

Cisco Firepower Threat Defenseソフトウェアの暗号化アーカイブファイルポリシーバイパスの脆弱性



アドバイザリーID : cisco-sa-ftd-archive-bypass-z4wQjwcN

[CVE-2024-20261](#)

初公開日 : 2024-05-22 16:00

バージョン 1.0 : Final

CVSSスコア : [5.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwf06818](#)

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 Firepower Threat Defense(FTD)ソフトウェアの暗号化されたアーカイブファイルの検査に使用されるファイルポリシー機能の脆弱性により、認証されていないリモートの攻撃者が、設定されたファイルポリシーをバイパスして暗号化されたアーカイブファイルをブロックする可能性があります。

この脆弱性は、暗号化されたアーカイブファイルの特定のクラスを検査する際の論理エラーが原因で発生します。攻撃者は、巧妙に細工された暗号化アーカイブファイルを該当デバイスを通じて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、攻撃者は暗号化されたアーカイブファイルを送信できる可能性があります。このファイルにはマルウェアが含まれている可能性があり、Cisco FTDデバイスでブロックおよびドロップされているはずですが。

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-ftd-archive-bypass-z4wQjwcN>

このアドバイザリーは、2024年5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ーバンドルの一部です。これらのアドバイザリー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5月』](#)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、暗号化されたアーカイブファイルをブロックするようにファイルポリシーが設定されている場合、この脆弱性はCisco FTDソフトウェアに影響を与えました。

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。

Cisco Firepower Management Center(FMC)デバイスでのCisco FTDソフトウェア設定の確認

Cisco FTDソフトウェアを実行しているCisco Firepower Management Center(FMC)デバイスのファイルポリシーが、暗号化されたアーカイブファイルをブロックするように設定されている場合、そのデバイスは影響を受けます。Cisco FMCデバイスで暗号化されたアーカイブファイルをブロックするようにファイルポリシーが設定されているかどうかを確認するには、次の手順を使用します。

1. 設定画面で、Policies > Access Control > Malware & Fileの順に選択します。
2. アーカイブファイルインスペクションオプションを表示するには、ファイルポリシーエディタでAdvanced Settingsを選択する。
3. Block Encrypted Archivesチェックボックスを確認します。オンにすると、デバイスは脆弱であると見なされます。

ファイルポリシーを使用してマルウェアをブロックする方法の詳細については、「[ファイルポリシーとファイルルール](#)」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 FMCソフトウェアには影響を与え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

[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	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、FTD、または FMC 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 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 Cisco TAC サポートケースの解決中に発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-archive-bypass-z4wQjwcN>

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5月22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。