Cisco Secure Firewall Management CenterおよびSecure Firewall Threat Defenseソフトウェアのsftunnelの脆弱性

High

Advisory ID : cisco-sa-fmcftd-sftun-multivulns-WGVHOrN3
初公開日 : 2026-09-16 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco Bug ID : CSCws43281 CSCwu16917

CVE-2026-20323
CVE-2026-20295

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 Management Center(FMC)ソフトウェアおよびCisco Secure Firewall Threat Defense(FTD)ソフトウェアの複数の脆弱性により、認証されていない攻撃者がsftunnel認証バイパスまたはsftunnelサービス拒否(DoS)攻撃を実行する可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

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-fmcftd-sftun-multivulns-WGVHOrN3

このアドバイザリは、アドバイザリグループの一部です。これらのアドバイザリとリンクの一覧については、2026年9月16日発行のCisco Advance Notification, Security Advisoriesを参照してください。また、Cisco Secure Firewall製品の改善と修正に関するさらに詳しいドキュメントについては、『Cisco Secure Firewall Adaptive Security Appliance Software、Secure Firewall Threat Defense Software、およびSecure Firewall Management Centerソフトウェア強化リリース：2026年9月』を参照してください。

該当製品

脆弱性がある製品

これらの脆弱性は、デバイスの設定に関係なく、Cisco Secure FMC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。

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 Firewall Adaptive Security Appliance(ASA)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-2026-20295:Cisco Secure FMCソフトウェアおよびSecure FTDソフトウェアのsftunnelメモリ枯渇によるDoS脆弱性

Cisco Secure FMCソフトウェアおよびCisco Secure FTDソフトウェアのsftunnel inter-device communication protocol（IPC；デバイス間通信プロトコル）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、該当デバイスで使用可能なメモリを枯渇させる可能性があります。

この脆弱性は、sftunnel TLS接続セットアップ時のメモリリソースの不適切な管理に起因します。攻撃者は、接続セットアップ中に巧妙に細工されたsftunnel TLSフレームを該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は該当デバイスで使用可能なメモリを使い果たし、DoS状態が発生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。

バグID: CSCws43281
CVE ID：CVE-2026-20295
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-2026-20323:Cisco Secure FMCソフトウェアおよびSecure FTDソフトウェアのsftunnelにおける不正な認証バイパスの脆弱性

Cisco Secure FMCソフトウェアおよびCisco Secure FTDソフトウェアのsftunnel inter-device communication protocol(IPC)における脆弱性により、認証されていない隣接する攻撃者がピアデバイスになりすましてマネージャロールのレベル(root)でアクセスを取得する可能性があります。

この脆弱性は、sftunnel管理接続のTLS証明書の管理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TLS証明書を使用してsftunnelポートに接続することにより、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、攻撃者はルートアクセスで登録済みsftunnelピアになる可能性があります。

注：攻撃が成功するのは、sftunnel接続がダウンしているか、攻撃を実行できるだけの時間sftunnel接続を中断できる場合だけです。

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: CSCwu16917
CVE ID：CVE-2026-20323
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.3
CVSSベクトル：CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/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。これらの脆弱性を修正し、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。

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。

関連情報

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

シスコは、これらの脆弱性を報告していただいた独立したセキュリティ研究者であるMark

Pralat氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmcftd-sftun-multivulns-WGVHOrN3

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	2026年9月16日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

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。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

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 Technical Assistance Center（TAC）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。

ソフトウェアのアップグレードを検討する際には、関連す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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、シスコ セキュリティ アドバイザリ ページをご覧ください。Cisco 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評価します。詳細については、シスコのセキュリティ脆弱性ポリシーを参照してください。

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。