Cisco Secure Firewall適応型セキュリティアプライアンスおよびSecure Firewall Threat Defenseソフトウェアのリモートアクセス VPN Webサーバにおける DoS 脆弱性

アドバイザリーID : cisco-sa-asaftd-vpnwebs-dos-hjBhmBsX
初公開日 : 2025-08-14 16:00
バージョン 1.0 : Final
CVSSスコア : 7.7
回避策 : No workarounds available
Cisco バグ ID : CSCwo08017

CVE-2025-20244

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 Secure Firewall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 Secure Firewall Threat Defense(FTD)ソフトウェアのリモートアクセスSSL VPNサービスの脆弱性により、VPNユーザとして認証されたリモート攻撃者がデバイスの予期せぬリロードを引き起こし、その結果サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、HTTPヘッダーフィールド値を解析する際の不完全なエラーチェックに起因します。攻撃者は、該当デバイスのターゲットリモートアクセスSSL VPNサービスに巧妙に細工されたHTTP要求を送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、DoS状態が引き起こされ、該当デバイスがリロードされる危険性があります。

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-vpnwebs-dos-hjBhmBsX

このアドバイザリは、Cisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェアセキュリティアドバイザリバンドルの2025年8月リリースの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: August 2025 Semiannual Cisco Secure Firewall

ASA, Secure FMC, and Secure 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

この脆弱性は、Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアに、次の2つの表にリストされている脆弱性のある設定が1つ以上存在する場合に影響を与えます。

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 Secure Firewall ASAソフトウェアの脆弱な設定

次の表では、左の列に、脆弱性が存在する可能性のあるCisco Secure Firewall ASAソフトウェアの機能を示しています。また右の列には、show running-config CLI コマンドで判断可能な、この機能の基本設定を示します。これらの機能により、SSLリスニングソケットが有効になる可能性があります。

Cisco Secure Firewall ASAソフトウェア機能	脆弱性の可能性がある設定
AnyConnect IKEv2 Remote Access（クライアント サービス有効時）	`crypto ikev2 enable [...] client-services port <port_number>`

モバイルユーザセキュリティ(MUS)[1]	`webvpn`
	` mus password <password>`
	` mus server enable port 610`
	` mus <ip_address> <subnet_mask> <interface_name>`

SSL VPN（トンネルモード）	`webvpn` ` enable <interface_name>`

1. この機能は、設定されたアクセスホストのIPアドレスに対してのみ脆弱です。

Cisco Secure FTDソフトウェアの脆弱な設定

次の表では、左の列に、脆弱性が存在する可能性のあるCisco Secure FTDソフトウェアの機能を示しています。また右の列には、show running-config CLI コマンドで判断可能な、この機能の基本設定を示します。これらの機能により、SSLリスニングソケットが有効になる可能性が

あります。

Cisco Secure FTDソフトウェア機能	脆弱性の可能性がある設定
AnyConnect IKEv2 Remote Access（クライアントサービスあり）[1]	`crypto ikev2 enable [...] client-services port <port_number>`
AnyConnect SSL VPN[1]	`webvpn` ` enable <interface_name>`

1. リモートアクセスVPN機能は、Cisco Secure Firewall Management Center(FMC)ソフトウェアの Devices > VPN > Remote Access、またはCisco Secure Firewall Device Manager(FDM)の Device > Remote Access VPNで有効になっています。

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性がCisco Secure FMCソフトウェアには影響を与え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 シスコサポート & ダウンロードページには、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完全なアップグレード ソリューション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。

Cisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェア

お客様がCisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェアの脆弱性による侵害の可能性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、セキュリティへの影

響の評価（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 Secure Firewall ASAソフトウェアの場合は9.16.2.11、Cisco Secure 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	Check	

Cisco Secure FTDホットフィックス

シスコはこの脆弱性に対処するために、次のホットフィックスをリリースしました。ホットフィックスは、Cisco.comのSoftware Centerからダウンロードできます。

Cisco Secure FTDソフトウェアリリース	ホットフィックス名
7.4	Cisco_FTD_Hotfix_EI-7.4.2.4-2.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_EI-7.4.2.4-2.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_EI-7.4.2.4-2.sh.RE L.tar Cisco_FTD_SSP_FP3K_Hotfix_EI-7.4.2.4-2.sh.RE L.tar Cisco_FTD_SSP_Hotfix_EI-7.4.2.4-2.sh.RE L.tar Cisco_Secure_FW_TD_4200_Hotfix_EI-7.4.2.4-2.sh.RE L.tar

これらのホットフィックスのダウンロードとインストールの詳細については、Cisco Secure Firewall Threat Defense/Firepower Hotfixリリースノートを参照してください。

シスコの 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済みリリース情報のみを検証します。

Cisco Secure FTDデバイスのアップグレード手順については、該当する『Cisco Secure FMC upgrade guide』を参照してください。

関連情報

最適なCisco Secure Firewall ASA、Secure FMC、またはSecure FTDソフトウェアリリースの判別に関しては、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 Secure Firewall 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 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、Cisco Advanced Security Initiatives Group(ASIG)のT.VEによる内部セキュリティテストで発見されました。

URL

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

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	2025年8月14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。