Cisco Firepower Management Center および Firepower システム ソフトウェア Sourcefire トンネル 制御通信路コマンドの実行脆弱性

Medium	**アドバイザリーID :** cisco-sa-20181003-fp-cmd-injection **初公開日 :** 2018-10-03 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 8.2 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvg46466	CVE-2018-0453

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

on Cisco 同じ Cisco FMC によって制御される Firepower Threat Defense （FTD）センサーを実行する Cisco Firepower システム ソフトウェアの Sourcefire トンネル 制御通信路 プロトコルの脆弱性は Cisco Firepower Management Center （FMC）の、または他の Firepower センサーの Cisco FMC を通した *ルート 特権*の特定の CLI コマンドを実行する認証された、ローカル攻撃者をおよびデバイスを可能にする可能性があります。 コマンドを送信 するために、攻撃者は少なくとも 1 台の影響を受けたセンサーまたは Cisco FMC のための *ルート 特権*がなければなりません。

影響を受けたソフトウェアが不十分行うので存在 する脆弱性はある特定の CLI コマンドがあるようにコマンドが Sourcefire トンネル接続によって実行される場合、確認します。 攻撃者は Firepower センサーか Cisco FMC に *ルート 特権*との認証、および Sourcefire トンネル接続によって別の Firepower センサーへ Cisco FMC へまたは Cisco FMC を通して特定の CLI コマンドを送信 することによってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者がデバイスコンフィギュレーションを修正するか、または Cisco FMC ソフトウェアを実行しているまたは Cisco FMC によって管理されるあらゆる Firepower デバイスのファイルを可能性がありますデバイスの削除することを可能にする。

この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-fp-cmd-

injection

該当製品

脆弱性のある製品

この脆弱性は Cisco Firepower システム ソフトウェアの脆弱なリリースを実行する場合、以下のシスコ製品に影響を及ぼします:

- FirePOWER サービスを使用する適応型セキュリティ アプライアンス（ASA）5500-X シリーズ
- 次世代ファイアウォール製品群を使用する適応型セキュリティ アプライアンス（ASA）5500-X シリーズ
- FirePOWER 7000 シリーズ アプライアンス
- FirePOWER 8000 シリーズ アプライアンス
- FirePOWER 2100 シリーズ セキュリティ アプライアンス
- FirePOWER 4100 シリーズ セキュリティ アプライアンス
- FirePOWER 9300 シリーズ セキュリティ アプライアンス
- Firepower Management Center
- Firepower Threat Defense
- Firepower Threat Defense Virtual（FTDv）
- 次世代侵入防御システム（NGIPS）バーチャル（NGIPSv）

情報に関してはどのについての Cisco Firepower システムソフトウェアリリースが脆弱であるか、このアドバイザリの修正済みソフトウェアのセクションを参照して下さい。

Firepower システムソフトウェアリリースを判別して下さい

、管理者はデバイスにログインどの Cisco Firepower システムソフトウェアリリースがデバイスで動作しているか判別し、**show version コマンドを** CLI で使用し、コマンドの出力を参照するためにできます。 次の例は Cisco Firepower システムソフトウェアリリース 6.2.0 を実行しているデバイスのためのコマンドの出力を示したものです:

```
> show version

--------------------[ ftd ]---------------------
Model : Cisco ASA5525-X Threat Defense (75) Version 6.2.0 (Build 362)
UUID : 2849ba3c-ecb8-11e6-98ca-b9fc2975893c
Rules update version : 2017-03-15-001-vrt
VDB version : 279
-------------------------------------------------
```

脆弱性を含んでいないことが確認された製品

このアドバイザリの 脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）（ISA）
- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- 侵入防御システム（IPS）ソフトウェア

詳細

Cisco FMC は Cisco Firepower センサーのためのネットワークの管理 デバイスです。 Firepower センサー実行 Cisco Firepower Threat Defense（FTD）ソフトウェア。 Firepower ソフトウェアおよびプラットフォームに関する詳細については、Cisco Firepower 互換性 ガイドを参照して下さい。

Cisco FMC によって Sourcefire トンネル 制御通信路 プロトコルが Firepower センサーを管理およびコントロールするのに使用されています。 このプロトコルを使用する接続である Sourcefire トンネル接続は Cisco FMC および Firepower センサー間の通信のために、使用されます。 Cisco FMC は Firepower センサーを制御するように意図されています。 ただし Firepower センサーが Cisco FMC または Cisco FMC によって管理されるその他のデバイスにコマンドを発行することができるように、認証が必要とする必要があります。 この アドバイザリに記載される 脆弱性は認証の欠如によって引き起こされます。

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

影響を受けたおよび修正済みソフトウェアリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。 不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

この脆弱性は、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-fp-cmd-injection

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-October-03

利用規約