性 CSCwa36678：FMC からの展開中にトレースバックを使用してランダム FTD がリロードされる CSCwa65389：ASDM を介してインターフェイス構成を変更する場合は、Unicorn Admin Handler で ASA トレースバックおよびリロードが発生
ホットフィックス Y	6.7.0.2	FDM を使用した Firepower 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_Y-6.7.0.3-7 FDM を使用した Firepower 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_Y-6.7.0.3-7 FDM を使用した Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_Y-6.7.0.3-7 FDM を使用した ASA 5500-X シリーズおよび ISA 3000： Cisco_FTD_Hotfix_Y-6.7.0.3-7 FDM を使用した FTDv： Cisco_FTD_Hotfix_Y-6.7.0.3-7 （注） FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。	CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス EL	6.7.0 6.7.x.x	FMC（すべてのハードウェアモデル）： Cisco_Firepower_Mgmt_Center_BIOSUPDATE_670_EL-7 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、およびRAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。
ホットフィックス C	6.7.0 6.7.x.x	FTD を使用した ISA 3000： Cisco_FTD_Hotfix_C-6.7.0.999-2	CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある

バージョン 6.6.x のホットフィックス

この表には、公開されているバージョン 6.6.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 *10* : バージョン *6.6.x* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス EB	6.6.7.1	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_EB-6.6.7.2-4	CSCwd88641：デバイスモデルと snort エンジンに基づいて VDB パッケージをプッシュするための展開の変更

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス DE	6.6.5 6.6.5.1	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_DE-6.6.5.2-8 FDM を使用した Firepower 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_DE-6.6.5.2-8 FDM を使用した Firepower 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_DE-6.6.5.2-8 FDM を使用した Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_DE-6.6.5.2-8 FDM を使用した ASA 5500-X シリーズおよび ISA 3000： Cisco_FTD_Hotfix_DE-6.6.5.2-8 FDM を使用した FTDv： Cisco_FTD_Hotfix_DE-6.6.5.2-8 ASDM を搭載した ASA FirePOWER： Cisco_Network_Sensor_Hotfix_DE-6.6.5.2-8 （注） FMC と、FDM、FDM/CDO、および ASDM 管理対象デバイスにのみこのホットフィックスを適用してください。FMC 管理対象デバイスには、FMC ホットフィックスによって対応します。	CSCwa70008：期限切れの証明書がセキュリティ Intel を引き起こし、マルウェアファイルの事前分類署名の更新が失敗する

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス DA	6.6.5.1	FDM を使用した Firepower 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_DA-6.6.5.2-4 FDM を使用した Firepower 2100 シリーズ Cisco_FTD_SSP_FP2K_Hotfix_DA-6.6.5.2-4 FDM を使用した Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_DA-6.6.5.2-4 FDM を使用した ASA 5500-X シリーズおよび ISA 3000： Cisco_FTD_Hotfix_DA-6.6.5.2-4 FDM を使用した FTDv： Cisco_FTD_Hotfix_DA-6.6.5.2-4 （注） FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。	CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性
ホットフィックス 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 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。
ホットフィックス EI	6.6.0 6.6.x 6.6.x.x	FMC 2000、4000： Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EI-15 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス AB	6.6.1	FTD を使用した ISA 3000： Cisco_FTD_Hotfix_AB-6.6.1.999-1	CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある
ホットフィックス N	6.6.0 6.6.0.x	FTD を使用した ISA 3000： Cisco_FTD_Hotfix_N-6.6.0.999-1	CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある

バージョン 6.5.0 のホットフィックス

この表では、公開されているバージョン 6.5.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 *11* : バージョン *6.5.0* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス EL	6.5.0 6.5.0	FMC 1000、1600、2500、2600、4500、4600： Cisco_Firepower_Mgmt_Center_BIOSUPDATE_650_EL-7 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス EI	6.5.0 6.5.0	FMC 2000、4000： Cisco_Firepower_Mgmt_Center_BIOSUPDATE_650_EI-15 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、およびRAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。
ホットフィックス T	6.5.0 6.5.0	FTD を使用した ISA 3000： Cisco_FTD_Hotfix_T-6.5.0.999-1	CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある
ホットフィックス O	6.5.0.4	FirePOWER 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_O-6.5.0.5-3 FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_O-6.5.0.5-3 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_O-6.5.0.5-3 FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 Cisco_FTD_Hotfix_O-6.5.0.5-3 FTDv： Cisco_FTD_Hotfix_O-6.5.0.5-3	CSCvt03598：Cisco ASA ソフトウェアおよび FTD ソフトウェア Web サービスの読み取り専用パストラバーサルの脆弱性

