

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



Advisory ID : cisco-sa-fmc2-multivulns-

HXgcqRG

初公開日 : 2026-09-16 16:00

バージョン 1.0 : Final

CVSSスコア : [9.0](#)

回避策 : No workarounds available

Cisco Bug ID : [CSCwu27279](#) [CSCwu16965](#)

[CSCwu12566](#)

[CVE-2026-](#)

[76413](#)

[CVE-2026-](#)

[76412](#)

[CVE-2026-](#)

[76420](#)

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、セッション偽造またはセッション偽装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-fmc2-multivulns-HXgcqRG>

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 ソフトウェアに影響します。

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。さらに、いずれかの脆弱性の影響を受けるソフトウェア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-2026-76420: Cisco Secure FMC ソフトウェアのピアなりすましの脆弱性

Cisco Secure FMC ソフトウェアの Apache JServ Protocol (AJP) コネクタの内部設定に存在する脆弱性により、認証されていないリモートの攻撃者がピアデバイスを偽装する可能性があります。

この脆弱性は、ブート時の AJP コネクタの暗号化パラメータの不適切な初期化に起因します。攻撃者は、巧妙に細工されたパケットを AJP コネクタに送信することにより、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、攻撃者はルートとしてコマンドを実行し、該当デバイスの FMC REST API を完全に制御できるようになります。

注：この脆弱性の不正利用が可能なのは、Cisco Secure FMC ソフトウェアと Cisco Secure FTD ソフトウェア間の有効な sftunnel 接続がダウンしている場合だけです。

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: [CSCwu27279](#)

CVE ID : CVE-2026-76420

セキュリティ影響評価 (SIR) : 致命的

CVSS ベーススコア : 9.0

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

CVE-2026-76412: Cisco Secure FMCソフトウェアにおけるrootへの権限昇格の脆弱性

Cisco Secure FMCソフトウェアのリモート診断デバッグの脆弱性により、認証されたりリモート攻撃者がリモート診断デバッグサービスを有効にできる可能性があります。

この脆弱性は、リモート診断を呼び出しているユーザの特権レベルをチェックする際のエラーに起因します。攻撃者は、Webベースの管理インターフェイスまたはREST APIを介してデバイスに認証され、リモート診断デバッグを使用してユーザに昇格された特権を付与することで、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、攻撃者は特権をrootに昇格できます。

注：

- この脆弱性をエクスプロイトするには、攻撃者は該当デバイスで有効なユーザーログイン情報を持っている必要があります。
- CVSSv3.1攻撃の複雑度は、この脆弱性を完全に不正利用するために必要な複数の段階のプロセスのために高くなっています。

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: [CSCwu12566](#)

CVE ID : CVE-2026-76412

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 8.5

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

CVE-2026-76413: Cisco Secure FMCシングルサインオントークンフォージェリアカウントの脆弱性

Cisco Secure FMCソフトウェアのCisco Adaptive Security Device Manager(ASDM)シングルサインオン(SSO)ハンドラの脆弱性により、認証されていないリモート攻撃者がCisco ASDM管理者ユーザとしてログインできる可能性があります。

この脆弱性は、Cisco ASDM SSOトークンの不適切な管理に起因します。攻撃者は、セッショントークンフォージェリ技術を実行することで、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、攻撃者は管理者ユーザとしてログインし、このアクションを繰り返すことで、正当な管理者をASDMから無期限にロックアウトできます。

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: [CSCwu16965](#)

CVE ID : CVE-2026-76413

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 8.5

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

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 Nicholas Michael Kloster 氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc2-multivulns-HXgcqRG>

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。