

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SSL VPNにおけるDoS脆弱性



アドバイザリーID : cisco-sa-asaftd-vpn-dos-mfPekA6e

初公開日 : 2025-08-14 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 : [CSCwk44165](#) [CSCwo15027](#)

[CVE-2025-20133](#)

[CVE-2025-20243](#)

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)ソフトウェアの管理およびVPN Webサーバの複数の脆弱性により、認証されていないリモートの攻撃者がデバイスの応答を停止させたり、予期せぬリロードを引き起こしたりして、サービス妨害(DoS)状態を発生させる可能性があります。

これらの脆弱性は、アプリケーションエンドポイントに対するユーザ入力の検証が不適切なことに起因します。攻撃者は、巧妙に細工されたHTTP要求をデバイス上のターゲットWebサーバに送信することで、これら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、デバイスが応答を停止したり、リロードしたりしたときに、DoS状態が引き起こされることがあります。

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-vpn-dos-mfPekA6e>

このアドバイザリーは、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ーバンドルの2025年8月リリースの一部です。アドバイザリー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

これらの脆弱性は、このセクションの表に記載されている脆弱な状態が1つ以上存在するCisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアに影響を与えます。

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。

デバイスが影響を受けるかどうかを確認する

Cisco Secure Firewall ASAソフトウェアまたはSecure FTD Softwareを実行しているデバイスが該当するかどうかを確認するには、`show asp table socket | include SSL`コマンドを使用して、任意のTCPポートでSSLリスニングソケットを検索します。出力にソケットが含まれている場合、そのデバイスは脆弱であると考えられます。次の例は、TCPポート443とTCPポート8443で2つのSSLリスニングソケットがあるCisco Secure Firewall ASAデバイスでの出力を示しています。

```
<#root>
```

```
ciscoasa#
```

```
show asp table socket | include SSL
```

```
SSL          00185038  LISTEN      172.16.0.250:
```

```
443
```

```
0.0.0.0:*
```

```
SSL          00188638  LISTEN      10.0.0.250:
```

```
8443
```

```
0.0.0.0:*
```

Cisco Secure Firewall ASAソフトウェアの設定が脆弱かどうかを確認する

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>
Cisco Adaptive Security Device Manager(ASDM)およびCisco Security Managerアクセスを含む管理Webサーバアクセス ¹	http server enable http <ip_address> <subnet_mask> <interface_name>
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ソフトウェアの設定に脆弱性があるかどうかを確認する

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>
HTTPサーバが有効 ^{2、3}	

Cisco Secure FTDソフトウェア 機能	脆弱性の可能性がある設定
	<pre>http server enable http <ip_address> <subnet_mask> <interface_name></pre>

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。
2. HTTP機能は、Cisco Secure FMCコンソールの Firepower Threat Defense Platform Settings > HTTPで有効になっています。
3. 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。

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 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。

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2025-20133: Cisco Secure Firewall ASAおよびSecure FTD SoftwareのリモートアクセスSSL VPN認証のターゲットDoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPN機能の管理およびVPN Webサーバの脆弱性により、認証されていないリモートの攻撃者がデバイスの応答を予期せず停止させ、DoS状態が発生する可能性があります。

この脆弱性は、リモートアクセスSSL VPN認証プロセス中のユーザ入力の検証が無効であることに起因します。攻撃者は、該当デバイスのVPNサービスに巧妙に細工された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状態が発生し、デバイスがリモートアクセスSSL VPN認証要求に応答しなくなります。

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。

バグID: [CSCwk44165](#)

CVE ID : CVE-2025-20133

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 8.6

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CVE-2025-20243: Cisco Secure Firewall ASAおよびSecure FTDソフトウェアのリモートアクセスSSL VPNのDoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアの管理およびVPN Webサーバの脆弱性により、認証されていないリモートの攻撃者がデバイスの予期しない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。

この脆弱性は、VPN Webサービスを使用するインターフェイスでユーザが行った入力の検証が不適切なことに起因します。攻撃者は、巧妙に細工されたHTTP要求を該当デバイスのターゲットWebサーバに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、攻撃者はデバイスのリロード時にDoS状態を引き起こす可能性があります。

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。

バグID: [CSCwo15027](#)

CVE ID : CVE-2025-20243

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 8.6

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

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。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) 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

CVE-2025-20133：この脆弱性は、Cisco Advanced Security Initiatives Group (ASIG) の Jason Crowder による内部セキュリティテストで発見されました。

CVE-2025-20243：この脆弱性は、Cisco ASIGのKeane O'Kelley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-vpn-dos-mfPekA6e>

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。