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス H	6.5.0.4	FirePOWER 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_H-6.5.0.5-2 FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_H-6.5.0.5-2 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_H-6.5.0.5-2 FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 Cisco_FTD_Hotfix_H-6.5.0.5-2 FTDv： Cisco_FTD_Hotfix_H-6.5.0.5-2	CSCvp93468：Cisco ASA ソフトウェアと Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性 CSCvr92168：OSPF Hello 処理時に OSPF プロセスで ASA/FTD の低速メモリリークが生じる CSCvs10748：Cisco 適応型アプライアンスおよび Firepower Threat Defense におけるサービス拒否攻撃に対する脆弱性 CSCvs50459：Cisco ASA および Cisco FTD の不正な OSPF パケット処理によるサービス拒否攻撃に対する脆弱性 CSCvt15163：Cisco ASA および FTD ソフトウェアの Web サービスに関する情報漏洩の脆弱性 CSCvu20521：HF のインストール後に OSPF が構成されない
ホットフィックス D	6.5.0.2	FirePOWER 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_D-6.5.0.3-3 FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_D-6.5.0.3-3 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_D-6.5.0.3-3 FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 Cisco_FTD_Hotfix_D-6.5.0.3-3 FTDv： Cisco_FTD_Hotfix_D-6.5.0.3-3	CSCvs55990：ローカル/FDM で管理されている FTD 上に設定された SI DNS を使用した展開が失敗する

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス B	6.5.0 6.5.0.1 および 6.5.0.2	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_B-6.5.0.3-3 （注） VDB 329+に更新し、設定の変更を展開する必要もあります。この操作は、ホットフィックスを適用する前または後に実行できます。	アプリケーション ID に関する問題を解決します。
ホットフィックス C	6.5.0.1	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_C-6.5.0.2-2	CSCvr52109：FTD のアクセスリストにはヒットカウントがあるが、トラフィックがアクセスポリシールールにヒットしていない

バージョン 6.4.0 のホットフィックス

この表では、公開されているバージョン 6.4.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 *12*：バージョン *6.4.0* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス EP	6.4.0.13	FDM を使用した Firepower 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_EP-6.4.0.14-9 FDM を使用した Firepower 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_EP-6.4.0.14-9 FDM を使用した ASA 5500-X シリーズおよび ISA 3000： Cisco_FTD_Hotfix_EP-6.4.0.14-9 FDM を使用した FTDv： Cisco_FTD_Hotfix_EP-6.4.0.14-9 （注） FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。	CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス EL	6.4.0 6.4.0	FMC 1000、1600、2500、2600、4500、4600： Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EL-7 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。
ホットフィックス EI	6.4.0 6.4.0	FMC 750、1500、2000、3500、4000： Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EI-15 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。
ホットフィックス DV	6.4.0 6.4.0	FTD を使用した ISA 3000： Cisco_FTD_Hotfix_DV-6.4.0.999-1	CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある
ホットフィックス BM	6.4.0.9	FirePOWER 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_BM-6.4.0.10-2 FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_BM-6.4.0.10-2 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_BM-6.4.0.10-2 FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 Cisco_FTD_Hotfix_BM-6.4.0.10-2 FTDv： Cisco_FTD_Hotfix_BM-6.4.0.10-2	CSCvt03598：Cisco ASA ソフトウェアおよび FTD ソフトウェア Web サービスの読み取り専用パストラバーサルの脆弱性

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス AY	6.4.0.8	FirePOWER 1000 シリーズ： Cisco_FTD_SSP_FP1K_Hotfix_AY-6.4.0.9-3 FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_AY-6.4.0.9-3 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_AY-6.4.0.9-3 FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 Cisco_FTD_Hotfix_AY-6.4.0.9-3 FTDv： Cisco_FTD_Hotfix_AY-6.4.0.9-3 （注） このホットフィックスを適用する代わりに、バージョン 6.4.0.9 以上にパッチを適用することを推奨します。パッチを適用できない場合は、このホットフィックスは最初にビルド 2 として 2020 年 5 月 6 日にリリースされ、2020 年 5 月 15 日にビルド 3 として再リリースされたことに注意してください。以前のビルドをインストールしている場合は、新しいビルドもインストールしてください。アンインストールする必要はありません。	CSCvp49481、CSCvp93468：Cisco ASA ソフトウェアおよび Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性 CSCvs10748：Cisco 適応型アプライアンスおよび Firepower Threat Defense におけるサービス拒否攻撃に対する脆弱性 CSCvo80853：Cisco Firepower Threat Defense ソフトウェアのパケットにおけるサービス拒否攻撃に対する脆弱性 CSCvs50459：Cisco ASA および Cisco FTD の不正な OSPF パケット処理によるサービス拒否攻撃に対する脆弱性 CSCvr86783：HA の構成後にスタンバイ FDM の接続が失われる CSCvr92168：OSPF Hello 処理時に OSPF プロセスで ASA/FTD の低速メモリリークが生じる CSCvt15163：Cisco ASA および FTD ソフトウェアの Web サービスに関する情報漏洩の脆弱性 CSCvq89361：Cisco Firepower 1000 シリーズの SSL/TLS におけるサービス拒否攻撃に対する脆弱性 CSCvu20521：HF のインストール後に OSPF が構成されない
ホットフィックス U	6.4.0.5 および 6.4.0.6	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_U-6.4.0.7-2	CSCvr95287：Cisco Firepower Management Center LDAP 認証バイパスの脆弱性
ホットフィックス T	6.4.0 6.4.0.1 ～ 6.4.0.4	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_T-6.4.0.5-1	CSCvr95287：Cisco Firepower Management Center LDAP 認証バイパスの脆弱性

