

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VPN WebサーバにおけるDoS脆弱性



アドバイザーID : cisco-sa-asaftd-http-file-[CVE-2025-hUyX2jL4](#)
[20251](#)

初公開日 : 2025-08-14 16:00

バージョン 1.0 : Final

CVSSスコア : [8.5](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwo00141](#) [CSCwo00880](#)

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(SSL)サービスの脆弱性により、認証されたりモートの攻撃者が、基盤となるオペレーティングシステム上で任意のファイルを作成または削除できる可能性があります。重要なシステムファイルが操作されると、新しいリモートアクセスSSL VPNセッションが拒否され、既存のセッションがドロップされ、サービス拒否(DoS)状態が発生する可能性があります。不正利用されたデバイスを回復するには、手動でリブートする必要があります。

この脆弱性は、HTTP要求を処理する際の不十分な入力検証に起因します。攻撃者は、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、この脆弱性をエクスプロイトすることができます。エクスプロイトに成功すると、攻撃者は基盤となるオペレーティングシステム上でファイルを作成または削除し、リモートアクセスSSL VPNサービスが応答しなくなる可能性があります。

この脆弱性を不正利用するには、該当デバイスのVPNユーザとして攻撃者を認証する必要があります。

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-asaftd-http-file-hUyX2jL4>

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Cisco Secure FTDソフトウェアに、次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。

セキュアファイアウォール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)	webvpn mus password mus server enable port mus
SSL VPN (トンネルモード)	webvpn enable

セキュアな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

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

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 [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
このアドバイザリのみ	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 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 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-http-file-hUyX2jL4>

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

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。