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と情報漏えいの脆弱性

Medium

アドバイザリーID : cisco-sa-fmc-xss-infodisc-RL4mJFer
初公開日 : 2024-10-23 16:00
バージョン 1.0 : Final
CVSSスコア : 5.4
回避策 : No workarounds available
Cisco バグ ID : CSCwj01321 CSCwj03056 CSCwi99692

CVE-2024-20377
CVE-2024-20388
CVE-2024-20387

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)の複数の脆弱性により、攻撃者がクロスサイトスクリプティング(XSS)攻撃を実行したり、該当デバイスの不正な情報にアクセス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-fmc-xss-infodisc-RL4mJFer

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-2024-20377:Cisco FMCソフトウェアで保存されるXSSの脆弱性

Cisco FMCソフトウェアのWebベース管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、インターフェイスのユーザに対してストアドXSS攻撃を実行する可能性があります。

この脆弱性は、Webベースの管理インターフェイスでユーザ入力が正しく検証されないことに起因します。攻撃者は、インターフェイスのユーザが巧妙に細工されたリンクをクリックするように仕向けることで、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、ブラウザベースの機密情報にアクセス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:CSCwj01321
CVE ID：CVE-2024-20377
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.4
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CVE-2024-20387:Cisco FMCソフトウェアのWebベース管理インターフェイスにおけるストアド

XSSの脆弱性

Cisco FMCソフトウェアのWebベース管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、XSS攻撃に使用する悪意のあるコンテンツを保存できる可能性があります。

この脆弱性は、Cisco FMCソフトウェアのWebベース管理インターフェイスにおける不適切な入力サニタイズに起因します。攻撃者は、悪意のあるリンクをクリックするようにユーザを誘導することで、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に対してストアドXSS攻撃を実行でき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:CSCwi99692
CVE ID：CVE-2024-20387
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.4
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CVE-2024-20388:Cisco FMCソフトウェアのAPI応答情報漏えいの脆弱性

Cisco FMCソフトウェアのパスワード管理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の有効なユーザ名を判別できる可能性があります。

この脆弱性は、パスワードの更新に伴う論理エラーが原因で発生します。攻撃者は、APIを使用して該当デバイスのパスワードを管理することにより、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、認証されていない攻撃者が設定されたユーザ名を特定でき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:CSCwj03056
CVE ID：CVE-2024-20388
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.3
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

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 FMCソフトウェアホットフィックス

シスコはこれらの脆弱性に対処するため、次のホットフィックスをリリースしました。このホットフィックスは、Cisco.comのSoftware Centerからダウンロードできます。

Cisco FMC ソフトウェア リリース	ホットフィックス名
7.0	Cisco_Firepower_Mgmt_Center_Hotfix_FI-7.0.6.4-1.sh.REL.tar

このホットフィックスのダウンロードとインストールの詳細については、『Cisco Firepowerホットフィックスリリースノート』を参照してください。

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されたリリース情報のみを検証します。

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 PSIRT は、このアドバイザリで説明されているいくつかの脆弱性に対して概念実証段階のエクスプロイトコードが利用可能であることを認識しています。

Cisco PSIRT では、このアドバイザリに記載されている脆弱性のいかなる悪用も認識していません。

出典

シスコは、これらの脆弱性を報告していただいたMohamed Tarek氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-infodisc-RL4mJFer

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、単独の転載や意訳を施した場合、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。