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス AA	6.4.0.4 ～ 6.4.0.7	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_AA-6.4.0.8-4 （注） VDB 329+ に更新し、設定の変更を展開する必要もあります。この操作は、ホットフィックスを適用する前または後に実行できます。	アプリケーション ID に関する問題を解決します。
ホットフィックス X	6.4.0.6	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_X-6.4.0.7-2	CSCvr52109：FTD のアクセスリストにはヒットカウントがあるが、トラフィックがアクセスポリシールールにヒットしていない
ホットフィックス F	6.4.0.2	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_F-6.4.0.3-2 FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_F-6.4.0.3-2 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_F-6.4.0.3-2 FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 Cisco_FTD_Hotfix_F-6.4.0.3-2 FTDv（VMware、FVM）： Cisco_FTD_Hotfix_F-6.4.0.3-2	CSCvq34224：マネージャをアップグレードすると、Firepower プライマリ検出エンジン プロセスが終了する。

バージョン 6.3.0 のホットフィックス

この表では、公開されているバージョン 6.3.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 *13* : バージョン *6.3.0* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス EL	6.3.0 6.3.0.x	FMC 1000、1600、2500、2600、4500、4600： Cisco_Firepower_Mgmt_Center_BIOSUPDATE_630_EL-7 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。
ホットフィックス EI	6.3.0 6.3.0.x	FMC 750、1500、2000、3500、4000： Cisco_Firepower_Mgmt_Center_BIOSUPDATE_630_EI-15 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。
ホットフィックス AZ	6.3.0 6.3.0.x	FTD を使用した ISA 3000： Cisco_FTD_Hotfix_AZ-6.3.0.999-1	CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある
ホットフィックス AV	6.3.0.5	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_ AV-6.3.0.6-3 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_ AV-6.3.0.6-3 FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 Cisco_FTD_Hotfix_AV-6.3.0.6-3 FTDv： Cisco_FTD_Hotfix_AV-6.3.0.6-3	CSCvt03598：Cisco ASA ソフトウェアおよび FTD ソフトウェア Web サービスの読み取り専用パストラバーサルの脆弱性

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス AO	6.3.0.5	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_ AO-6.3.0.6-2 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_ AO-6.3.0.6-2 FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 Cisco_FTD_Hotfix_AO-6.3.0.6-2 FTDv： Cisco_FTD_Hotfix_AO-6.3.0.6-2	CSCvp93468：Cisco ASA ソフトウェアと Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性 CSCvo80853：Cisco Firepower Threat Defense ソフトウェアのパケットにおけるサービス拒否攻撃に対する脆弱性 CSCvr07419 CSCvs50459：Cisco ASA および Cisco FTD の不正な OSPF パケット処理によるサービス拒否攻撃に対する脆弱性 CSCvs10748：Cisco 適応型アプライアンスおよび Firepower Threat Defense におけるサービス拒否攻撃に対する脆弱性 CSCvp49481：Cisco ASA ソフトウェアと Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性 CSCvt15163：Cisco ASA および FTD ソフトウェアの Web サービスに関する情報漏洩の脆弱性 CSCvr55825：Cisco ASA および FTD ソフトウェアのパストラバーサルの脆弱性
ホットフィックス AI	6.3.0 6.3.0.1 ～ 6.3.0.5	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_AI-6.3.0.6-2	CSCvr95287：Cisco Firepower Management Center LDAP 認証バイパスの脆弱性
ホットフィックス AK	6.3.0.5	FMC/FMCv： Cisco_Firepower_Mgmt_Center_Hotfix_AK-6.3.0.6-2 （注） VDB 329+ に更新し、設定の変更を展開する必要もあります。この操作は、ホットフィックスを適用する前または後に実行できます。	アプリケーション ID に関する問題を解決します。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス AA	6.3.0.3	ASA 5508-X および FTD 搭載の ASA 5516-X： Cisco_FTD_Hotfix_AA-6.3.0.4-2	CSCvp36425：Cisco ASA & FTD ソフトウェアの暗号化 TLS および SSL ドライバにおけるサービス拒否攻撃に対する脆弱性
ホットフィックス W	6.3.0.3	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_W-6.3.0.4-4	CSCvn77248：シスコ セキュアブート ハードウェアにおける改ざんの脆弱性
ホットフィックス B	6.3.0	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_B-6.3.0.1-1 （注） 複数のインスタンス（1 つのセキュリティ モジュールに複数の論理デバイス）を設定している場合は、このホットフィックスを適用しないでください。	CSCvo02577：SSL HW 復号化によるバッファ枯渇

