Cisco Firepower Threat Defense ソフトウェアのコマンドインジェクションの脆弱性

Medium

アドバイザリーID : cisco-sa-20190501-ftd-cmd-inject CVE-2019-1699
初公開日 : 2019-05-01 16:00
バージョン 1.0 : Final
CVSSスコア : 6.7
回避策 : No workarounds available
Cisco バグ ID : CSCvm14217 CSCvn33026

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 Threat Defense(FTD)ソフトウェアのCLIの脆弱性により、認証されたローカルの攻撃者がコマンドインジェクション攻撃を実行する可能性があります。

この脆弱性は、入力に対する不十分な検証に起因します。攻撃者は、特定のコマンドの引数にコマンドを挿入することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は root 権限でコマンドを実行できる可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。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。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-ftd-cmd-inject

該当製品

脆弱性のある製品

この脆弱性は、Cisco FTDソフトウェアの脆弱性が存在するリリースを実行しているシスコ製品に影響を与えます。脆弱性が存在する Cisco FTD ソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

Cisco FTD ソフトウェア リリースの判別

デバイスで実行中の Cisco FTD ソフトウェア リリースを確認するために、管理者はデバイス

にログインし、CLI で show version コマンドを使用してコマンドの出力を参照できます。デバイスが Cisco FTD ソフトウェア リリース 6.2.0 を実行している場合、コマンドの出力例は次のようになります。

```
<#root>

>

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のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコでは、この脆弱性が Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアに影響を及ぼさないことを確認しています。

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

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リリースしています。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、アクセスまたはその他の方法で使用した場合、お客様は https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載の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。

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、[シスコのセキュリティアドバイザリおよびアラート（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。

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（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

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

この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。次の表では、左の列にシスコソフトウェアのリリースを記載しています。右の列は、リリースがこのアドバイザリに記載された脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。

Cisco FTD ソフトウェア

Cisco FTD ソフトウェア リリース	この脆弱性のための推奨リリース
6.0	6.2.3.12
6.0.1	6.2.3.12
6.1.0	6.2.3.12
6.2.0	6.2.3.12
6.2.1	6.2.3.12
6.2.2	6.2.3.12
6.2.3	6.2.3.12
6.3.0	脆弱性なし
6.4.0	脆弱性なし

Cisco FTD ソフトウェアの修正済みリリースにアップグレードするには、次のいずれかの操作を行います。

- Cisco Firepower Management Center（FMC）を使用して管理しているデバイスについては、FMC インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。
- Cisco Firepower Device Manager（FDM）を使用して管理しているデバイスについては、FDM インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

シスコは、この脆弱性を報告していただいたTower Street社のLubomir Vesely氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-ftd-cmd-inject

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2019 年 5 月 1 日

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。