Cisco Firepower 4100 シリーズ NGFW および Firepower 9300 セキュリティ アプライアンスでの Smart Licensing におけるコマンド インジェクションの脆弱性

High

アドバイザリーID : cisco-sa-20171101-fpwr

初公開日 : 2017-11-01 16:00

バージョン 1.0 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCvb86863

CVE-2017-12277

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

Cisco Firepower 4100 シリーズ次世代ファイアウォール（NGFW）および Firepower 9300 セキュリティ アプライアンスのスマートな認可マネージャ サービスの脆弱性は *ルート 特権*と実行できる任意のコマンドをインジェクトする認証される、リモート攻撃者可能にする可能性があります。

この脆弱性は、特定の Smart Licensing 設定パラメータの入力検証が不十分なことに起因するものです。 この脆弱性は、認証を受けている攻撃者が該当機能の内部に悪意ある URL を設定することによって、不正利用される可能性があります。 正常なエクスプロイトは攻撃者が *ルート 特権*の任意のコマンドを実行することを可能にする可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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。
101-fpwr

該当製品

脆弱性のある製品

この脆弱性は、FX-OS コード列 1.1.3、1.1.4、2.0.1 を実行している下記 Cisco Firepower セキュリティ製品に影響します。 バージョン 2.1.1、2.2.1、2.2.2 は影響を受けません。

- Firepower 4100 シリーズ次世代ファイアウォール
- Firepower 9300 セキュリティ アプライアンス

ソフトウェアのどのバージョンがデバイス（ *パッケージVers* ）で現在動作しているか判別するために、管理者は Admin ポータルでデバイス CLI でまたは **概要**タブへのナビゲートによって次のコマンドを使用することができます。 次の例は FX-OS 2.2(2.14) を実行するデバイスの CLI コマンド **show version** の出力を示したものです:

```
QP4120B1 # scope system
QP4120B1 /system # show version
FPRM:
Running-Vers: 4.2(2.15)
Package-Vers: 2.2(2.14)
Activate-Status: Ready
```

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

次の製品は、この脆弱性の影響を受けません。

- ASA 5500-X with FirePOWER Services
- FirePOWER 2100 シリーズ NGFW
- Firepower NGFW 仮想（NGFWv）

詳細

セキュリティ侵害の痕跡

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通

常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

下記の Cisco Firepower セキュリティ アプライアンス FX-OS リリースでは、この脆弱性への対処が行われています。 次の表に示すように、適切なリリースにアップグレードする必要があります。

Firepower 4100 および 9300 シリーズ セキュリティ アプライアンス FX-OS コード列	この脆弱性に対する最初の修正リリース
1.1.3 以前のリリース	影響あり。 2.0.1 以降への移行が必要
1.1.4	1.1.4.175
2.0.1	2.0.1.135
2.1.1	Not affected
2.2.1	Not affected
2.2.2	Not affected

注: FX-OS コード列バージョン 1.x は、サポート終了段階に入っています。 その他の情報に関しては Cisco Firepower 拡張可能なオペレーティング システム リリース 1.x のための終りの販売お

よびサポート終了（EOL）速報を参照して下さい。

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、内部テスト チームによってシスコに報告されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-fpwr

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017 年 11 月 1 日

利用規約