Cisco Secure Firewall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Secure Firewall Threat Defenseソフトウェアの VPN Webサーバにおける不正アクセスの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-webvpn-YROOTUW
初公開日 : 2025-09-25 16:00
最終更新日 : 2025-09-26 16:35
バージョン 1.1 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwq79815

CVE-2025-20362

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 Adaptive Security Appliance(ASA)ソフトウェアおよびCisco Secure Firewall Threat Defense(FTD)ソフトウェアのVPN Webサーバの脆弱性により、認証されていないリモート攻撃者が、リモートアクセスVPNに関連する制限されたURLエンドポイントにアクセスできるようになります。このURLエンドポイントには、認証を行わないとアクセスできない可能性があります。

この脆弱性は、HTTP(S)要求での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、制限されたURLに認証なしでアクセスでき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。これらの脆弱性が修正済みのソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。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-webvpn-YROOTUW

このアドバイザリで説明されている脆弱性の詳細については、『Cisco Event Response:

Continued Attacks Against Cisco Firewall Platforms』を参照してください。

該当製品

脆弱性のある製品

この脆弱性の公開時点では、シスコデバイスでCisco Secure Firewall ASAソフトウェアまたはCisco Secure FTDソフトウェアの脆弱性が存在するリリースが実行されており、さらに、次の2つの表に示す1つ以上の脆弱性が存在する設定が実行されている場合に、シスコデバイスに影響が及びました。

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、左列に潜在的脆弱性のある Cisco Secure Firewall ASA ソフトウェアの機能を記載しています。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 ソフトウェアの機能	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 <interface name> client-services port <port_numbers>`

モバイル ユーザ セキュリティ (MUS)	`webvpn`
	` mus password`
	` mus server enable <port_number>`
	` mus <IPv4_address> <IPv4_mask> <interface_name>`

SSL VPN	`webvpn` ` enable <interface_name>`

Cisco Secure Firewall 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 Firewall 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 ソフトウェアの機能	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 <interface_name> client-services port <port_number>`
AnyConnect SSL VPN	`webvpn` ` enable <interface_name>`

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

シスコでは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策は一時的な解決策であると考えています。この脆弱性を完全に修復し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明されている修正済みソフトウェアにアップグレードすることを強く推奨します。

Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェア

お客様が Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアにおける脆弱性のリスクの有無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 9.20.3.4、Cisco Secure FTD ソフトウェアの場合は 7.4.2 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	

不正利用事例と公式発表

Cisco PSIRTでは、この脆弱性の不正利用が試みられたことを認識しています。これらの脆弱性が修正済みのソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。

出典

この脆弱性は 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、この調査をサポートしていただいた次の組織に感謝いたします。

- オーストラリア信号局オーストラリアサイバーセキュリティセンター
- カナダのサイバーセキュリティセンター（通信セキュリティ施設の一部）
- 英国National Cyber Security Center(NCSC)
- 米国サイバーセキュリティおよびインフラストラクチャセキュリティ機関(CISA)

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	エンドポイントを明確化。	要約	Final	2025年9月26日
1.0	初回公開リリース	—	Final	2025年9月25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、単独の転載や意訳を施した場合、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。