

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 ソフトウェアのリモートアクセス SSL VPN におけるサービス妨害の脆弱性



アドバイザリーID : cisco-sa-asa-dos-tL4uA4AA

[CVE-2022-20715](#)

初公開日 : 2022-04-27 16:00

最終更新日 : 2022-08-10 19:07

バージョン 1.3 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwa04461](#)

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 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) ソフトウェアのリモートアクセス SSL VPN 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サービス妨害 (DoS) 状態を引き起こす可能性があります。

この脆弱性は、リモートアクセス VPN を使用したクライアント接続の結果としてログに記録されるエラーの不適切な検証に起因します。攻撃者は、細工された要求を該当システム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。不正利用に成功すると、攻撃者が該当デバイスを再起動させ、その結果として DoS 状態に陥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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-dos-tL4uA4AA>

このアドバイザリーは、2022 年 4 月に公開された Cisco ASA、FTD、および FMC のセキュリティアドバイザリーバンドルに含まれています。アドバイザリーとリンクの一覧については、[Cisco Event Response : 2022 年 4 月に公開された Cisco ASA、FMC、および FTD ソフトウェア セキ](#)

[ユリティアドバイザリバンドル](#) を参照してください。

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、シスコ製品で、脆弱性のある Cisco ASA ソフトウェアまたは FTD ソフトウェアリリースを実行しており、AnyConnect または WebVPN が脆弱性のある設定になっている場合です。

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。

Cisco ASA ソフトウェア設定の確認

show-running-config CLI コマンドを使用して、デバイスのソフトウェアに脆弱性のある機能が設定されているかどうかを確認します。次の表の左列は、脆弱性のある Cisco ASA 機能を示します。右の列は、機能が有効になっているデバイスでの show running-config CLI コマンドの出力を示しています。脆弱性のあるリリースがデバイスで実行されており、いずれかの機能が設定されている場合は、この脆弱性の影響を受けます。

Cisco ASA ソフトウェアの機能	脆弱性の存在するコンフィギュレーション
AnyConnect SSL VPN	webvpn enable <interface_name>
クライアントレス SSL VPN	webvpn enable <interface_name>

Cisco FTD ソフトウェア設定の確認

show-running-config CLI コマンドを使用して、デバイスのソフトウェアに脆弱性のある機能が設定されているかどうかを確認します。次の表の左列は、脆弱性のある Cisco FTD 機能を示します。右の列は、機能が有効になっているデバイスでの show running-config CLI コマンドの出力を示しています。脆弱性のあるリリースがデバイスで実行されており、いずれかの機能が設定されている場合は、この脆弱性の影響を受けます。

Cisco FTD ソフトウェアの機能	脆弱性の存在するコンフィギュレーション
AnyConnect SSL VPN ^{1, 2}	

Cisco FTD ソフトウェアの機能	脆弱性の存在するコンフィギュレーション
	webvpn enable <interface_name>

1. リモートアクセス VPN 機能は、Cisco FTD ソフトウェアリリース 6.2.2 で導入されました。
2. リモートアクセス VPN 機能は、Cisco Firepower Management Center (FMC) で [デバイス (Devices)] > [VPN] > [リモートアクセス (Remote Access)] の順に選択するか、または Cisco Firepower Device Manager (FDM) で [デバイス (Devices)] > [リモートアクセス VPN (Remote Access VPN)] の順に選択すると有効になります。

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。](#)

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ン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です。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

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。右側の列は、リリースがこのバンドルに記載された「重大」または「高」SIR 脆弱性のいずれかに該当するかどうか、およびそれらの脆弱性に対する修正を含むリリースを示しています。

ASA ソフトウェア

Cisco ASA 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対する最初の修正済みリリース
9.7 以前 ¹	脆弱性なし	修正済みリリースに移行。
9.8	脆弱性なし	9.8.4.44 (June 2022)
9.91	脆弱性なし	修正済みリリースに移行。
9.101	脆弱性なし	修正済みリリースに移行。
9.12	脆弱性なし	9.12.4.38
9.131	脆弱性なし	修正済みリリースに移行。
9.14	脆弱性なし	9.14.4
9.15	脆弱性なし	9.15.1.21
9.16	9.16.2.11	9.16.2.14

Cisco ASA 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対する最初の修正済みリリース
9.17	脆弱性なし	9.17.1.7

1. Cisco ASA ソフトウェアリリース 9.7 以前、および 9.9、9.10、9.13 リリースについては、[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。

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対する最初の修正済みリリース
6.2.2 以前 ¹	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 ¹	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	6.4.0.13	6.4.0.15 (May 2022)
6.5.01	修正済みリリースに移行。	修正済みリリースに移行。
6.6.0	6.6.5.2	6.6.5.2
6.7.0	Cisco_FTD_Hotfix_AA-6.7.0.4-2.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_AA-6.7.0.4-2.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_AA-6.7.0.4-2.sh.RE L.tar Cisco_FTD_SSP_Hotfix_AA-6.7.0.4-2.sh.RE L.tar	修正済みリリースに移行。
7.0.0	7.0.2 (May 2022)	7.0.2 (May 2022)
7.1.0	7.1.0	7.1.0.1

1. Cisco FMC および FTD ソフトウェアリリース 6.2.2 以前および 6.3.0、6.5.0 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。

FTD デバイスのアップグレード手順については、[Cisco Firepower Management Center アップグレードガイド](#)を参照してください。

Product Security Incident Response Team (PSIRT; プロダクト セキュリティ インシデント レスポンス チーム) は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザーに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

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-asa-dos-tL4uA4AA>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.3	Cisco FTDソフトウェアの修正済みバージョン情報を修正。	修正済みソフトウェア	Final	2022年8月10日
1.2	CVSSスコアを修正。	—	Final	2022年8月8日
1.1	ASA 9.8 の最初の修正済みリリースに関する情報を更新。	修正済みソフトウェア	Final	2022年6月1日
1.0	初回公開リリース	—	Final	2022年4月27日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。