

# Cisco 適応型セキュリティアプライアンスおよび Firepower Threat Defense ソフトウェアのローカルコード実行における永続的な脆弱性



アドバイザーID : cisco-sa-asaftd-persist-rce-FLsNXF4h [CVE-2024-20359](#)

初公開日 : 2024-04-24 16:00

バージョン 1.0 : Final

CVSSスコア : [6.0](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwi98284](#)

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

VPN クライアントとプラグインのプリロードを可能にするレガシー機能は、Cisco 適応型セキュリティアプライアンス ( ASA ) ソフトウェアおよび Cisco Firepower Threat Defense ( FTD ) ソフトウェアで使用可能であり、認証されたローカルの攻撃者が root レベルの権限で任意のコードを実行できるという脆弱性があります。この脆弱性をエクスプロイトするには、管理者レベルの権限が必要です。

この脆弱性は、システムのフラッシュメモリから読み取るファイルの検証が不適切であることに起因します。攻撃者は、影響を受けるデバイスの disk0: ファイルシステムに巧妙に細工されたファイルをコピーして、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、攻撃者は該当デバイスの次回リロード後にこのデバイスで任意のコードを実行でき、それによりシステム動作が変更される可能性があります。挿入されたコードはデバイスの再起動後も存続する可能性があるため、シスコはこのアドバイザリのセキュリティ影響評価 ( SIR ) を [中 ( Medium ) ] から [高 ( High ) ] に引き上げました。

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-asaftd-persist-rce-FLsNXF4h>

このアドバイザリに記載されている脆弱性の詳細については、『[Cisco Event Response: Attacks](#)』

[Against Cisco Firewall Platforms』](#)を参照してください。

## 該当製品

### 脆弱性のある製品

この脆弱性による影響を受けるのは、シスコ製品で脆弱性のある Cisco ASA ソフトウェアまたは FTD ソフトウェアリリースを実行している場合です。したがって、特別な設定は必要ありません。

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およびサービスの[みが、こ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、この脆弱性が Cisco Firepower Management Center ( FMC ) ソフトウェアに影響を及ぼさないことを確認しました。

## 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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェアバージョンとフィーチャセットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

<https://www.cisco.com/c/en/us/products/end-user-license-agreement.html>

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限りです。通常、これは以前購入したソフトウェアのメンテナンスアップグレードです。無償のセキュリティソフトウェアアップデートによって、お客様に新しいソフトウェアライセンス、追加ソフトウェアフィーチャセット、またはメジャーリビジョンアップグレードに対する権限が付与されることはありません。

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。

[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。

## サービス契約をご利用でないお客様

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 TAC ( [https://www.cisco.com/c/ja\\_jp/support/web/tsd-cisco-worldwide-contacts.html](https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html) ) 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。

## 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	オン	

FTD デバイスのアップグレード手順については、『[Cisco Firepower Management Center Upgrade Guide](#)』を参照してください。

## 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](#)

## 推奨事項

この脆弱性に対する修正を含むリリースにアップグレードした後、デバイスの CLI で `dir disk0:` コマンドの出力を調べ、アップグレード前にはなかった新たな .zip ファイルが表示されていないかを確認することを推奨します。

アップグレード後に、`client_bundle_install.zip` やその他通常とは異なる名前の新たな .zip ファイルが表示された場合は、`copy` コマンドを使ってそのファイルをデバイスからコピーし、CVE-2024-20359 を参照の上 [psirt@cisco.com](mailto:psirt@cisco.com) までご連絡ください。このとき、デバイスの `dir disk0:` コマンドと `show version` コマンドの出力、およびデバイスから抽出した .zip ファイルを含めてメールでお送りください。

## 不正利用事例と公式発表

シスコは、この脆弱性がエクスプロイトされたことを確認しました。この脆弱性を解消するため、修正済みのソフトウェアへのアップグレードを強く推奨します。また、システムログを監視して、文書化されていない設定変更、スケジュールされていない再起動、および異常なログインアクティビティの兆候がないかを確認することを強くお勧めします。

## 出典

今回の調査にご協力いただきました、次の機関に感謝申し上げます。

- オーストラリア信号局 Australian Cyber Security Centre
- Canadian Centre for Cyber Security ( カナダ信安全保証部の機関 )
- 英国 National Cyber Security Center ( NCSC )
- 米国サイバーセキュリティ・インフラストラクチャ セキュリティ庁 ( CISA )

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h>

## 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 4 月 24 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。