UCSファブリックインターコネクト向けCisco Nexus 9300-FX3シリーズファブリックエクステンダにおける認証バイパスの脆弱性

Medium	**アドバイザリーID :** cisco-sa-elyfex-dos-gfvcByx **初公開日 :** 2023-02-22 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 5.3 **回避策 :** No workarounds available **Cisco バグ ID :** CSCwc52750	CVE-2023-20012

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 Nexus 9300-FX3シリーズファブリックエクステンダ(FEX)のCLIコンソールログイン認証における脆弱性は、UCSファブリックインターコネクトの導入で使用される場合、認証をバイパスするために物理的にアクセスする認証されていない攻撃者を可能にする可能性があります。

この脆弱性は、パスワード検証機能の不適切な実装に起因します。攻撃者は、該当デバイスのコンソールポートにログインすることで、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、攻撃者は認証をバイパスし、FEXに対してローカルな一連のコマンドを実行する可能性があり、その結果、デバイスのリブートおよびサービス妨害(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。

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-elyfex-dos-gfvcByx

このアドバイザリは、2023年2月のCisco FXOSおよびNX-OSソフトウェアセキュリティアドバイザリバンドル公開の一部です。アドバイザリの完全なリストとそのリンクについては、『Cisco Event Response: February 2023 Semiannual Cisco FXOS and NX-OS 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

この脆弱性は、Cisco Nexus 9300-FX3シリーズFEXが、Cisco UCS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とともに使用された場合に影響を与えます。

- UCS 6400 シリーズ ファブリック インターコネクト
- UCS 6500 シリーズ ファブリック インターコネクト

脆弱性が存在するのは、FEXモードで設定されている次のCisco Nexus 9000シリーズPIDのみです。

- N9K-C93180YC-FX3
- N9K-C93180YC-FX3S

注:これらのPIDは、Cisco Nexus 9000親スイッチとともにFEXモードで使用されている場合、またはスタンドアロンのトップオブラック(TOR)スイッチとして設定されている場合は、脆弱性の影響を受けません。

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。

Cisco Nexus 9000シリーズのPIDの確認

Intersight Management Mode(IMM)でFEX PIDを確認するには、次の例に示すように**show fex**コマンドを使用します。

IMM:

```
6500-FI#show fex
FEX 23:
  Name: FEX0023
    Model: N9K-C93180YC-FX3
  Serial: FDO250.....
State: Online
```

UCSM管理モード(UMM)でFEX PIDを確認するには、**show fex detail | grep PID**コマンドを使用して、次の例のようにCLIで実行します。

UMM:

```
6400-FI# show fex detail | grep PID
   PID: N9K-C93180YC-FX3
```

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。

- 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
- 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
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- Cisco Secure Firewall 3100 シリーズ
- 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

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 UCS 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た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ます。

Cisco UCS 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
4.0	脆弱性なし1
4.1	脆弱性なし1
4.2	4.2(2d)

1. Nexus 9300-FX3シリーズFEXは、Cisco UCSソフトウェアリリース4.2(1d)以降でのみサポートされています。

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

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-elyfex-dos-gfvcByx

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	2023年2月22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。