Cisco Secure Firewall適応型セキュリティアプライアンスおよびSecure Firewall Threat Defenseソフトウェアの認証済み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-ftd-cmd-inj-mTzGZexf
初公開日 : 2026-03-04 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwq01526 CSCwq01519 CSCwp81377 CSCwo73885
CVE-2026-20063
CVE-2026-20017
CVE-2026-20016
CVE-2026-20064

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 Secure Firewall Threat Defense(FTD)ソフトウェアのCLI機能における複数の脆弱性により、認証されたローカルの攻撃者が、昇格された特権でデバイスにコマンドを実行させたり、予期せぬリロードを引き起こしたりして、サービス妨害(DoS)状態を発生させ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-ftd-cmd-inj-mTzGZexf

このアドバイザリは、2026年3月に公開された『Cisco Secure Firewall ASA、Secure FMC、およびSecure 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。アドバイザリとリンクの一覧については、『Cisco Event Response: March 2026 Semiannual Cisco Secure Firewall ASA, Secure FMC, and Secure FTD Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

CVE-2026-20017、CVE-2026-20063、CVE-2026-20064：公開時点で、これらの脆弱性はデバイス設定に関係なくCisco Secure FTDソフトウェアに影響を与えています。

CVE-2026-20016：この脆弱性の公開時点で、Cisco Secure ASAソフトウェアおよびSecure FTDソフトウェアが次のCisco FXOSソフトウェアベースのデバイス上で実行されている場合、デバイス設定に関係なく、これらのデバイスが影響を受けました。

- プラットフォームモードで動作するFirepower 2100シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス

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 Secure Firewall Management Center(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。

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-2026-20064:Cisco Secure FTDソフトウェアの認証済みDoS脆弱性

Cisco Secure FTDソフトウェアのCLIの脆弱性により、権限の低い認証されたローカル攻撃者がデバイスのリロードを引き起こし、その結果DoS状態が発生する可能性があります。

この脆弱性は、ユーザーが指定したコマンド引数の入力検証が不十分であることに起因します。攻撃者は、特定のCLIコマンドに対して巧妙に細工された入力を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。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生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: CSCwq01526
CVE ID：CVE-2026-20064
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.5
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20016:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアにおける認証済みコマンドインジェクションの脆弱性

Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのCisco FXOSソフトウェアのCLI機能における脆弱性により、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上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、攻撃者は該当デバイスで有効な管理者クレデンシャルを持っている必要があります。

この脆弱性は、ユーザーが指定したコマンド引数の入力検証が不十分であることに起因します。攻撃者は、特定のCLIコマンドに対して巧妙に細工された入力を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、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。

バグID: CSCwo73885
CVE ID：CVE-2026-20016
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.0
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

CVE-2026-20017およびCVE-2026-20063:Cisco Secure FTDソフトウェアで認証されたコマンドインジェクションの脆弱性

Cisco Secure FTDソフトウェアのCLIにおける複数の脆弱性により、認証されたローカルの攻撃者が、基盤となるオペレーティングシステムでルートとして任意のコマンドを実行できる可能性があります。これらの脆弱性をエクスプロイトするには、攻撃者は該当デバイスで有効な管理者クレデンシャルを持っている必要があります。

これらの脆弱性は、ユーザが指定するコマンド引数の入力検証が不十分であることに起因します。攻撃者は、特定のCLIコマンドに対して巧妙に細工された入力を送信することにより、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、攻撃者はルートとして基盤となるオペレーティングシステムでコマンドを実行でき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。

Bug ID:CSCwq01519およびCSCwp81377
CVE ID：CVE-2026-20017 および CVE-2026-20063
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.0
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。これらの脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェア

お客様が Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアにおける脆弱性のリスクの有無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、セキュリティへの影響の評価（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 Secure Firewall ASA ソフトウェアの場合は 9.20.3.4、Cisco Secure FTD ソフトウェアの場合は 7.4.2 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 Secure FTD デバイスのアップグレード手順については、該当の Cisco Secure FMC アップグレードガイドを参照してください。

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スプロイト事例とその公表は確認しておりません。

出典

CVE-2026-20016：この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のKeane O'Kelleyによる内部セキュリティテストで発見されました。

CVE-2026-20017およびCVE-2026-20064：これらの脆弱性は、Cisco ASIGのKatherine Askewによる内部セキュリティテストで発見されました。

CVE-2026-20063：この脆弱性は、Cisco ASIGのKatherine AskewおよびKyle Ossingerによる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-ftd-cmd-inj-mTzGZexf

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	2026年3月4日

利用規約

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。