

Cisco Secure Firewall Management Center ソフトウェアの脆弱性



Advisory ID : cisco-sa-fmc-mulivulns-4PsnFwvx [CVE-2026-20343](#)
初公開日 : 2026-09-16 16:00 [CVE-2026-20344](#)
バージョン 1.0 : Final [CVE-2026-20341](#)
CVSSスコア : [9.1](#) [CVE-2026-20342](#)
回避策 : No workarounds available [CVE-2026-20340](#)
Cisco Bug ID : [CSCwu27275](#) [CSCwu36643](#) [CSCwu42586](#) [CSCwu16954](#) [CSCwu24501](#)

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)ソフトウェアの複数の脆弱性により、リモート攻撃者がルートアクセスを取得したり、機密ファイルをダウンロードしたり、SQLインジェクション攻撃を実行したり、サービス拒否(DoS)状態を引き起こしたり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、このアドバイザリの「[詳細情報](#)」の項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-fmc-mulivulns-4PsnFwvx>

本アドバイザリは一連のアドバイザリの一部です。アドバイザリの完全なリストおよび各アドバイザリへのリンクについては、「[Cisco Advance Notification for Publication of September 16, 2026, Security Advisories](#)」を参照してください。さらに、Cisco Secure Firewall 製品の改善と修正に関する詳細な情報については、「[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、Cisco Secure Firewall Threat Defense ソフトウェア、および Cisco 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

CVE-2026-20341：この脆弱性は、デバイス設定に関係なく、Cisco Secure FMCソフトウェアに影響を与えます。攻撃者は、管理対象のCisco Firepower Threat Defense(FTD)デバイスのルートアクセス権を持っている必要があります。

CVE-2026-20340およびCVE-2026-20342：これらの脆弱性は、デバイス設定に関係なく、Cisco Secure FMCソフトウェアに影響を与えます。攻撃者は、Security Analystロールなどの権限の低いユーザとしてログインできる必要があります。

CVE-2026-20343およびCVE-2026-20344：これらの脆弱性は、デバイス設定に関係なく、Cisco Secure FMC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。

脆弱性を含ま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、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- 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
- Cisco Secure Firewall Threat Defense (FTD) ソフトウェア

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別の脆弱性をエクスプロイトする必要はありません。また、これらの脆弱性のいずれかに該当するソフトウェアリリースでも、他の脆弱性には該当しない可能性があります。

脆弱性の詳細は以下のとおりです。

CVE-2026-20341：Cisco Secure FMC ソフトウェアの sftunnel 逆シリアル化によるルート権限でのコマンド実行の脆弱性

Cisco Secure FMC ソフトウェアの sftunnel デバイス間通信プロトコルにおける脆弱性により、認証されたりモートの攻撃者がルート権限を取得する可能性があります。

この脆弱性は、sftunnel の管理接続を介して、信頼できないデータの安全でない逆シリアル化起因します。攻撃者は、巧妙に細工された sftunnel リモートプロシージャコール (RPC) を送信することで、この脆弱性をエクスプロイト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、Cisco Secure FMC ソフトウェアおよびその高可用性ピアを実行しているデバイスでルート権限を取得する可能性があります。

この脆弱性をエクスプロイトするには、攻撃者は管理対象の Cisco FTD デバイスで有効な管理者ログイン情報を持っている必要があります。

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。

Bug ID : [CSCwu16954](#)

CVE ID : CVE-2026-20341

セキュリティ影響評価 (SIR) : 致命的

CVSS ベーススコア : 9.1

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVE-2026-20340 : Cisco Secure FMC ソフトウェアの逆シリアル化によるルート権限での任意のコマンド実行の脆弱性

Cisco Secure FMC ソフトウェアの脆弱性により、認証されたりモート攻撃者が、ルート権限レベルで任意のコマンドを実行する可能性があります。

この脆弱性は、Web 管理ユーザー制御データの安全でない逆シリアル化に起因します。攻撃者は、デバイスに対して認証を行い、巧妙に細工された HTTP ペイロードを送信することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は巧妙に細工されたペイロードを保存し、それを基盤となるオペレーティングシステムでルートとして実行する可能性があります。

この脆弱性をエクスプロイトするには、攻撃者は、少なくとも Security Analyst (読み取り専用) ロールが付与されたユーザーアカウントの有効なログイン情報を取得している必要があります。

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。

Bug ID : [CSCwu27275](#)

CVE ID : CVE-2026-20340

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 8.8

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2026-20344 : Cisco Secure FMC ソフトウェアの SQL インジェクションの脆弱性

Cisco Secure FMC ソフトウェアの Web ベースの管理インターフェイスの脆弱性により、認証されたりモートの攻撃者が影響を受けるデバイスに対して SQL インジェクション攻撃を実行する可能性があります。この脆弱性をエクスプロイトするには、攻撃者は、デバイスで Security Approver、Access Admin、または Network Admin のロールが付与された有効なアカウントを取得している必要があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、該当デバイスの Web ベース管理インターフェイスに細工された HTTP リクエストを送信することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は、データベースから任意のデータを取得したり、認証された管理者のセッションログイン情報を取得したり、該当デバイスで管理者権限を使用してアクションを実行したり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。

Bug ID : [CSCwu24501](#)

CVE ID : CVE-2026-20344

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 8.8

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2026-20342 : Cisco Secure FMC ソフトウェアにおける任意のファイルダウンロードの脆弱性

Cisco Secure FMC ソフトウェアの特定のファイルダウンロード API における脆弱性により、認証されたりモートの攻撃者が該当システムから任意のファイルをダウンロードする可能性があります。

この脆弱性は、ユーザー入力がサニタイズされていないために発生します。攻撃者は、巧妙に細工された HTTPS リクエストを送信することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者が該当システムから任意のファイルをダウンロードする可能性があります。

この脆弱性をエクスプロイトするには、攻撃者は、少なくとも Security Analyst (読み取り専用) ロールが付与されたユーザーアカウントの有効なログイン情報を取得している必要があります。

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。

Bug ID : [CSCwu42586](#)

CVE ID : CVE-2026-20342

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 7.7

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CVE-2026-20343 : Cisco Secure FMC ソフトウェアの情報開示およびディスク DoS の脆弱性

Cisco Secure FMC ソフトウェアの重要な API における脆弱性により、認証されていないリモー

トの攻撃者が機密ファイルをダウンロードしたり、無制限のディスク容量を使用したりする可能性があります。

この脆弱性は、重要な API に認証が欠けているために発生します。攻撃者は、API を繰り返し呼び出すことにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は制限されるべき機密ファイルをダウンロードし、ディスク容量を消費することで、デバイスが応答しなくなり、DoS 状態を引き起こす可能性があります。

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。

Bug ID : [CSCwu36643](#)

CVE ID : CVE-2026-20343

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 7.5

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/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	

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

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

これらの脆弱性を報告してくださった NATO Cyber Security Centre (NCSC) の Christophe Schleyden 氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-multivulns-4PsnFwvx>

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 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。