

Cisco適応型セキュリティアプライアンス (ASA)およびFirepower Threat DefenseソフトウェアのリモートアクセスSSL VPN認証の対象を絞ったDoS脆弱性



アドバイザリーID : cisco-sa-asa-vpn-4gYEWKkg

[CVE-2024-20493](#)

初公開日 : 2024-10-23 16:00

バージョン 1.0 : Final

CVSSスコア : [5.3](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwf34069](#)

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Cisco Firepower Threat Defense(FTD)ソフトウェアのリモートアクセスSSL VPN(SSL VPN)機能のログイン認証機能の脆弱性により、認証されていないリモートの攻撃者が数分間以降のVPNユーザ認証を拒否し、その結果、一時的なサービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、認証プロセス中のメモリリソースの効果的な処理に起因します。攻撃者は、巧妙に細工されたパケットを送信することで、この脆弱性を不正利用し、認証プロセスのリソース枯渇を引き起こす可能性があります。不正利用に成功すると、攻撃者はリモートアクセスSSL VPNユーザの認証を数分間にわたって拒否し、一時的な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。

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-asa-vpn-4gYEWKkg>

このアドバイザリーは、2024年10月に公開されたCisco ASA、FMC、および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一部です。これらのアドバイザリーとリンクの一覧については、『[シスコイベントレスポンス : Cisco ASA、FMC、およびFTDソフトウェアに関するセキュリティ](#)』

[アドバイザー公開半年刊2024年10月](#)』を参照してください。

該当製品

脆弱性のある製品

公開時点では、この脆弱性は、Cisco ASAまたはFTDソフトウェアの脆弱性が存在するリリースを実行していて、リモートアクセスSSL VPN機能が有効になっているシスコ製品に影響を与えました。

公開時点で脆弱性が確認されている Cisco ソフトウェアのリリースについては、このアドバイザーの「修正済みソフトウェア」セクションを参照してください。

SSL VPN 設定の確認

ソフトウェアでリモートアクセスSSL VPN機能が有効になっているかどうかを確認するには、show running-config CLIコマンドを使用します。次の表では、左の列にソフトウェア、中央の列に脆弱性のある機能を示します。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。脆弱性が存在するリリースを実行していて、その機能が有効になっているデバイスは、この脆弱性の影響を受けます。

シスコソフトウェア	影響を受ける機能	脆弱性の存在するコンフィギュレーション
ASA ソフトウェア	SSL VPN	webvpn enable
FTDソフトウェア ¹	SSL VPN	webvpn enable

1. リモートアクセスVPN機能は、Cisco Secure Firewall Management Center (以前の Firepower Management Center) ソフトウェアで Devices > VPN > Remote Accessの順に選択することで有効にできます。Cisco Firepower Device Managerで、リモートアクセスVPN機能を有効にするには、Remote Access VPNを選択します。

脆弱性を含んでいないことが確認された製品

このアドバイザーの[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、この脆弱性がCisco Secure Firewall Management Center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

[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。

Cisco ASA、FMC、および FTD ソフトウェア

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性に対するリスク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、[セキュリティ影響評価 \(SIR\)](#) 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 ASA ソフトウェアの場合は 9.16.2.11、Cisco 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	

注：Cisco ASAソフトウェアを実行しているCisco 3000シリーズ産業用セキュリティアプライアンス (ISA) については、Cisco ASAソフトウェアリリース9.16.4.67のリリースは延期されており、リリース9.16.4.70に置き換えられています。

Cisco 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 FMC upgrade guide](#)』を参照してください。

関連情報

最適な Cisco ASA、FMC、または FTD ソフトウェアリリースの決定方法については、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 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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-vpn-4gYEWMKg>

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	2024年10月23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。