バージョン 6.2.3 のホットフィックス

この表では、公開されているバージョン 6.2.3 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 *14 :* バージョン *6.2.3* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス EM	6.2.3.17	FDM を使用した Firepower 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_EM-6.2.3.18-13 FDM を使用した ASA 5500-X シリーズおよび ISA 3000： Cisco_FTD_Hotfix_EM-6.2.3.18-13 FDM を使用した FTDv： Cisco_FTD_Hotfix_EM-6.2.3.18-13 （注） FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。	CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス EL	6.2.3 6.2.3.x	FMC 1000、2500、4500： Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EL-7 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。
ホットフィックス EI	6.2.3 6.2.3.x	FMC 750、1500、2000、3500、4000： Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EI-15 （注） このホットフィックスにより、これらの Management Center モデルに対する他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。	BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。 Management Center ハードウェアの BIOS およびファームウェアのホットフィックス （8 ページ）を参照してください。
ホットフィックス EH	6.2.3 6.2.3.x	FTD を搭載した ASA 5506-X シリーズ： Cisco_FTD_Hotfix_EH-6.2.3.999-6	CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス DT	6.2.3.15	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_DT-6.2.3.16-3 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_DT-6.2.3.16-3 FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 Cisco_FTD_Hotfix_DT-6.2.3.16-3 FTDv： Cisco_FTD_Hotfix_DT-6.2.3.16-3	CSCvr55825：Cisco ASA および FTD ソフトウェアのパストラバーサルの脆弱性 CSCvp49481、CSCvp93468：Cisco ASA ソフトウェアおよび Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性 CSCvp16945、CSCvp16949：Cisco ASA ソフトウェアおよび Cisco FTD ソフトウェアの MGCP におけるサービス拒否攻撃に対する脆弱性 CSCvo62077：Cisco Firepower Threat Defense ソフトウェアの VPN システムロギングにおけるサービス拒否攻撃に対する脆弱性 CSCvs10748：Cisco 適応型アプライアンスおよび Firepower Threat Defense におけるサービス拒否攻撃に対する脆弱性 CSCvs50459：Cisco ASA および Cisco FTD の不正な OSPF パケット処理によるサービス拒否攻撃に対する脆弱性 CSCvo80853：Cisco Firepower Threat Defense ソフトウェアのパケットにおけるサービス拒否攻撃に対する脆弱性 CSCvr07419：Cisco ASA および FTD ソフトウェアの IPv6 DNS におけるサービス拒否攻撃に対する脆弱性 CSCvt15163：Cisco ASA および FTD ソフトウェアの Web サービスに関する情報漏洩の脆弱性

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス DW	6.2.3.15	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_DW-6.2.3.16-6 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_DW-6.2.3.16-6 FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 Cisco_FTD_Hotfix_DW-6.2.3.16-6 FTDv： Cisco_FTD_Hotfix_DW-6.2.3.16-6	CSCvs84578：4100/9300 プラットフォーム上の FTD を 6.2.3.15 にアップグレードすると、SSHD が破損し、FTD インスタンスの起動が妨げられる CSCvs84713：ASA55XX/ISA 3000/FTDv 上の FTD を 6.2.3.15 ビルド 38 にアップグレードした後、デバイスに SSH 接続できない CSCvs95725：6.2.3.15 で実行されている仮想 FTD が SSH 要求をブロックし、FMC との接続を失う
ホットフィックス DO	6.2.3 6.2.3.1 ～ 6.2.3.15	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_DO-6.2.3.16-3	CSCvr95287：Cisco Firepower Management Center LDAP 認証バイパスの脆弱性
ホットフィックス DQ	6.2.3.15	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_DQ-6.2.3.16-2 （注） VDB 329+ に更新し、設定の変更を展開する必要もあります。この操作は、ホットフィックスを適用する前または後に実行できます。	アプリケーション ID に関する問題を解決します。
ホットフィックス CY	6.2.3.14	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_CY-6.2.3.15-2	CSCvq34224：マネージャをアップグレードすると、Firepower プライマリ検出エンジン プロセスが終了する。
ホットフィックス CK	6.2.3.12	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_CK-6.2.3.13-1	CSCvn77248：シスコ セキュア ブート ハードウェアにおける改ざんの脆弱性
ローカルマルウェア証明書のホットフィックス	6.2.3 6.2.3.x	FMC/FMCv： Hotfix_Local_Malware_Cert-6.2.3.999-4	CSCvm81052：証明書チェーンが無効であるため、ローカル マルウェア検出の更新が FMC にダウンロードされない。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス H	6.2.3 6.2.3.1 ～ 6.2.3.3	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_H-6.2.3.999-5 Firepower 7000/8000 シリーズ： 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 デバイスは Threat Grid 証明書を信頼する必要があります。
ホットフィックス G	6.2.3 6.2.3.1 ～ 6.2.3.3	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_G-6.2.3.999-6 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_G-6.2.3.999-6 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_G-6.2.3.999-6 FTDv（VMware、KVM、AWS）： Cisco_FTD_Hotfix_G-6.2.3.999-6	CSCvj07038：Firepower デバイスは Threat Grid 証明書を信頼する必要があります。
ホットフィックス T	6.2.3.1 ～ 6.2.3.3	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_T-6.2.3.4-4	CSCvk06176：実行ファイルが誤っているため SSEConnector が起動しない。
ホットフィックス A	6.2.3	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_A-6.2.3.1-10 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_A-6.2.3.1-10 FTD を搭載した ASA 5500-X シリーズ： 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、および AnyConnect セキュリティ モビリティ クライアントの SAML 認証セッションの固定における脆弱性。 CSCvi16029: ASA Web インターフェイス認証のバイパス。

