Cisco NX-OSソフトウェアのLink Layer Discovery Protocolにおける Denial of Service(DoS)の脆弱性

High

アドバイザリーID : cisco-sa-n3kn9k_aci_lldp_dos-NdgRrrA3
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 : CSCwi75282 CSCwq60777 CSCwq33193

CVE-2026-20010

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Link Layer Discovery Protocol(LLDP)機能の脆弱性により、認証されていない隣接する攻撃者がLLDPプロセスを再起動させ、該当デバイスの予期しないリロードを引き起こす可能性があります。

この脆弱性は、LLDPフレームの特定のフィールドの不適切な処理に起因します。攻撃者は、巧妙に細工されたLLDPパケットを該当デバイスのインターフェイスに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、攻撃者はデバイスのリロードを引き起こし、その結果サービス妨害（DoS）状態に陥る危険性があります。

注：LLDPはレイヤ2リンクプロトコルです。この脆弱性をエクスプロイトするには、攻撃者が影響を受けるデバイスのインターフェイスに、物理的または論理的に（たとえば、LLDPプロトコルを転送するように設定されたレイヤ2トンネルを介して）直接接続され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-n3kn9k_aci_lldp_dos-NdgRrrA3

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

この脆弱性は、次のシスコ製品で脆弱性が存在するソフトウェアリリースを実行しており、LLDP機能がグローバルに、および少なくとも1つのインターフェイスで有効になっている場合に、影響を与えます。

- Nexus 3000シリーズスイッチ(CSCwi75282)
- ACIモードのNexus 9000シリーズファブリックスイッチ(CSCwq33193)
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ(CSCwi75282)
- 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(CSCwq60777)

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。

スタンドアロンモードのCisco NX-OSソフトウェアのLLDPのステータスを確認する

スタンドアロンモードでCisco NX-OSソフトウェアを実行しているCisco Nexusスイッチでは、LLDP機能はデフォルトで無効になっています。LLDP機能が有効になっているかどうかを確認するには、デバイスのCLIでshow feature | include lldpコマンドを使用します。次の例は、LLDP機能が有効になっていることを示しています。

<#root>

```
switch#
show feature | include lldp

lldp                  1         enabled
```

LLDP機能が有効になっている場合、デフォルトではすべてのインターフェイスでLLDPも有効になります。着信LLDPパケットの処理は、no lldp receiveインターフェイスレベル設定コマンドを使用して、特定のインターフェイスで選択的に無効にできます。

特定のインターフェイスのLLDPのステータスを確認するには、デバイスのCLIでshow lldp interface ethernet module/interfaceコマンドを使用します。enable(rx)ステータスがYに設定されている場合、インターフェイスは着信LLDPパケットを受け入れます。この例を、次に示します。

<#root>

switch#

show lldp interface ethernet

1/1
Interface Information:

Enable

(tx/

rx

/dcbx): Y/

Y

/Y   Port Mac address: 00:a6:ca:b6:84:5a

ACIモードのCisco Nexus 9000シリーズファブリックスイッチ上のLLDPのステータスの確認

LLDP機能は、ACIモードのCisco Nexus 9000シリーズファブリックスイッチではデフォルトで有効になっており、完全に無効にすることはできません。LLDPは、すべてのファブリックポートとアクセスポートでデフォルトで有効になっています。

APIC NX-OSスタイルのCLIからno lldp receiveインターフェイスレベルの設定コマンドを使用するか、適用されたアクセスポリシーでLLDPを無効にすることにより、特定のアクセスポートで着信LLDPパケットの処理を選択的に無効にすることができます。詳細については、『シスコアプリケーションセントリックインフラストラクチャの基礎ガイド』の「アクセスポリシーの概要」セクションを参照してください。

特定のインターフェイスのLLDPのステータスを確認するには、デバイスのCLIでshow lldp interface ethernet module/interface コマンドを使用します。enable(rx)ステータスがYに設定されている場合、インターフェイスは着信LLDPパケットを受け入れます。この例を、次に示します。

<#root>

switch#

show lldp interface ethernet

1/1
Interface Information:

Enable

(tx/

rx

/dcbx): Y/

Y

/N   Port Mac address: 50:87:89:a2:10:39

Cisco UCS Xシリーズ直接ファブリックインターコネクト9108 100GでのLLDPのステータスの確認

Cisco UCS XシリーズDirect Fabric Interconnect 9108 100Gでは、LLDP機能はデフォルトで有効になっており、完全に無効にすることはできません。LLDPは、次のインターフェイスで常に有効になります。

- イーサネット アップリンク ポート（ネットワーク接続用にアップストリームスイッチに接続するネットワークインターフェイス）
- イーサネット ポート チャネル メンバ
- Fibre Channel over Ethernet（FCoE）アップリンクポート
- 管理インターフェイス(mgmt0)

LLDPは、ネットワーク制御ポリシーを通じて、サーバポート（Cisco UCS Managerドメイン内のサーバに提供されるインターフェイス）とアプライアンスポート（直接接続されたNFSストレージに接続するインターフェイス）でも有効にできます。詳細については、『Cisco UCS Managerネットワーク管理ガイド』の「ネットワーク制御ポリシーの設定」セクションを参照してください。

特定のインターフェイスのLLDPのステータスを確認するには、デバイスのCLIでconnect nxosコマンドを使用してから、show lldp interface ethernet module/interfaceコマンドを使用します。enable(rx)ステータスがYに設定されている場合、インターフェイスは着信LLDPパケットを受け入れます。この例を、次に示します。

<#root>

FI-A#

show lldp interface ethernet

1/1

Interface Information:

Enable

(tx/

rx

/dcbx):Y/

Y

/Y   Port Mac address: 00:c8:8b:84:a2:54

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
- 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
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 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

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	

Cisco UCS ソフトウェア

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。中央の列は、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、および脆弱性のある最初のリリースを示しています。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。

UCS 9108 100Gファブリックインターコネクト

Cisco UCS ソフトウェアリリース	UCS Managerモードの最初の修正済みリリース	Intersightマネージドモードの最初の修正済みリリース
4.3	4.3(6e)	4.3（6.260003）
6.0	脆弱性なし	脆弱性なし

シスコの 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済みリリース情報のみを検証します。

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 Cisco Technical Assistance Center（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-n3kn9k_aci_lldp_dos-NdgRrrA3

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。