Cisco FXOSソフトウェアのCLIにおける任意のファイルの読み取りと書き込みの脆弱性

Medium

アドバイザリーID : cisco-sa-20200226-fxos-cli-file　CVE-2020-3166
初公開日 : 2020-02-26 16:00
最終更新日 : 2020-03-10 18:18
バージョン 1.2 : Final
CVSSスコア : 4.2
回避策 : No workarounds available
Cisco バグ ID : CSCvo42637 CSCvr09748

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 FXOSソフトウェアのCLIにおける脆弱性により、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(OS)上で任意のファイルの読み取りまたは書き込みを行う可能性があります。

この脆弱性は、入力に対する不十分な検証に起因します。攻撃者は、特定のCLIコマンドに巧妙に細工された引数を含めることにより、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、攻撃者は基盤となるOS上の任意のファイルの読み取りまたは書き込みを行え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-20200226-fxos-cli-file

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 FXOSソフトウェアの脆弱性のあるリリースを実行している次のシスコ製品に影響を与えました。

- Firepower 1000 シリーズ

- 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

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、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- MDS 9000 シリーズ マルチレイヤ スイッチ
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 3000 シリーズ スイッチ
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- Nexus 9000 シリーズ ファブリック スイッチ（アプリケーション セントリック インフラストラクチャ（ACI）モード）
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- UCS 6200 シリーズ ファブリック インターコネクト
- UCS 6300 シリーズ ファブリック インターコネクト
- UCS 6400 シリーズ ファブリック インターコネクト

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、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] 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完全なアップグレード ソリューション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 FXOS ソフトウェア

発行時点では、次の表に記載されているリリース情報は正確でした。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。

左の列はシスコソフトウェアリリースを示し、右の列はリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。

Firepower 1000 シリーズおよび 2100 シリーズ アプライアンスは、基盤となるオペレーティングシステムとして Cisco FXOS ソフトウェアを使用します。これは、Cisco ASA ソフトウェアの統合イメージバンドルまたは Cisco FTD ソフトウェアの統合イメージバンドルに含まれています。

Firepower 1000シリーズおよびFirepower 2100シリーズ用ASAソフトウェア：CSCvr09748

Cisco ASA ソフトウェア リリース	この脆弱性に対する最初の修正リリース
9.8	修正済みリリースに移行。
9.9	9.9.2.66
9.10	修正済みリリースに移行。
9.12	修正済みリリースに移行。
9.13	9.13.1.7

Firepower 1000シリーズおよびFirepower 2100シリーズ用FTDソフトウェア：CSCvr09748

Cisco FTD ソフトウェア リリース	この脆弱性に対する最初の修正リリース
6.2.2	修正済みリリースに移行。
6.2.3	6.2.3.16（2020 年 4 月）
6.3.0	修正済みリリースに移行。
6.4.0	修正済みリリースに移行。
6.5.0	6.5.0.4

Firepower 4100シリーズおよびFirepower 9300セキュリティアプライアンス用FXOSソフトウェア：CSCvo42637

Cisco FXOS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
2.2 より前	修正済みリリースに移行。
2.2	2.2.2.97

Cisco FXOS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
2.3	2.3.1.155
2.4	2.4.1.238
2.6	2.6.1.157
2.7	脆弱性なし

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fxos-cli-file

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	FTDリリースを更新。	修正済みソフトウェア	Final	2020年3月10日
1.1	ASAリリースを追加。	修正済みソフトウェア	Final	2020年3月6日
1.0	初回公開リリース	—	Final	2020 年 2 月 26 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。