Cisco Firepower Threat Defense ソフトウェアの SSL 復号ポリシー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-ftd-ssl-decrypt-dos-DdyLuK6c

初公開日 : 2021-04-28 16:00

最終更新日 : 2021-06-08 21:10

バージョン 1.1 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvo46649

CVE-2021-1402

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）ソフトウェアのソフトウェアベース SSL/TLS メッセージハンドラにおける脆弱性により、認証されていないリモートの攻撃者が該当デバイスのリロードを引き起こし、サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、デバイスがソフトウェアベースの SSL 復号を実行するときに SSL/TLS メッセージの検証が不十分であることに起因します。攻撃者は、該当デバイスを*通じ*て細工された SSL/TLS メッセージを送信することで、この脆弱性をエクスプロイトする可能性があります。該当デバイスに送信される SSL/TLS メッセージは、この脆弱性の原因になりません。攻撃者がエクスプロイトに成功すると、プロセスがクラッシュする可能性があります。このクラッシュにより、デバイスのリロードが引き起こされます。リロード後にデバイスを回復するために手動で介入する必要はありません。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-ssl-decrypt-dos-DdyLuK6c

このアドバイザリは、2021 年 4 月に公開された Cisco ASA、FMC、および FTD ソフトウェアのセキュリティ アドバイザリ バンドルの一部です。これらのアドバイザリとリンクの一覧について

は、以下を参照してください。シスコのイベント対応：2021 年 4 月に公開された Cisco ASA、FMC、および FTD ソフトウェアのセキュリティ アドバイザリ バンドル。

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、シスコの次の製品で、脆弱性のある Cisco FTD ソフトウェア リリースを実行しており、SSL 復号ポリシーが有効になっていて、次のハードウェア プラットフォームのいずれかが動作している場合です。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）
- ASA 5512-X 適応型セキュリティ アプライアンス
- ASA 5515-X 適応型セキュリティ アプライアンス
- ASA 5525-X 適応型セキュリティ アプライアンス
- ASA 5545-X 適応型セキュリティ アプライアンス
- ASA 5555-X 適応型セキュリティ アプライアンス
- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Firepower Threat Defense Virtual（FTDv）

脆弱性が存在する Cisco 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。

SSL 復号ポリシーが有効になっているかどうかを確認する方法

SSL 復号ポリシーが有効になっているかどうかは、次の 2 つの方法で確認できます。

オプション 1：CLI の使用

CLI コマンドの **show ssl-policy-config を使用して、デバイスで SSL 復号ポリシーが有効になっているかどうかを確認します。**次の例は、SSL ポリシーが*設定されておらず*、脆弱性が存在*しない*デバイスでの *show ssl-policy-config コマンドの出力を示します。*

```
> show ssl-policy-config
SSL policy not yet applied.
```

show ssl-policy-config コマンドによって返されるその他すべての出力は、SSL ポリシーが設定されており、デバイスに脆弱性が存在することを示します。

show ssl-policy-config コマンドの詳細については、Cisco Firepower Threat Defense のコマンドリファレンスを参照してください。

オプション 2：GUI の使用

デバイスで SSL 復号ポリシーが有効になっているかどうかを確認するには、適切なポリシーを確認します。

- Firepower Management Center（FMC）によって管理されているデバイスの場合は、次のように選択します。
  [ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [SSL]
- Firepower Device Manager（FDM）によって管理されているデバイスの場合は、次のように選択します。
  [ポリシー（Policies）] > [SSL復号（SSL Decryption）]

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。

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Firepower Management Center（FMC）ソフトウェア
- このアドバイザリの「脆弱性のある製品」に記載されているプラットフォーム以外のプラットフォームで実行されている FTD ソフトウェア

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、シスコ セキュリティ アドバイザリ 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アップグレード ソリューション一式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 Cisco Service Contract 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 POS 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

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に該当するかどうか、および、こ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。右の列は、リリースがこのバンドル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。

FTD ソフトウェア

Cisco FTD ソフトウェア リリース	この脆弱性に対する最初の修正リリース	アドバイザリのバンドルに記載されているすべての脆弱性に関して推奨される修正済みリリース
6.2.21 より前	脆弱性なし	修正済みリリースに移行。
6.2.2	脆弱性なし	修正済みリリースに移行。
6.2.3	脆弱性なし	修正済みリリースに移行。
6.3.0	修正済みリリースに移行。	修正済みリリースに移行。
6.4.0	脆弱性なし	6.4.0.12 (May 2021)
6.5.0	脆弱性なし	修正済みリリースに移行。
6.6.0	脆弱性なし	6.6.42
6.7.0	脆弱性なし	6.7.0.2

1. Cisco FMC および FTD ソフトウェアリリース 6.0.1 以前および 6.2.0、6.2.1 については、ソフトウェアのメンテナンスが終了しています。この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

2. 6.6.0 コードトレインに関する最初の修正済みリリースは 6.6.3 ですが、CSCvx86231 に関連するアップグレードの問題のため、推奨されるリリースは 6.6.4 です。

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

この脆弱性は、シスコ内部でセキュリティ テストを実施中に、Sanmith Prakash によって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-ssl-decrypt-dos-DdyLuK6c

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	脆弱性のないリリースをより明確に識別するため、修正済みリリースの表を更新。	修正済みソフトウェア	最終版	2021 年 6 月 8 日
1.0	初回公開リリース	—	最終版	2021-APR-28

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。