Cisco FXOS および NX-OS ソフトウェア リンク レイヤ検出プロトコルのサービス妨害（DoS）の脆弱性

Medium

アドバイザリーID : cisco-sa-nxos-lldp-dos-z7PncTgt　CVE-2024-20294
初公開日 : 2024-02-28 16:00
バージョン 1.0 : Final
CVSSスコア : 6.6
回避策 : No workarounds available
Cisco バグ ID : CSCwi31871 CSCwe86457 CSCwf67408 CSCwf67409 CSCwi29934 CSCwf67411 CSCwf67468 CSCwf67412

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該当デバイスにサービス妨害(DoS)状態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し、認証されたユーザにCLI showコマンドまたはSimple Network Management Protocol(SNMP)要求を介して該当デバイスからLLDP統計情報を取得させることで、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LLDPサービスをクラッシュさせ、該当デバイスで実行を停止できる可能性があります。特定の状況では、LLDPのクラッシュにより該当デバイスのリロードが発生する場合があります。

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、攻撃者は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-nxos-lldp-dos-z7PncTgt

このアドバイザリは、2024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 2024 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

公開時点で、この脆弱性は、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て、LLDP機能がグローバルに、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受けました。

- Firepower 4100シリーズ(CSCwi29934)
- Firepower 9300セキュリティアプライアンス(CSCwi29934)
- MDS 9000シリーズマルチレイヤスイッチ(CSCwf67408)
- Nexus 3000シリーズスイッチ(CSCwe86457)
- Nexus 5500プラットフォームスイッチ(CSCwf67411)
- Nexus 5600プラットフォームスイッチ(CSCwf67411)
- Nexus 6000シリーズスイッチ(CSCwf67411)
- Nexus 7000シリーズスイッチ(CSCwf67409)
- ACIモードのNexus 9000シリーズファブリックスイッチ(CSCwi31871)
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ(CSCwe86457)
- UCS 6200シリーズファブリックインターコネクト(CSCwf67412)
- UCS 6300シリーズファブリックインターコネクト(CSCwf67412)
- UCS 6400シリーズファブリックインターコネクト(CSCwf67468)
- UCS 6500シリーズファブリックインターコネクト(CSCwf67468)

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

Cisco FXOSソフトウェアのLLDPのステータスの確認

LLDP機能は、Cisco FXOSソフトウェア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、管理インターフェイス(mgmt0)と、ブレードに接続する内部バックプレーンポートで常に有効になります。他のすべてのインターフェイスでは、デフォルトでLLDPが無効になっており、ネットワーク制御ポリシーを通じて有効にするオプションがあります。詳細については、『Cisco Firepower 4100/9300 FXOS Firepower Chassis Managerコンフィギュレーションガイド』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 fxos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次の例に示すように着信LLDPパケットを受け入れます。

```
<#root>

FPR#

show lldp interface ethernet

 1/1
Interface Information:

Enable

 (tx/

rx

/dcbx): Y/

Y

/Y    Port Mac address: 00:fc:ba:05:04:94
```

Cisco NX-OSソフトウェアを実行しているCisco MDSおよびNexusスイッチでのLLDPのステータスの確認

Cisco NX-OSソフトウェアを実行しているCisco MDSまたは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、show feature | include lldpコマンドをデバイスのCLIで実行します。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、インターフェイスレベルの設定コマンドno lldp

receive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次の例に示すように着信LLDPパケットを受け入れます。

<#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での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。

着信LLDPパケットの処理は、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選択的に無効にできます。詳細については、『Cisco Application Centric Infrastructure Fundamentals Guide』の「Access Policies Overview」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次の例に示すように着信LLDPパケットを受け入れます。

<#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ファブリックインターコネクト上のLLDPのステータスの確認

LLDP機能は、Cisco UCS 6200、6300、6400、および6500シリーズファブリックインターコネクト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ドメインのサーバに認識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次の例に示すように着信LLDPパケットを受け入れます。

```
<#root>

FI-A#

show lldp interface ethernet

 1/1/1
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
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ

詳細

この脆弱性が不正利用されると、LLDPサービスが繰り返しクラッシュし、該当デバイス上に1つ以上のコアファイルが生成される可能性があります。クラッシュが繰り返し発生すると、影響を受けるデバイスでLLDPサービスが実行されなくなるか、デバイスの全体的なリロードが発生する可能性があります。

該当するデバイスでLLDPサービスの実行が停止した場合、デバイスのCLIでshow lldpコマンドを実行すると、次の例に示すようにservice not enabledの出力が表示されます。

<#root>

switch#

show lldp traffic

Service not enabled

この状況では、LLDPサービスを再起動するために、影響を受けるデバイスのリロードが必要です。

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、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。

Cisco FXOS および NX-OS ソフトウェア

お客様が Cisco FXOS および 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 Firepower 4100シリーズセキュリティアプライアンスの場合は2.9.1.158、Cisco Nexus 3000シリーズスイッチの場合は7.0(3)I7(5)などです。
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 FXOS 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

発行時点では、次の表に記載されているリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列はシスコソフトウェアリリースを示し、右の列はリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。

UCS 6200、6300、6400、および6500シリーズ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	First Fixed Release（修正された最初のリリース）
4.1 より前	修正済みリリースに移行。
4.1	4.1(3m)
4.2	4.2(3j)
4.3	4.3(2b)

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された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
VMware 向け Cisco Nexus 1000V 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 PSIRT では、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は確認しておりません。

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-lldp-dos-z7PncTgt

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	2024年2月28日

利用規約

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。