

Cisco Secure Firewall Management CenterソフトウェアのXPATHインジェクションの脆弱性



アドバイザリーID : cisco-sa-fmc-xpathinj- [CVE-2025-](#)

COrThdMb

[20218](#)

初公開日 : 2025-08-14 16:00

バージョン 1.0 : Final

CVSSスコア : [4.9](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwj06006](#)

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 Secure Firewall Management Center(FMC)ソフトウェアのWebベースの管理インターフェイス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デバイスから機密情報を取得できる可能性があります。

この脆弱性は、不十分な入力検証に起因します。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巧妙に細工された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、攻撃者は影響を受けるデバイスから機密情報を取得できる可能性があります。

この脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャルを持っている必要があります。

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。

このアドバイザリーは、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-xpathinj-COrThdMb>

このアドバイザリーは、Cisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェアセキュリティアドバイザリーバンドルの2025年8月リリースの一部です。アドバイザリーとリンクの一覧については、『[Cisco Event Response: August 2025 Semiannual Cisco Secure Firewall ASA, Secure FMC, and Secure FTD Software Security Advisory Bundled Publication](#)』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、ロックダウンモードが有効になっている場合、この脆弱性はCisco Secure FMCソフトウェアに影響を与えました。ロックダウンモードはデフォルトで無効になっています。

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。

注：ロックダウンモードが無効の場合、Cisco Secure FMCソフトウェアを実行しているデバイスでexpert CLIコマンドを使用することで、ルートレベルのシェルアクセスを含むLinuxシェルアクセスをすぐに使用できます。ロックダウンモードの詳細については、『[Cisco Secure Firewall Management Center強化ガイド](#)』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](#)にリストされている製品だけがこの脆弱性の影響を受けることが知られています。

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。

- セキュアファイアウォール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
- Secure IPS(旧称：Cisco Next-Generation Intrusion Prevention System(NGIPS))

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完全なアップグレード ソリューション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 Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェア

お客様がCisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェアの脆弱性に

よる侵害の可能性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 9.16.2.11、Cisco Secure 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	

関連情報

最適なCisco Secure Firewall ASA、Secure FMC、またはSecure FTDソフトウェアリリースの判別に関しては、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) 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

この脆弱性は、シスコ内部でセキュリティ テストを実施中に、Sanmith Prakash によって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xpathinj-COrThdMb>

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	2025年8月14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、単独の転載や意識を施した場合、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。