Cisco NX-OS ソフトウェア NX-API サービス拒否の脆弱性

Medium	**アドバイザリーID :** cisco-sa-20190828-nxos-api-dos **初公開日 :** 2019-08-28 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 :** CSCvn31273 CSCvn57900 CSCvn26502	CVE-2019-1968

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 機能の脆弱性はリモート攻撃者非認証により NX-API システム プロセスは予想に反して再起動しますする可能性があります。

脆弱性は NX-API に送信 される 要求の HTTP ヘッダの不正確な検証が原因です。 攻撃者は影響を受けたデバイスの NX-API へ巧妙に細工された HTTP 要求を送信 することによってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者により NX-API サービスでサービス拒否 （DoS）状態を引き起こすことを可能にする可能性があります; ただし、NX-OS デバイス自体はまだ利用可能 なおよび通過 ネットワークトラフィックです。

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ました。 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-20190828-nxos-api-dos

該当製品

脆弱性のある製品

パブリケーションの時に、この脆弱性は Cisco NX-OS ソフトウェアの脆弱なリリースを実行して、NX-API 機能を有効に してもらったら以下のシスコ製品に影響を及ぼしました:

- 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

情報に関してはどのについての Cisco NX-OS ソフトウェアがリリースするかパブリケーションの時に脆弱、見ますこのアドバイザリの修正済みソフトウェアのセクションをでした。 最も完全な、現在の情報についてはこのアドバイザリの上でバグID の詳細 セクションを参照して下さい。

この脆弱性は、NX-API 機能が有効になっている Cisco NX-OS デバイスにのみ影響を与えます。 NX-API 機能はデフォルトで無効になっています。 該当デバイスで NX-API 機能が有効に設定されているかどうかを判断するにあたっては、管理者が Cisco NX-OS の CLI から **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-switch# 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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス
- VMware vSphere のための Nexus 1000 バーチャル エッジ
- 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

詳細

この脆弱性を不正利用するために、リモート攻撃者は外部 NX-API に巧妙に細工された HTTP または HTTPS パケットを送信 する必要があります。

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、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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。

修正済みリリース

パブリケーションの時に、次のテーブルのリリース情報は正確でした。 最も完全な、現在の情報についてはこのアドバイザリの上でバグID の詳細 セクションを参照して下さい。

左カラムは Ciscoソフトウェアリリースをリストし、リリースがこの アドバイザリに記載される脆弱性から影響を受けしたこの脆弱性のための修正が含まれていたかどうかリリースし、右の列は示します。

MDS 9000 シリーズ マルチレイヤ スイッチ： CSCvn26502

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	脆弱性なし
6.2	脆弱性なし
7.3	8.3(2)
8.1	8.3(2)
8.2	8.3(2)
8.3	8.3(2)
8.4	脆弱性なし

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： CSCvn31273

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)U4 より先に	脆弱性なし
6.0(2)U4、6.0(2)U5 および 6.0(2)U6	7.0(3)I4(9)
6.1(2)I1	脆弱性なし
6.1(2)I2 および 6.1(2)I3	7.0(3)I4(9)
7.0(3)I4	7.0(3)I4(9)
7.0(3)I7	7.0(3)I7(6)
9.2	9.2(3)
9.3	脆弱性なし

Nexus 3500 プラットフォーム スイッチ： CSCvn31273

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)A より先に	脆弱性なし
6.0(2)A8	6.0(2)A8(11a)
7.0(3)I7	7.0(3)I7(6)
9.2	9.2(3)
9.3	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: CSCvn31273

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)F	9.2(3)
9.2	9.2(3)
9.3	脆弱性なし

Nexus 5500 および 5600 プラットフォーム スイッチおよび Nexus 6000 シリーズ スイッチ: CSCvn57900

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
先により 7.1	脆弱性なし
7.1	7.3(5)N1(1)
7.2	7.3(5)N1(1)
7.3	7.3(5)N1(1)

Nexus 7000 および 7700 シリーズ スイッチ CSCvn26502

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
先により 6.2	脆弱性なし
6.2	脆弱性なし
7.2	7.3(4)D1(1)
7.3	7.3(4)D1(1)
8.0	8.2(3)
8.1	8.2(3)

8.2	8.2(3)
8.3	8.3(2)
8.4	脆弱性なし

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 シリーズ スイッチ
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 シリーズ スイッチ
Cisco Nexus 9000 シリーズ スイッチ
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）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-20190828-nxos-api-dos

改訂履歴

バージョン	説明	セクション	ステータス	Date

1.0	初回公開リリース		最終版	2019-August-28

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
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。