Cisco Firepower Threat Defense ソフトウェアの TCP 入力ハンドラにおけるサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-20190501-firepower-dos

初公開日 : 2019-05-01 16:00

最終更新日 : 2019-05-02 17:55

バージョン 1.1 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvg76064 CSCvf95761 CSCvn51149 CSCvk35736

CVE-2018-15462

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）ソフトウェアへの管理アクセスを設定したデータ インターフェイスの TCP 入力ハンドラの脆弱性により、認証されていないリモートの攻撃者が CPU とメモリの使用量を増やしてサービス妨害（DoS）状態になる危険性があります。

この脆弱性は、TCP ポート 22（SSH）および 443（HTTPS）の入力 TCP レート制限が不十分であることに起因します。 攻撃者は、該当デバイスへの管理アクセスが設定されているデータ インターフェイスでポート 22 または 443 に細工された TCP トラフィックの一定のストリームを送信することにより、この脆弱性をエクスプロイトする危険性があります。

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ました。 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-20190501-firepower-dos

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のあるリリースを実行する次のシスコ製品に影響を与えます。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）
- 適応型セキュリティ アプライアンス（ASA）5500-X シリーズ ファイアウォール
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス
- FTD Virtual（FTDv）

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。

```
> 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
-------------------------------------------------
```

SSH および HTTP サービスの設定の確認

次の表では、左の列に脆弱性が存在する可能性がある Cisco FTD の機能を記載しています。また右の列には、**show running-config** CLI コマンドで判断可能な、この機能の基本設定を示します。 これらの機能のいずれかが設定されているデバイスは、このアドバイザリに記載されている脆弱性の影響を受けます。

Cisco FTD 機能	脆弱性の存在するコンフィギュレーション
HTTP サービスが有効[1、2]	http server enable <port> http <remote_ip_address> <remote_subnet_mask> <interface_name>
SSH サービスが有効[1、3]	ssh <remote_ip_address> <remote_subnet_mask> <interface_name>

[1] デバイスは、HTTP または SSH コマンドで設定された範囲の IP アドレスに対してのみ脆弱です。

[2] FDM アクセス用に設定されたすべてのデバイスで HTTP サービスが有効になっています。

[3] FMC によって管理されているすべてのデバイスで SSH サービスが有効になっています。

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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.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。
https://www.cisco.com/c/en/us/support/web/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

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。
本アドバイザリは以下のアドバイザリを含むコレクションの一部です。お客様におかれましては、これらも考慮したうえでアップグレード ソリューション全体をご確認ください。

- cisco-sa-20190501-asa-csrf： Cisco 適応型セキュリティ アプライアンス ソフトウェアで発見されたクロスサイト リクエスト フォージェリの脆弱性
- cisco-sa-20190501-asa-frpwrtd-dos： Cisco 適応型セキュリティ アプライアンス ソフトウェアおよび Cisco Firepower Threat Defense ソフトウェアの TCP タイマー処理におけるサービス妨害の脆弱性
- cisco-sa-20190501-asa-ftd-dos： Cisco 適応型セキュリティ アプライアンス ソフトウェアおよび Firepower Threat Defense ソフトウェアの WebVPN におけるサービス妨害の脆弱性
- cisco-sa-20190501-asa-ftd-entropy： Cisco 適応型セキュリティ アプライアンス ソフトウェアおよび Firepower Threat Defense ソフトウェアの低エントロピー キーの脆弱性
- cisco-sa-20190501-asa-ftd-ike-dos： Cisco 適応型セキュリティ アプライアンス ソフトウェアおよび Cisco Firepower Threat Defense ソフトウェアの MOBIKE におけるサービス妨害の脆弱性
- cisco-sa-20190501-asaftd-saml-vpn： Cisco 適応型セキュリティ アプライアンス ソフトウェアおよび Firepower Threat Defense ソフトウェアの VPN SAML 認証バイパスの脆弱性
- cisco-sa-20190501-asa-ipsec-dos： Cisco 適応型セキュリティ アプライアンス ソフトウェアの IPsec におけるサービス妨害の脆弱性
- cisco-sa-20190501-firepower-dos： Cisco Firepower Threat Defense ソフトウェアの TCP 入力ハンドラにおけるサービス妨害の脆弱性
- cisco-sa-20190501-frpwr-dos： Cisco Firepower Threat Defense ソフトウェアのパケット処理におけるサービス妨害の脆弱性
- cisco-sa-20190501-frpwr-smb-snort： Cisco Firepower Threat Defense ソフトウェアの SMB プロトコル プリプロセッサ検出エンジンにおけるサービス妨害の脆弱性
- cisco-sa-20190501-sd-cpu-dos： Cisco 適応型セキュリティ アプライアンス ソフトウェアおよび Firepower Threat Defense ソフトウェアの WebVPN におけるサービス妨害の脆弱性

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。 中央の列には、リリースがこのアドバイザリに記載されている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。 右の列は、リリースがこのアドバイザリ集に記載された何らかの脆弱性に該当するかどうか、および、それらすべての脆弱性に対する修正を含む最初の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	このアドバイザリ集で説明している脆弱性すべてに対す
6.0	6.2.3.12	6.2.3.12
6.0.1	6.2.3.12	6.2.3.12
6.1.0	6.2.3.12	6.2.3.12
6.2.0	6.2.3.12	6.2.3.12
6.2.1	6.2.3.12	6.2.3.12
6.2.2	6.2.3.12	6.2.3.12
6.2.3	6.2.3.12	6.2.3.12
6.3.0	6.3.0.3	6.3.0.3
6.4.0	脆弱性なし	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）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-20190501-firepower-dos

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	FTD ソフトウェア リリース 6.3.0.3 が使用可能になったことを示すために FTD の修	修正済みソフトウェア	最終版	2019 年 5 月 2

	正済みリリースの表を更新。			日
1.0	初回公開リリース		最終版	2019 年 5 月 1 日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。