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トンネルにおけるDoS脆弱性



Advisory ID : cisco-sa-asaftd-tunnel-dos-s6mgkb75
CVE-2026-76418
初公開日 : 2026-10-28 19:15
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco Bug ID : CSCwx26625

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

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 VPN)サービスの脆弱性により、認証されていないリモートの攻撃者がデバイスの予期せぬリロードを引き起こし、その結果サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、トンネルグループでセカンダリ認証が設定されている場合の口ジックエラーが原因で発生します。攻撃者は、SSLリモートアクセスVPNに接続する際に、巧妙に細工された要求を送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は該当デバイスの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。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-asaftd-tunnel-dos-s6mgkb75

該当製品

脆弱性のある製品

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を実行しているシスコデバイスが、SSLリモートアクセスVPNログインサービスに到達でき、次のセクションで説明するトンネルグループスコープでセカンダリ認証が設定されている場合、この脆弱性の影響を受けます。

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。

SSLリモートアクセスVPN設定の確認

実行コンフィギュレーションにwebvpnキーワードが含まれており、SSL VPNが少なくとも1つのインターフェイスで有効になっている場合、そのコンフィギュレーションには脆弱性が存在します (次の表を参照) 。

Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェア機能	脆弱な設定
sslリモートアクセスVPN[1]	webvpn enable <*interface_name*>

1. Cisco Secure FTD ソフトウェアの場合、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 [デバイス (Devices)] > [VPN] > [リモートアクセス (Remote Access)] または Cisco Secure Firewall Device Manager （ FDM ）の [リモートアクセスVPN (Remote Access VPN)] から有効にすることができます。

トンネルグループ設定の決定

tunnel-group-list enableが設定されている場合、デフォルトのトンネルグループDefaultWEBVPNGroupを含むすべてのトンネルグループでsecondary-authentication-server-groupを確認します。

注：このチェックは、ログインページのグループリストに表示されるプロファイルに限定されません。

tunnel-group-list enableコマンドがない場合、またはno tunnel-group-list enableコマンドを使用して削除された場合は、デフォルトのトンネルグループDefaultWEBVPNGroupでsecondary-authentication-server-groupを確認します。これは、デフォルトのグループでセカンダリ認証が使用されている場合、グループリストを無効にしても公開が削除されないためです。

注：Cisco Secure FTDソフトウェアで、導入されたリモートアクセスVPNポリシーと、その結果Cisco Secure FMCソフトウェアまたはCisco Secure FDMで実行されるデバイスの設定を確認してください。該当する処理パスに到達するためにVPNログインが成功する必要はありませ

ん。

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、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- クラウド配信ファイアウォール(CDFW)
- クラウド提供のファイアウォール管理センター(cdFMC)
- セキュアアクセス(CSA)
- Cisco Secure FMC ソフトウェア

回避策

この脆弱性に対処する回避策はありません。ただし、ユーザ設定のトンネルグループリストまたはデフォルトのトンネルグループDefaultWEBVPNGroupでセカンダリ認証を無効にする緩和策があります。

ケース1:DefaultWEBVPNGroupでセカンダリ認証が使用されていない場合は、トンネルグループリストを無効にします。WebVPNコンフィギュレーションモードで、no tunnel-group-list enableと入力します。トンネルグループリストが無効になっていると、ユーザは指定されたリストから接続プロファイル（tunnel-group名）を選択することができなくなり、代わりに使用する正しいプロファイルを知る必要があります。

ケース2:DefaultWEBVPNGroupがセカンダリ認証を使用する場合は、no secondary-authentication-server-group CLIコマンドを使用してセカンダリ認証を削除します。セカンダリ認証を無効にすると、リモートアクセスVPNのセキュリティポスチャが低下します。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。お客様は、実装される回避策や緩和策が、お客様固有の導入シナリオと制限に基づいて、ネットワークの機能、パフォーマンス、セキュリティポスチャに悪影響を及ぼす可能性があることを認識しておく必要があります。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

このアドバイザリの「修正済みソフトウェア」セクションに記載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お勧めします。

修正済みソフトウェア

シスコでは、回避策や緩和策（該当する場合）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の一時的な解決策であると考えています。この脆弱性を修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイ

ザリに記載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。

修正リリース

次の表では、左の列にシスコソフトウェアのリリースを記載しています。右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco Secure Firewall ASA ソフトウェアリリース	第 1 修正済みリリース
9.16 以前	9.16.4.104
9.18	9.18.4.96
9.20	9.20.4.50
9.22	9.22.3.200
9.23	9.23.1.48
9.24	9.24.1.27 9.24.10.1

Cisco Secure FTD ソフトウェアリリース	第 1 修正済みリリース
7.0 以前	7.0.11
7.2	7.2.13
7.4	7.4.9
7.6	7.6.7
7.7	7.7.14
10.0	10.0.3
10.1	10.1.1

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

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	

Cisco Secure FTD デバイスのアップグレード手順については、該当の Cisco Secure FMC アップグレードガイドを参照してください。

その他のリソース

最適な Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各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新しいリリースが推奨される場合、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

2026 年 10 月、Cisco PSIRT は、この脆弱性が実際にエクスプロイトされていることを把握しました。こ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強くお勧めします。

送信元

この脆弱性は、Eric FernaldがCisco Technical Assistance Center(TAC)のサポートケースの解決中に発見しました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75

改訂履歴

バージョン	説明	セクション	Status	日付
1.0	初版リリース	—	Final	2026年10月28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ー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。