バージョン 6.2.2 のホットフィックス

この表では、公開されているバージョン 6.2.2 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 *15 :* バージョン *6.2.2* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス CB	6.2.2.5	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_CB-6.2.2.6-2	CSCvn77248：シスコ セキュアブート ハードウェアにおける改ざんの脆弱性
ホットフィックス BY	6.2.2 6.2.2.x	FMC（すべてのハードウェアモデル）： Sourcefire_3D_Defense_Center_S3_Hotfix_BY-6.2.2.999-1	RAID コントローラのファームウェアを更新します。
ローカルマルウェア証明書のホットフィックス	6.2.2 6.2.2.x	FMC/FMCv： Hotfix_Local_Malware_Cert-6.2.2.999-4 （注） バージョン 6.2.3 にアップグレードした後、新しいローカルマルウェア証明書のホットフィックスを適用する必要があります。	CSCvm81052：証明書チェーンが無効であるため、ローカル マルウェア検出の更新が FMC にダウンロードされない。
ホットフィックス BZ	6.2.2.4	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_BZ-6.2.2.5-4 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_BZ-6.2.2.5-4 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_BZ-6.2.2.5-4 FTDv（VMware、KVM、AWS）： Cisco_FTD_Hotfix_BZ-6.2.2.5-4	CSCvm43975：SIP インスペクションの脆弱性による Cisco ASA および FTD のサービス拒否または高 CPU。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス BN	6.2.2 6.2.2.1 ～ 6.2.2.4	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_BN-6.2.2.999-5 FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_BN-6.2.2.999-5 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_BN-6.2.2.999-5 FTD を搭載した ASA 5500-X シリーズ： 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 シリーズ： 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 デバイスは Threat Grid 証明書を信頼する必要があります。
ホットフィックス BS	6.2.2.4	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_BS-6.2.2.5-3	CSCvk17382：ルールの評価の処理中に Snort が予期せず終了する
ホットフィックス BD	6.2.2.2	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_BD-6.2.2.3-4 Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_BD-6.2.2.3-4 FTD を搭載した ASA 5500-X シリーズ： 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、および AnyConnect セキュリティ モビリティ クライアントの SAML 認証セッションの固定における脆弱性。 CSCvi16029: ASA Web インターフェイス認証のバイパス。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス AO	6.2.2.1	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_AO-6.2.2.2-1 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_AO-6.2.2.2-1 FTDv： Cisco_FTD_Hotfix_AO-6.2.2.2-1 （注） ホットフィックス AB はホットフィックス AO に置換されます。ホットフィックス AB をインストールしている場合は、ホットフィックス AO をインストールする必要があります。	CSCvg35618：Cisco 適応型セキュリティ アプライアンスの Remote Code Execution とサービス拒否攻撃に対する脆弱性。 CSCvh79732、CSCvh81737、CSCvh81870：Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性。
ホットフィックス AN	6.2.2.1	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_AN-6.2.2.2-4 （注） ホットフィックス AC はホットフィックス AN に置換されます。ホットフィックス AC をインストールしている場合は、ホットフィックス AN をインストールする必要があります。	CSCvg35618：Cisco 適応型セキュリティ アプライアンスの Remote Code Execution とサービス拒否攻撃に対する脆弱性。 CSCvh79732、CSCvh81737、CSCvh81870：Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性。
ホットフィックス Z	6.2.2 6.2.2.1	FTDv： Cisco_FTD_Hotfix_Z-6.2.2.2-7	CSCvg68914：TCP トラフィック処理中（StreamQueue）のセグメンテーション違反。
ホットフィックス D	6.2.2	FirePOWER 2100 シリーズ： Cisco_FTD_SSP_FP2K_Hotfix_D-6.2.2.1-4	CSCvg06695：検出サービス モジュールの障害により FP2100 Threat Defense ペアがステータスのレポートに失敗する。

