Cisco適応型セキュリティアプライアンスおよびFirepower Threat Defenseソフトウェアのコマンドインジェクションの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-cmd-inj-ZJV8Wysm
CVE-2024-20358
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 : CSCwi90040

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 ASAソフトウェアおよびCisco Firepower Threat Defense(FTD)ソフトウェアで使用できるCisco適応型セキュリティアプライアンス(ASA)の復元機能の脆弱性により、認証されたローカルの攻撃者が、rootレベルの権限を使用して基盤となるオペレーティングシステムで任意のコマンドを実行する可能性があります。この脆弱性を不正利用するには、管理者レベルの権限が必要です。

この脆弱性は、復元時にバックアップファイルの内容が不適切にサニタイズされることに起因します。攻撃者は、該当デバイスに巧妙に細工されたバックアップファイルを復元することにより、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rootとして基盤となるLinuxオペレーティングシステムで任意のコマンド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。

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-cmd-inj-ZJV8Wysm

このアドバイザリに記載されている脆弱性についての詳細は、『Ciscoイベントレスポンス：Ciscoファイアウォールプラットフォームに対する攻撃』を参照してください。

該当製品

脆弱性のある製品

公開時点では、この脆弱性は、Cisco ASAソフトウェアまたはFTDソフトウェアの脆弱性のあるリリースを実行しているシスコ製品に影響を与えました。特別な設定は必要ありません。

注：Cisco FTDソフトウェアが影響を受けるのは、ロックダウンモードが有効でLinuxシェルアクセスが制限されている場合だけです。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。ロックダウンモードが無効になっている場合は、Cisco FTD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、root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 Threat Defense強化ガイド』を参照してください。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細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。

詳細

この脆弱性は、Cisco ASAシリーズの『General Operations CLI Configuration Guide』の「Software and Configurations」の章に記載されているCisco ASA restore CLIコマンドに影響を与えます。

『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「System Management」の章、および『Firepower Management Center Configuration Guide』の「Backup and Restore」の章に記載されているバックアップ復元機能は、この脆弱性の影響を受けません。

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、FMC、またはFTDソフトウェアリリースの決定に関するヘルプは、次の推奨

リリースに関する文書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、シスコの社内セキュリティテストで、Brian Stevens、Dany Rochefort、および Soumya Kalahastiによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm

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

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。