Cisco Nexus 3600および9500-Rシリーズスイッチングプラットフォームのレイヤ2ループにおけるDenial of Service(DoS)の脆弱性

アドバイザリーID : cisco-sa-nxos-ether-dos-Kv8YNWZ4
CVE-2026-20051
初公開日 : 2026-02-25 16:00
バージョン 1.0 : Final
CVSSスコア : 7.4
回避策 : No workarounds available
Cisco バグ ID : CSCwo94451

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 3600プラットフォームスイッチおよびCisco Nexus 9500-RシリーズスイッチングプラットフォームのイーサネットVPN(EVPN)レイヤ2入力パケット処理の脆弱性により、認証されていない隣接する攻撃者がレイヤ2トラフィックループを引き起こす可能性があります。

この脆弱性は、巧妙に細工されたレイヤ2入力フレームを処理する際の論理エラーに起因します。攻撃者は、巧妙に細工されたイーサネットフレームのストリームをターゲットデバイスを介して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。エクスプロイトに成功すると、攻撃者はレイヤ2 Virtual eXtensible LAN(VxLAN)トラフィックループを引き起こし、その結果サービス妨害(DoS)状態が発生する可能性があります。このレイヤ2ループは、ネットワークインターフェイスの帯域幅をオーバーサブスクライブする可能性があり、すべてのデータプレーントラフィックがドロップされます。この脆弱性を不正利用するには、攻撃者は該当デバイスにレイヤ2で隣接している必要があります。

注：この脆弱性のアクティブな不正利用を停止するには、巧妙に細工されたトラフィックを停止し、関連するすべてのネットワークインターフェイスをフラップさせるために、手動の介入が必要です。この脆弱性に関連するレイヤ2ループが疑われる場合は、Cisco Technical Assistance Center(TAC)または適切なサポートプロバイダーに問い合わせてください。

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-nxos-ether-dos-Kv8YNWZ4

このアドバイザリは、2026年2月に公開された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の一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: February 2026 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

脆弱性のあるCisco NX-OSソフトウェアリリースを実行し、EVPNが設定されている場合、この脆弱性は次のCisco Nexus 3600および9500-Rスイッチングプラットフォーム製品ID(PID)にのみ影響を与えます。

- N3K-C36180YC-R
- N3K-C3636C-R
- N9K-X96136YC-R
- N9K-X9636C-R
- N9K-X9636C-RX
- N9K-X9636Q-R

注：N9K-X9624D-R2 PIDは、この脆弱性の影響を受けません。

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。

インストールされているPIDの判別

インストールされているPIDを表示するには、show inventory CLIコマンドを使用します。

<#root>

```
9K-A# show inventory
NAME: "Chassis",  DESCR: "Nexus9500 C9508 (8 Slot) Chassis"
PID: N85-C8508           ,  VID: V02 ,  SN: FGE19270WQ4

NNAME: "Slot 1",  DESCR: "16x10G + 32x10/25G + 4x100G Module"
PID:
```

N9K-X96136YC-R

```
      ,  VID: V01 ,  SN: JAE222808LK

NAME: "Slot 2",  DESCR: "36p 100G Ethernet Module"
PID:
```

N9K-X9636C-RX

```
      ,  VID: V00 ,  SN: JAE211803N0
.
.
.
```

EVPN設定の確認

EVPNが設定されているかどうかを確認するには、show running-config | include nv overlay evpn CLIコマンドを使用します。このコマンドがデバイス設定に存在する場合、デバイスは脆弱であると見なされます (次の例を参照) 。

<#root>

```
n9K# show running-config | include "nv overlay evpn"
nv overlay evpn
```

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

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
- 「脆弱性のある製品」セクションに示されているモデル以外の 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
- ACI モードの Nexus 9000 シリーズ ファブリック スイッチ
- 「脆弱性のある製品」セクションに示されているモデル以外の Nexus 9000 シリーズ スイッチ
- Cisco Secure Firewall 200 シリーズ
- Cisco Secure Firewall 1200 シリーズ
- Cisco Secure Firewall 3100 シリーズ

- Cisco Secure Firewall 4200 シリーズ
- Cisco Secure Firewall 6100 シリーズ
- 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
- UCS 6500 シリーズ ファブリック インターコネクト
- UCS 6600 シリーズ ファブリック インターコネクト
- UCS Xシリーズダイレクトファブリックインターコネクト9108 100G

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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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に、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。 また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべて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。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco Nexus 3000 シリーズ スイッチの場合は 10.4(4)、ACI モードの Cisco NX-OS ソフトウェアの場合は 16.0(8e) です。
5. [チェック（Check）] をクリックします。

2		Critical,High,Medium

このアドバイザのみ	Cisco NX-OS ソフトウェア
あらゆるプラットフォーム	

Enter release number | Check

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
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

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ether-dos-Kv8YNWZ4

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	2026年2月25日

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。

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。