バージョン 6.2.0 のホットフィックス

この表では、公開されているバージョン 6.2.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 *16 :* バージョン *6.2.0* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ローカルマルウェア証明書のホットフィックス	6.2.0 6.2.0.x	FMC/FMCv： Hotfix_Local_Malware_Cert-6.2.0.999-1 （注） バージョン 6.2.2 または 6.2.3 にアップグレードした後、新しいローカル マルウェア証明書のホットフィックスを適用する必要があります。	CSCvm81052：証明書チェーンが無効であるため、ローカル マルウェア検出の更新が FMC にダウンロードされない。
ホットフィックス CE	6.2.0.6	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_CE-6.2.0.7-1 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_CE-6.2.0.7-1 FTDv： Cisco_FTD_Hotfix_CE-6.2.0.7-1	CSCvm43975：SIP インスペクションの脆弱性による Cisco ASA および FTD のサービス拒否または高 CPU。
ホットフィックス BX	6.2.0 6.2.0.1 ～ 6.2.0.5	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_BX-6.2.0.999-5 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_BX-6.2.0.999-5 FTDv： Cisco_FTD_Hotfix_BX-6.2.0.999-5	CSCvj07038：Firepower デバイスは Threat Grid 証明書を信頼する必要があります。
ホットフィックス BW	6.2.0 6.2.0.1 ～ 6.2.0.5	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_BW-6.2.0.999-6 Firepower 7000/8000 シリーズ： 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 デバイスは Threat Grid 証明書を信頼する必要があります。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス BN	6.2.0.4	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_BN-6.2.0.5-3 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_BN-6.2.0.5-3 FTDv： Cisco_FTD_Hotfix_BN-6.2.0.5-3	CSCvg35618：Cisco 適応型セキュリティ アプライアンスの Remote Code Execution とサービス拒否攻撃に対する脆弱性。 CSCvh79732、CSCvh81737、CSCvh81870：Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性。
ホットフィックス BH	6.2.0.3	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_BH-6.2.0.4-1	CSCvg32885：6.2.0.3 にアップグレードした後、一部のアクセス コントロール ルールの欠落で編集または展開ができない。
ホットフィックス AQ	6.2.0.2	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_AQ-6.2.0.3-3	CSCve82386：Threat Defense クラスタでの診断ポート チャネル インターフェイスの IP プールの設定に失敗する。
ホットフィックス U	6.2.0.1	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_U-6.2.0.2-1	CSCve44987：eStreamer サービスが破損したメッセージと、接続されていない状態のスパム ログ ファイルを送信する。
ホットフィックス S	6.2.0.1	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_S-6.2.0.2-1	CSCve35816：handle_host_address_changes() の null ポインタの逆参照による SFDataCorrelator segfault。
ホットフィックス N	6.2.0	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_N-6.2.0.1-1 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_N-6.2.0.1-1 FTDv： Cisco_FTD_Hotfix_N-6.2.0.1-1	CSCve02069：Cisco FirePOWER の検出エンジンの SSL 復号時のメモリ使用による Denial of Service（DoS）の脆弱性。
ホットフィックス G	6.2.0	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_G-6.2.0.1-4	CSCvd27278：インポート リスト内のユーザーのいずれかが削除されていると、UIMP はすべてのユーザーのインポートに失敗する。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス F	6.2.0	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_F-6.2.0.1-3 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_F-6.2.0.1-3 FTDv： Cisco_FTD_Hotfix_F-6.2.0.1-3	CSCvc96586: 9K ブロック カウンタには Snort へパンとされたトラフィックを停止し、Snort をビジー状態にする問題がある。
ホットフィックス B	6.2.0	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_B-6.2.0.1-2	CSCvc57533：デルタ スプリットの論理障害によりポリシーの展開が失敗する場合がある。
ホットフィックス AM	6.2.0.2	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_AM-6.2.0.3-3 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_AM-6.2.0.3-3 FTDv： Cisco_FTD_Hotfix_AM-6.2.0.3-3	CSCve04326：スタンバイは出力インターフェイスがダウンしているときのトラフィックの転送にブラックホールではなく CCL を使用する必要があります。
ホットフィックス AG	6.2.0 6.2.0.1	FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_AG-6.2.0.2-3	CSCve95026：UUID が EOAttributes にないと、Threat Defense デバイスで ids_event_alertercauses により CPU 使用率が高くなる。
ホットフィックス AC	6.2.0.2	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_AC-6.2.0.3-2 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_AC-6.2.0.3-2 FTDv： Cisco_FTD_Hotfix_AC-6.2.0.3-2	CSCve71661：Firepower Threat Defense：マルチキャストと BPDU トラフィックが dst-l2_lookup-fail によりドロップされる。
ホットフィックス AU	6.2.0 6.2.0.1 ～ 6.2.0.3	FMC 1000、2500、4500： Sourcefire_3D_Defense_Center_S3_Hotfix_AU-6.2.0.4-1	CSCvf77493：Firepower Management Center 4500、2500、または 1000 上で管理インターフェイスが見つからない。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス A	6.2.0	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_A-6.2.0.1-10 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_A-6.2.0.1-10 ASDM を搭載した ASA FirePOWER： Cisco_Network_Sensor_Hotfix_A-6.2.0.1-10	CSCvc88603：地理位置情報を使用しているすべてのポリシーがトラフィックをブロックしている。

