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

Medium

アドバイザリーID : cisco-sa-asa-vpn-nyH3fhp
初公開日 : 2024-10-23 16:00
バージョン 1.0 : Final
CVSSスコア : 6.8
回避策 : No workarounds available
Cisco バグ ID : CSCwf34070

CVE-2024-20331

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)機能のセッション認証機能における脆弱性により、認証されていないリモートの攻撃者がユーザの認証を妨げる可能性があります。

この脆弱性は、認証プロセスのエントロピーが不十分であることに起因します。攻撃者は、認証ユーザのハンドルを特定し、それを使用して認証セッションを終了することにより、この脆弱性をエクスプロイトする可能性があります。不正利用に成功すると、攻撃者はユーザに認証プロセスを再起動させ、正当なユーザによるリモートアクセスVPNセッションの確立を阻止す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-asa-vpn-nyH3fhp

このアドバイザリは、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バンドルの一部です。これらのアドバイザリ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

ィアドバイザリ公開半年刊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ソフトウェアまたはCisco 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 ASA ソフトウェア設定の確認

脆弱性のある機能がソフトウェアで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。次の表の左列は、脆弱性のある Cisco ASA 機能を示します。右側の列に示す各機能の基本設定は、show running-config CLI コマンドを実行すると表示されます。デバイスが脆弱なリリースを実行しており、これらの機能のいずれかが有効になっている場合、そのデバイスは脆弱です。

Cisco ASA 機能	脆弱性の存在するコンフィギュレーション
SSL VPN	webvpn enable

Cisco FTD ソフトウェア設定の確認

脆弱性のある機能がソフトウェアで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。次の表の左列は、脆弱性のある Cisco FTD 機能を示します。右側の列に示す各機能の基本設定は、show running-config CLI コマンドを実行すると表示されます。デバイスが脆弱なリリースを実行しており、これらの機能のいずれかが有効になっている場合、そのデバイスは脆弱です。

Cisco FTD 機能	脆弱性の存在するコンフィギュレーション
SSL VPN[1]	webvpn enable

1. Cisco Secure Firewall Management Center(FMC)（以前のFirepower Management Center Software）のリモートアクセスVPN機能を有効にするには、 Devices > VPN > Remote Accessの順に選択します。Cisco Firepower Device Manager(FDM)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 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

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-nyH3fhp

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。