

Cisco Secure Firewall Management Centerソフトウェアのクロスサイトスクリプティングの脆弱性



アドバイザリーID : cisco-sa-fmc-xss-dhJxQYZs [CVE-2024-20298](#)
初公開日 : 2024-10-23 16:00 [CVE-2024-20364](#)
バージョン 1.0 : Final [CVE-2024-20386](#)
CVSSスコア : [6.1](#)
回避策 : No workarounds available [CVE-2024-20264](#)
Cisco バグ ID : [CSCwi85823](#) [CSCwi78594](#) [CSCwi78593](#) [CSCwh69787](#) [CSCwh70866](#) [CVE-2024-20264](#)
[CSCwi61058](#) [CSCwi23477](#) [CSCwj19632](#) [CVE-2024-20300](#)
[CSCwf61443](#) [CSCwj77284](#) [CSCwj09456](#) [CVE-2024-20410](#)
[CSCwj11119](#) [CSCwi32423](#) [CVE-2024-20269](#)
[CVE-2024-20403](#)
[CVE-2024-20415](#)
[CVE-2024-20409](#)
[CVE-2024-20273](#)
[CVE-2024-20372](#)

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(旧Firepower 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複数の脆弱性により、認証されていないリモートの攻撃者が、該当デバイスのインターフェイスのユーザに対してクロスサイトスクリプティング(XSS)攻撃を実行する可能性があります。

これらの脆弱性は、Webベースの管理インターフェイスによるユーザ入力の検証が不十分であることに起因します。攻撃者は、巧妙に細工された入力を該当インターフェイスの各種データフィールドに挿入することにより、これら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、攻撃者はインターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザの機密情報にアクセスしたりする可能性があります。

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-xss-dhJxQYZs>

このアドバイザリは、2024年10月に公開されたCisco ASA、FMC、およびFTDソフトウェアセキュリティアドバイザリバンドルの一部です。これらのアドバイザリとリンクの一覧については、『[シスコイベントレスポンス：Cisco ASA、FMC、およびFTDソフトウェアに関するセキュリティアドバイザリ公開半年刊2024年10月](#)』を参照してください。

該当製品

脆弱性のある製品

このドキュメントの発行時点で、これらの脆弱性はCisco FMCソフトウェアに影響を与えていました。

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。

シスコでは、これらの脆弱性がCisco 適応型セキュリティアプライアンス (ASA) ソフトウェアまたはCisco Firepower Threat Defense (FTD) ソフトウェアに影響を及ぼさないことを確認しています。

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

[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。

Cisco ASA、FMC、および FTD ソフトウェア

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性に対するリスク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、[セキュリティ影響評価 \(SIR \)](#) 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 ASA ソフトウェアの場合は 9.16.2.11、Cisco 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
このアドバイザリのみ	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 ASA、FMC、または FTD 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 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спロイト事例とその公表は確認しておりません。

出典

CVE-2024-20264：この脆弱性は、シスコの社内セキュリティテストで発見されました。

CVE-2024-20269、CVE-2024-20300、CVE-2024-20403、およびCVE-2024-20409：これらの脆弱性は、シスコの社内セキュリティテストでAnanthapadmanabhan A氏によって発見されました。

CVE-2024-20273およびCVE-2024-20364：これらの脆弱性は、シスコのArunesh Shukla氏が社内セキュリティテストで発見したものです。

CVE-2024-20298：この脆弱性は、シスコのSanmith Prakash氏による社内セキュリティテストで発見されました。

CVE-2024-20372：この脆弱性を報告していただいたIeraeのGMO Cybersecurityの川根健太郎氏に感謝いたします。

CVE-2024-20386およびCVE-2024-20415：これらの脆弱性は、シスコの社内セキュリティテストでSatheeshkumar Eswaramoorthy氏によって発見されました。

CVE-2024-20410：この脆弱性は、内部セキュリティテストで発見されました。

URL

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

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	2024年10月23日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。