Cisco NX-OS ソフトウェアの NX-API におけるコマンド インジェクションに関する脆弱性

High

アドバイザリーID : cisco-sa-nxos-nxapi-cmdinject-ULukNMZ2

初公開日 : 2022-02-23 16:00

バージョン 1.0 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCvz81047 CSCvz80191

CVE-2022-20650

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 NX-OS ソフトウェアの NX-API 機能の脆弱性により、認証されたリモート攻撃者が、root 権限で任意のコマンドを実行できるようになります。

この脆弱性は、NX-APIに送信されるユーザ指定データの入力検証が不十分であることに起因します。攻撃者は、該当デバイスのNX-APIに巧妙に細工されたHTTP POST要求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。攻撃者がエクスプロイトに成功すると、*ルート権限を用いて、基盤となるオペレーティングシステムに対して任意のコードが実行される危険性があります。*

注：NX-API 機能はデフォルトで無効になっています。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-nxapi-cmdinject-ULukNMZ2

このアドバイザリは、2022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。これらのアドバイザリとリンクの一覧については、以下を参照してください。シスコのイベント対応：2022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。

該当製品

脆弱性のある製品

この脆弱性は、Cisco NX-OSソフトウェアの脆弱性のあるリリースを実行し、NX-API機能を有効にしている次のシスコ製品に影響を与えます。

- Nexus 3000シリーズスイッチ(CSCvz80191)
- Nexus 5500プラットフォームスイッチ(CSCvz81047)
- Nexus 5600プラットフォームスイッチ(CSCvz81047)
- Nexus 6000シリーズスイッチ(CSCvz81047)
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ(CSCvz80191)

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。

NX-API機能のステータスの確認

NX-API 機能はデフォルトで無効になっています。デバイスでNX-API機能が有効に設定されているかどうかを確認するには、**show feature | include nxapi**コマンドを使用して、機能が有効になっていることを確認します。次の例は、Cisco NX-OS ソフトウェアを実行しているデバイスで NX-API 機能が有効になっていることを示しています。

```
nxos# show feature | include nxapi
nxapi 1 enabled
```

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 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）

- 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。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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、お客様は以下のリンクに記載された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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

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。

Cisco.com の Cisco Support and Downloads ページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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。

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 Cisco Service Contract 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 POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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。

Cisco NX-OS ソフトウェア

お客様が Cisco NX-OS ソフトウェアの脆弱性による侵害の可能性を判断できるよう、シスコでは Cisco Software Checker を提供しています。このツールにより、特定の Cisco NX-OS ソフトウェアリリースに該当するシスコ セキュリティアドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。 また該当する場合、そのリリースに関するすべてのアドバイザリ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。

お客様は、Cisco Software Checker を使用して次の方法でアドバイザリを検索できます。

- ソフトウェア、プラットフォーム、および 1 つ以上のリリースを選択する
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- **show version コマンドの出力を入力する**

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリまたは 1 つ以上の特定のアドバイザリが含まれるように検索をカスタマイズできます。

また、次のフォームを使用して、Cisco NX-OS ソフトウェアとプラットフォームを選択、およびリリースを入力することで（例：Cisco Nexus 3000 シリーズ スイッチの **7.0(3)I7(5)、ACI モードの Cisco NX-OS ソフトウェアの 14.0(1h)）、シスコ セキュリティ アドバイザリの対象となるリリースであるかを判断することもできます。**

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating（SIR）が「重大」または「高」の脆弱性だけが含まれます。 「中間」の SIR 脆弱性の結果を含めるには、Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価（Impact Rating）] **ドロップダウンリストの [中間（Medium）]** チェックボックスをオンにします。

Cisco Nexus 3000 および 9000 シリーズ スイッチ SMU

シスコはこの脆弱性に対処する次の SMU もリリースしています。SMUは、Cisco.comのSoftware Centerからダウンロードできます。

Cisco NX-	Platform	SMU 名

OS ソフトウェア リリース		
7.0(3)I7(10)	Nexus 3000および9000シリーズスイッチ	nxos.CSCvz80191-n9k_ALL-1.0.0-7.0.3.I7.10.lib32_n9000.rpm
9.3(8)	Nexus 3000および9000シリーズスイッチ	nxos.CSCvz80191-n9k_ALL-1.0.0-9.3.8.lib32_n9000.rpm

これらのSMUのダウンロードとインストールの詳細については、Cisco Nexus 3000シリーズスイッチまたはCisco Nexus 9000シリーズスイッチのCisco NX-OSシステム管理設定ガイドの「ソフトウェアメンテナンスアップグレードの実行」セクションを参照してください。

その他のリソース

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際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 スイッチ向け Cisco Nexus 1000V
Cisco Nexus 3000 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 5600 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 ソフトウェアに最適なリリースを確認するには、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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-nxapi-cmdinject-ULukNMZ2

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	—	最終版	2022年2月23日

利用規約