バージョン 6.1.0 のホットフィックス

この表では、公開されているバージョン 6.1.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 *17*：バージョン *6.1.0* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス ES	6.1.0 6.1.0.1 ～ 6.1.0.7	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_ES-6.1.0.8-2	CSCvr95287：Cisco Firepower Management Center LDAP 認証バイパスの脆弱性
ローカルマルウェア証明書のホットフィックス	6.1.0 6.1.0.x	FMC/FMCv： Hotfix_Local_Malware_Cert-6.1.0.999-1.sh （注） バージョン 6.2.0 または 6.2.3 にアップグレードした後、新しいローカル マルウェア証明書のホットフィックスを適用する必要があります。	CSCvm81052：証明書チェーンが無効であるため、ローカル マルウェア検出の更新が FMC にダウンロードされない。
ホットフィックス EM	6.1.0 6.1.0.1 ～ 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 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_EM-6.1.0.999-51 FTDv： Cisco_FTD_Hotfix_EM-6.1.0.999-51	CSCvj07038：Firepower デバイスは Threat Grid 証明書を信頼する必要があります。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス ER	6.1.0.7	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_ER-6.1.0.8-1.sh FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_ER-6.1.0.8-1.sh FTDv： Cisco_FTD_Hotfix_ER-6.1.0.8-1.sh	CSCvm43975：SIP インスペクションの脆弱性による Cisco ASA および FTD のサービス拒否または高 CPU。
ホットフィックス EI	6.1.0.6	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_EI-6.1.0.7-2 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_EI-6.1.0.7-2 FTDv： Cisco_FTD_Hotfix_EI-6.1.0.7-2 （注） ホットフィックス DZ はホットフィックス EI に置換されます。ホットフィックス DZ をインストールしている場合は、ホットフィックス EI もインストールする必要があります。	CSCvg35618：Cisco 適応型セキュリティ アプライアンスの Remote Code Execution とサービス拒否攻撃に対する脆弱性。 CSCvh95456、CSCvh23085：Cisco 適応型セキュリティ アプライアンスのアプリケーション レイヤ プロトコルのインスペクションにおける DoS に対する脆弱性。 CSCvh79732：Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性。 CSCvi16029：Cisco 適応型セキュリティ アプライアンスの WebVPN におけるサービス拒否攻撃に対する脆弱性。
ホットフィックス CF	6.1.0.1 6.1.0.2	Firepower 4100/9300 Cisco_FTD_SSP_Hotfix_CF-6.1.0.3-3 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_CF-6.1.0.3-3 FTDv： Cisco_FTD_Hotfix_CF-6.1.0.3-3	CSCvd78303：バージョン 6.1.0.1 またはバージョン 6.1.0.2 を実行している Firepower Threat Defense デバイスが、稼働時間が 213 日後にトラフィックの受け渡しを停止し、接続の制限からトラフィックの停止に至るまでの問題が発生した。
ホットフィックス DH	6.1.0.5	FirePOWER 8000 シリーズ： Sourcefire_3D_Device_S3_Hotfix_DH-6.1.0.6-48	CSCvf66660：ハイアベイラビリティ環境で設定されたクラスタ化 Firepower 8000 シリーズ スタックをバージョン 6.1.0.5 に更新すると、ピアに継続的なフェールオーバーが発生する。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス DQ	6.1.0.5	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_DQ-6.1.0.6-1	CSCve82410：TCP、UDP、ICMP、または IP スキャンをブロックするように設定された侵入ポリシーを展開すると、Firepower Management Center はポート スキャンを検出しても、ブロックが必要な場合にブロックしない。
ホットフィックス AJ	6.1.0 6.1.0.1	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_AJ-6.1.0.2-1	CSCvb96776：Firepower Management Center ハイアベイラビリティ ペアをバージョン 6.1.0 以降からバージョン 6.2.0 への正常な更新に失敗した後、ハイアベイラビリティの同期の再確立に失敗した。
ホットフィックス AZ	6.1.0.2	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_AZ-6.1.0.3-1	CSCvd10943：同じ侵入ポリシーを参照する 2 つ以上のアクセス コントロール ルールを含んでいるアクセス コントロール ポリシーを展開したが、バージョン 6.1.0.2 を実行している Firepower Management Center とは異なる変数セットを使用している場合、展開に失敗した。
ホットフィックス AI	6.1.0	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_AI-6.1.0.2-3	CSCvc49789：最適化コンポーネントが誤ったデータベースに接続しようとすると CPU 使用率の上昇や全般的なパフォーマンスの低下などのシステムの問題が発生した。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス AF	6.1.0	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_AF-6.1.0.2-1 Firepower 7000/8000 シリーズ 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：Firepower 8350 デバイスまたはAMP8350デバイスがシリアル ポート コンソール、または、有効にしていた場合はLights-out管理（LOM）コンソールで異常に大きなメッセージのストリームを生成した場合にデバイスが応答しなくなった。

