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 Web サービスインターフェイスにおけるサービス妨害の脆弱性

アドバイザリーID : cisco-sa-asafdt-webvpn-dos-tzPSYern
初公開日 : 2022-04-27 16:00
最終更新日 : 2022-11-09 16:02
バージョン 1.2 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCwb87950 CSCvz70595 CSCwb93914

CVE-2022-20745

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 VPN 機能の Web サービスインターフェイスにある脆弱性により、認証されていないリモートの攻撃者がサービス妨害 (DoS) 状態を発生させる可能性があります。

この脆弱性は、HTTPS リクエストを解析するときの入力検証が適切でないことに起因します。細工された HTTPS リクエストが該当デバイスに送信されると、この脆弱性がエクスプロイトされる危険性があります。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生す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-asafdt-webvpn-dos-tzPSYern

このアドバイザリは、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 バンドルに含まれています。アドバイザリ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 セキュリティ 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 Cisco FTD ソフトウェアリリースを実行しており、リモートアクセス VPN の設定に脆弱性がある場合です。

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。

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、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。右側の列に示す各機能の基本設定は、show running-config CLI コマンドを実行すると表示されます。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、脆弱性が存在します。

Cisco ASA 機能	脆弱性の存在するコンフィギュレーション
AnyConnect インターネット キー エクスチェンジ バージョン 2 リモートアクセス (クライアントサービス有効時)	`crypto ikev2 enable <interface_name> client-services port <port #>`
AnyConnect SSL VPN	`webvpn` ` enable <interface_name>`
クライアントレス SSL VPN	`webvpn` ` enable <interface_name>`

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、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。右側の列に示す各機能の基本設定は、show running-config CLI コマンドを実行すると表示されます

。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、脆弱性が存在します。

Cisco FTD 機能	脆弱性の存在するコンフィギュレーション
AnyConnect インターネット キー エクスチェンジ バージョン 2 リモートアクセス（クライアントサービス有効時）[1、2]	`crypto ikev2 enable <interface_name> client-services port <port #>`
AnyConnect SSL VPN[1、2]	`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。

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	CSCvz70595 の最初の修正済みリリース	CSCwb87950 および CSCwb93914 の最初の修正済みリリース
9.6 以前[1]	脆弱性なし	脆弱性なし
9.7[1]	修正済みリリースに移行。	修正済みリリースに移行。
9.8	9.8.4.44	9.8.4.46
9.91	修正済みリリースに移行。	修正済みリリースに移行。
9.101	修正済みリリースに移行。	修正済みリリースに移行。
9.12	9.12.4.35	9.12.4.52
9.131	修正済みリリースに移行。	修正済みリリースに移行。
9.14	9.14.3.13	9.14.4.16
9.15	9.15.1.21	修正済みリリースに移行。
9.16	9.16.2.7	9.16.3.15
9.17	脆弱性なし	9.17.1.16
9.18	脆弱性なし	9.18.1.3

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	CSCvz70595 の最初の修正済みリリース	CSCwb87950 および CSCwb93914 の最初の修正済みリリース
6.1.0 以前[1]	脆弱性なし	脆弱性なし
6.2.2[1]	修正済みリリースに移行。	修正済みリリースに移行。
6.2.3	修正済みリリースに移行。	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	6.4.0.16
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	6.6.5.1	6.6.7.1
6.7.0	Cisco_FTD_Hotfix_AA-6.7.0.4-2.sh.REL.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-	修正済みリリースに移行。

Cisco FTD ソフトウェア リリース	CSCvz70595 の最初の修正済みリリース	CSCwb87950 および CSCwb93914 の最初の修正済みリリース
	2.sh.RE L.tar	
7.0.0	7.0.2	7.0.4
7.1.0	脆弱性なし	7.1.0.3
7.2.0	脆弱性なし	7.2.1

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、本アドバイザリ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

この脆弱性は元々、Cisco TAC サポートケースの解決中に発見されました。

シスコは、脆弱性の修正が不完全であったことを報告していただいたインドネシアの Saleh Iskandar 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-tzPSYern

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	修正済みリリースの表を更新し、Cisco Bug CSCwb87950 および CSCwb93914 に対するその他の修	修正済みソフトウェア	Final	2022 年 11 月 9

バージョン	説明	セクション	ステータス	日付
	正を反映しました。ソースも更新されました。	、ソース		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

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。