Firepower 2100 シリーズ アプライアンス向け 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 SSL/TLS におけるサービス妨害の脆弱性

アドバイザリーID : cisco-sa-asaftd-ssl-dos-uu7mV5p6
CVE-2023-20006
初公開日 : 2023-06-07 16:00
最終更新日 : 2024-05-22 16:37
バージョン 1.2 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCwc94466 CSCwf62729

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 2100 シリーズ アプライアンス向け Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアおよび Cisco Firepower Threat Defense（FTD）ソフトウェアのハードウェアベースの SSL/TLS 暗号化機能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で予期しない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、SSL/TLS トラフィック処理がハードウェアにオフロードされるときの暗号化機能内の実装エラーに起因します。攻撃者は、細工された一連の SSL/TLS トラフィックを該当デバイスに送信することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者はハードウェアベースの暗号化エンジンで予期しないエラーを引き起こし、デバイスをリロードさせ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-asaftd-ssl-dos-uu7mV5p6

該当製品

脆弱性のある製品

SSL/TLS 用に設定された Cisco Firepower 2100 シリーズ アプライアンスで実行されている場合、この脆弱性は、Cisco ASA ソフトウェアおよび Cisco FTD ソフトウェアの特定のリリースに影響します。

注：

- Cisco ASA ソフトウェアの場合、デバイスで終了する SSL/TLS 接続が、この脆弱性をエクスプロイトするために使用される可能性があります。対象には、管理トラフィック、SSL/TLS トラフィックを終端する機能 (リモートアクセス VPN など) が含まれます。
- Cisco FTD ソフトウェアの場合、影響を受ける機能セットは、SSL 復号ポリシーとリモートアクセス VPN に限定されます。

脆弱性のある Cisco ソフトウェアリリースの詳細については、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。

デバイスで SSL または TLS メッセージ処理の可能性があるかどうかの確認

Cisco ASA ソフトウェアまたは Cisco FTD ソフトウェアを実行中の Cisco Firepower 2100 シリーズ アプライアンスで、SSL または TLS パケットが処理されるかどうかを確認するには、show asp table socket | include SSL|DTLS コマンドを使用して、コマンドの出力を確認します。このコマンドの出力が空の場合、デバイスはこの脆弱性の影響を受けていません。このコマンドの出力が返される場合、デバイスはこの脆弱性の影響を受けています。次の例を参照してください。

<#root>

```
ftd#
show asp table socket | include SSL|DTLS

SSL        0005aa68  LISTEN     x.x.x.x:443      0.0.0.0:*
SSL        002d9e38  LISTEN     x.x.x.x:8443     0.0.0.0:*
DTLS       0018f7a8  LISTEN     10.0.0.250:443   0.0.0.0:*
```

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 Cisco Firepower Management Center（FMC）ソフトウェアに影響を及ぼさないことを確認しました。

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。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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。

Cisco.com の Cisco Support and Downloads ページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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シスコ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。

Cisco ASA、FMC、および FTD ソフトウェア

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性に対するリスクを判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース (「First Fixed」) を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース (「Combined First Fixed」) を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。すべてのアドバイザリ、セキュリティ影響評価 (SIR) が「重大」または「高」のアドバイザリのみ、またはこのアドバイザリのみを選択します。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco ASA ソフトウェアの場合は 9.16.2.11、Cisco FTD ソフトウェアの場合は 6.6.7 と入力します。
5. [チェック (Check)] をクリックします。

2		Critical,High,Medium
このアドバイザのみ	Cisco ASA ソフトウェア	
あらゆるプラットフォーム		
Enter release number	オン	

FTD デバイスのアップグレード手順については、『Cisco Firepower Management Center Upgrade Guide』を参照してください。

関連情報

最適な Cisco ASA、FMC、または FTD ソフトウェアリリースの決定方法については、次の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco ASA の互換性
Cisco Secure Firewall ASA アップグレードガイド
Cisco Secure Firewall Threat Defense 互換性ガイド

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 Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ssl-dos-uu7mV5p6

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	Cisco Bug ID CSCwf62729 を追加し、「脆弱性のある製品」セクションを更新し、ソフトウェアチェッカーの修正済みリリースを更新。	ヘッダー、脆弱性のある製品、修正済みソフトウェア	Final	2024 年 5 月 22 日
1.1	破損したリンクを修正。	修正済みソフトウェア	Final	2024 年 1 月 19 日
1.0	初回公開リリース	—	Final	2023 年 6 月 7 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。

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。