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 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-ftd-vpn-dos-fpBcpEcD
初公開日 : 2021-04-28 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCvv56644 CSCvv65184

CVE-2021-1445
CVE-2021-1504

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 Firepower Threat Defense（FTD）ソフトウェア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。

これらの脆弱性は、HTTP リクエストの入力検証が適切に行われていないことに起因します。攻撃者は、細工された HTTP 要求を該当デバイスに送信することで、これら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。

注：この脆弱性の影響を受けるのは、特定のAnyConnectおよびWebVPN設定のみです。詳細については、「脆弱性のある製品」のセクションを参照してください。

シスコはこれら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。これら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-asa-ftd-vpn-dos-fpBcpEcD

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。アドバイザリの完全なリストとそのリンクにつ

いては、『Cisco Event Response: April 2021 Cisco ASA, FMC, and FTD Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

これらの脆弱性の影響を受けるのは、シスコのデバイスが、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、AnyConnect VPN クライアント接続を終了させるように設定されている場合です。

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。

ASA ソフトウェア

次の表の左列は、脆弱性のある Cisco ASA 機能を示します。右列に示す Cisco ASA 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。ここに示す機能のいずれかがデバイスに設定されている場合は、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 IKEv2 Remote Access（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>`

FTD ソフトウェア

次の表の左列は、脆弱性のある Cisco FTD 機能を示します。右列に示す Cisco ASA 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。ここに示す機能のいずれかがデバイスに設定されている場合は、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 IKEv2 Remote Access（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、	

Cisco FTD 機能	脆弱性の存在するコンフィギュレーション
2	webvpn enable <interface_name>

1. 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。
2.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からサポートされています。

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のある製品セクションに記載されている製品のみが、これら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、これらの脆弱性が Cisco Firepower Management Center（FMC）ソフトウェアおよび Web ブラウザベースの VPN 接続に影響を及ぼさないことを確認しました。

回避策

これら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。2 列目と 3 列目は、リリースがこのアドバイザリに記載された脆弱性の影響を受けるかどうかと、各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、リリースがアドバイザリ集に記載された何らかの脆弱性の影響を受けるかどうかと、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 ASA ソフトウェア

Cisco ASA ソフトウェア リリース	CVE-2021-1445 (CSCvv56644)	CVE-2021-1504 (CSCvv65184)	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修正済みリリース
9.71 より前	脆弱性なし	脆弱性なし	修正済みリリースに移行。
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。	修正済みリリースに移行。
9.8	9.8.4.34	9.8.4.35	9.8.4.35
9.9	9.9.2.85	9.9.2.85	9.9.2.85
9.10	修正済みリリースに移行。	修正済みリリースに移行。	修正済みリリースに移行。
9.12	9.12.4.13	9.12.4.10	9.12.4.18
9.13	9.13.1.21	9.13.1.21	9.13.1.21
9.14	9.14.2.8	9.14.2.4	9.14.2.13
9.15	9.15.1.7	9.15.1.7	9.15.1.15

1. Cisco ASA ソフトウェアリリース 9.7 以前および 9.10 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。

Cisco FTD ソフトウェア

Cisco FTD ソフトウェア リリース	CVE-2021-1445 (CSCvv56644)	CVE-2021-1504 (CSCvv65184)	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推奨リリース
6.2.21 より前	修正済みリリースに移行。	修正済みリリースに移行。	修正済みリリースに移行。
6.2.2	修正済みリリースに移行。	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。	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。	修正済みリリースに移行。
6.4.0	6.4.0.12 (May 2021)	6.4.0.12 (May 2021)	6.4.0.12 (May 2021)
6.5.0	修正済みリリースに移行。	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	6.6.4	6.6.4	6.6.42
6.7.0	6.7.0.1	6.7.0.1	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コードトレインの最初の修正済みリリースは6.6.3でした。ただし、CSCvx86231に関連するアップグレードの問題のため、推奨リリースは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）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とその公表は確認しておりません。

出典

これらの脆弱性を報告していただいた PT Security 社の Nikita Abramov 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-vpn-dos-fpBcpEcD

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2021-APR-28

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。