Cisco FXOSおよびNX-OSソフトウェアのセキュアな設定バイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-20190515-nxos-conf-bypass
初公開日 : 2019-05-15 16:00
最終更新日 : 2021-07-12 14:24
バージョン 1.3 : Final
CVSSスコア : 6.7
回避策 : No workarounds available
Cisco バグ ID : CSCvi96577 CSCvi96578 CSCvi96579 CSCvh20223 CSCvi96580 CSCvi96583 CSCvi96584

CVE-2019-1728

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ソフトウェアおよびCisco NX-OSソフトウェアのセキュア設定検証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、システムのブート時にroot権限で任意のコマンドを実行できる可能性があります。

この脆弱性は、ファイルシステムから永続的な設定情報を読み取る際に、システムファイルの適切な検証が行われないことに起因します。攻撃者は、デバイスへの認証を行い、永続的な設定ストレージを悪意のある実行可能ファイルで上書きすることで、この脆弱性をエクスプロイトする可能性があります。この不正利用により、攻撃者はシステムの起動時に任意のコマンドを実行する可能性があり、これらのコマンドはrootユーザとして実行されます。攻撃者は、デバイスに対する有効な管理者用のログイン情報を持っている必要があります。

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-20190515-nxos-conf-bypass

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、次のシスコ製品で脆弱性が存在する Cisco FXOS または NX-OS ソフトウェア リリースを実行している場合です。

- 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
- Nexus 3000 シリーズ スイッチ
- Nexus 3500 プラットフォーム スイッチ
- Nexus 3600 プラットフォーム 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 7700 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
- Nexus 9500 R シリーズ スイッチング プラットフォーム

脆弱性が存在するCisco FXOSまたはNX-OS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 2100 シリーズ
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- 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）
- 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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリ

リースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載のシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

2019年3月のCisco FXOSおよびNX-OSソフトウェアバンドルに対応する推奨リリースをすでに適用しているお客様は、アップグレード操作を行う必要はありません。バンドルされているアドバイザリのリストについては、『Cisco Event Response: 2019年3月Cisco FXOSおよびNX-OSソフトウェアのセキュリティアドバイザリバンドル公開』を参照してください。

2019年3月のバンドルに対応する推奨リリースを適用していないお客様は、このセクションの該当する表に示されているように、適切なリリースにアップグレードすることをお勧めします。次の表では、左の列に Cisco FXOS および NX-OS ソフトウェアのリリースを記載します。右の列

は、この脆弱性が修正済みの最初の推奨リリースです。

Firepower 4100シリーズおよびFirepower 9300セキュリティアプライアンス：CSCvi96584

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
2.4	2.4.1.101
2.4	2.4.1.101

MDS 9000シリーズマルチレイヤスイッチ：CSCvi96578

Cisco NX-OS 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
5.2	6.2(29)
6.2	6.2(29)
8.1	8.1(1b)
8.2	8.2(1)
8.3	8.3(1)

スタンドアロンNX-OSモードのNexus 3000シリーズスイッチおよびNexus 9000シリーズスイッチ：CSCvh20223

Cisco NX-OS 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
7.0(3)I7より前	7.0(3)I7(3)
7.0(3)I7	7.0(3)I7(3)
9.2(1)	脆弱性なし

Nexus 3500プラットフォームスイッチ：CSCvi96579

Cisco NX-OS 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
6.0(2)A8 より前	6.0(2)A8(11)
6.0(2)A8	6.0(2)A8(11)
7.0(3)	7.0(3)I7(3)
9.2	脆弱性なし

Nexus 3600 プラットフォーム スイッチおよび Nexus 9500 R シリーズ スイッチング プラットフォーム：0.CSCvi96577

Cisco NX-OS 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
7.0(3)	7.0(3)F3(5)
9.2	脆弱性なし

Nexus 5500、5600、6000 シリーズ スイッチ： 0.CSCvi96580

Cisco NX-OS 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
7.3	7.3(4)N1(1)
7.3	7.3(4)N1(1)

Nexus 7000および7700シリーズスイッチ：CSCvi96578

Cisco NX-OS 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 より前	6.2(22)
6.2	6.2(22)
7.2	7.3(3)D1(1)
7.3	7.3(3)D1(1)
8.0	8.3(1)
8.1	8.3(1)
8.2	8.3(1)
8.3	8.3(1)

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェア リリースの決定に関してサポートが必要な場合は、以下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 MDS シリーズ スイッチ
VMware 向け Cisco Nexus 1000V スイッチ
Cisco Nexus 3000 シリーズおよび 3500 シリーズ スイッチ
Cisco Nexus 5000 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9000 Series Switches
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS に最適な Cisco NX-OS ソフトウェア リリースの確認に関してサポートが必要な場合は、デバイスのリリース ノートに記載されている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。

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-20190515-nxos-conf-bypass

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.3	MDS 9000シリーズマルチレイヤスイッチの修正済みリリース情報を更新。	—	Final	2021年7月12日
1.2	UCSのバグID CSCvi96583を削除。	一般	Final	2020年2月24日
1.1	UCS 6200および6300シリーズファブリックインターコネクトを「脆弱性を含んでいないことが確認された製品」のリストに移動し、これらの製品の修正済みソフトウェアテーブルを削除。	脆弱性のある製品、脆弱性がないと確認された製品、修正済みソフトウェア	Final	2020年2月21日
1.0	初回公開リリース	—	Final	2019年5月15日

利用規約

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。