バージョン 6.0.1 のホットフィックス

この表では、公開されているバージョン 6.0.1 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 *18 :* バージョン *6.01* ホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス BH	6.0.1.4	Firepower 4100/9300： Cisco_FTD_SSP_Hotfix_BH-6.0.1.5-1 FTD を搭載した ASA 5500-X シリーズ： Cisco_FTD_Hotfix_BH-6.0.1.5-1 FTDv： Cisco_FTD_Hotfix_BH-6.0.1.5-1	CSCvg35618：Cisco適応型セキュリティ アプライアンスの Remote Code Execution とサービス拒否攻撃に対する脆弱性。 CSCvh79732、CSCvh81870：Cisco適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性。
ローカルマルウェア証明書のホットフィックス	6.0.1 6.0.1.x	FMC/FMCv： Hotfix_Local_Malware_Cert-6.0.1.999-1 （注） バージョン6.1にアップグレードした後、新しいローカル マルウェア証明書のホットフィックスを適用する必要があります。	CSCvm81052：証明書チェーンが無効であるため、ローカル マルウェア検出の更新がFMCにダウンロードされない。

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス AU	6.0.1.1	Firepower 7000/8000 シリーズ： Sourcefire_3D_Device_S3_Hotfix_AU-6.0.1.3-1	CSCvc26880：場合によっては、シリーズ 3 デバイスがシリアル ポート コンソール、または、有効にしていた場合は Lights-out 管理（LOM）コンソールで異常に大きなメッセージのストリームを生成した場合にデバイスが応答しなくなる。

バージョン 6.0.0 のホットフィックス

この表では、公開されているバージョン 6.0.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 *19*：バージョン *6.0.0* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ローカルマルウェア証明書のホットフィックス	6.0.0 6.0.0.1	FMC/FMCv： Hotfix_Local_Malware_Cert-6.0.0.999-1 （注） バージョン 6.0.1 にアップグレードした後、新しいローカルマルウェア証明書のホットフィックスを適用する必要があります。	CSCvm81052：証明書チェーンが無効であるため、ローカル マルウェア検出の更新が FMC にダウンロードされない。
ホットフィックス O	6.0.0.1	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_O-6.0.0.999-1 ASDM を搭載した ASA FirePOWER： Cisco_Network_Sensor_Hotfix_O-6.0.0.0.999-1	CSCuy99274：Firepower Management Center またはローカル管理のいずれかからセキュリティ ゾーンで設定された ASA Firepower モジュールにアクセス コントロール ルールを展開した場合、システムは誤った順序で制御ルールを展開し、必要な設定でトリガーされることがないルールを着信トラフィックがトリガーされる。
ホットフィックス K	6.0.0.1	FMC/FMCv： Sourcefire_3D_Defense_Center_S3_Hotfix_K-6.0.0.2-3	CSCuy60529：SRU の更新後、新しい共有オブジェクト ルールがセンサーにプッシュされない。

バージョン 5.4.x のホットフィックス

この表には、公開されているバージョン 5.4.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 *20* : バージョン *5.4.x* のホットフィックス

ホットフィックス	バージョン	プラットフォーム	解決済み
ホットフィックス CX	5.4.1.8	ASA FirePOWER（ASA 5506-X シリーズ、5508-X、5516-X、ISA 3000）： Cisco_Network_Sensor_Hotfix_CX-5.4.1.9-1	CSCuv11738：リモート NTP サーバーを使用して、バージョン 5.4 よりも前のバージョンを実行している登録済みの ASA FirePower モジュールとシステムの時刻を同期するように設定している場合にうるう秒が発生すると、システムが CPU を大量に使用する可能性がある。
ホットフィックス DK	5.4.0.9	Firepower 7000/8000 シリーズ： 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：過剰なロギングによって、ディスク領域の問題、パフォーマンスの低下、およびストレージの制限が発生する。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。