# Cisco IOSおよびIOS XEソフトウェアのLink Layer Discovery Protocolにおける DoS脆弱性

アドバイザリーID : cisco-sa-lldp-dos-sBnuHSjT
CVE-2021-34703
初公開日 : 2021-09-22 16:00
バージョン 1.0 : Final
CVSSスコア : 6.8
回避策 : No workarounds available
Cisco バグ ID : CSCvv12527

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 IOSソフトウェアおよびCisco IOS XEソフトウェアのLink Layer Discovery Protocol(LLDP)メッセージパーサーの脆弱性により、攻撃者が該当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)状態が発生する可能性があります。

この脆弱性は、バッファの不適切な初期化に起因します。攻撃者は、次のいずれかの方法でこの脆弱性を不正利用する可能性があります。

- 認証されたリモートの攻撃者は、デバイスが特定の状態にある間に、CLIまたはSNMPのいずれかを介してLLDPネイバーテーブルにアクセスする可能性があります。
- 認証されていない隣接する攻撃者は、特定のLLDPフレームをネットワークに挿入し、デバイスの管理者またはデバイスを管理するネットワーク管理システム(NMS)がCLIまたはSNMPを介してデバイスのLLDPネイバーテーブルを取得するのを待機することで、LLDPネイバーテーブルを破損する可能性があります。
- SNMPの読み取り専用クレデンシャルを持ち、デバイスCLIに対する権限が低い、認証された隣接する攻撃者は、特定のLLDPフレームをネットワークに挿入し、CLIまたはSNMP経由でLLDPネイバーテーブルにアクセスすることにより、LLDPネイバーテーブルを破損する可能性があります。

エクスプロイトに成功すると、攻撃者は該当デバイスをクラッシュさせ、その結果デバイスのリロードが発生する可能性があります。

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-lldp-dos-sBnuHSjT

このアドバイザリは、Cisco IOSおよびIOS XEソフトウェアのセキュリティアドバイザリバンドル公開の2021年9月リリースの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2021 Semiannual Cisco IOS and IOS XE 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

公開時点では、この脆弱性は、Cisco IOSまたはIOS XEソフトウェアの脆弱性が存在するリリースを実行し、LLDP機能が有効になっているシスコデバイスに影響を与えました。

Cisco IOSおよびIOS XEソフトウェアでは、LLDP機能はデフォルトで無効になっています。

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。

## デバイス設定の確認

LLDP機能が有効になっているかどうかを確認するには、show running-config | include lldp runコマンドをデバイスのCLIで実行します。コマンドの出力が返された場合、デバイスはこの脆弱性の影響を受けます。空の出力は、LLDP機能が有効になっていないこと、およびデバイスがこの脆弱性の影響を受けないことを示します。

注：LLDP設定の判別にはshow lldpコマンドを使用しないでください。このコマンドを使用すると、このアドバイザリで説明されている脆弱性が引き起こされ、デバイスのリロードが発生する可能性があります。

## 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。

- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

# 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 IOS および IOS XE ソフトウェア

Cisco IOS ソフトウェアおよび IOS XE 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。

- ソフトウェアと 1 つ以上のリリースを選択します。
- 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、特定のアドバイザリ、または最新の公開資料に記載されているすべて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、次の形式を使用して、Cisco IOS または IOS XE ソフトウェアリリース（15.1(4)M2 や 3.13.8S など）を入力することで、そのリリースがシスコ セキュリティ アドバイザリの影響を受けているかどうかを判断できます。

Check

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.com にある 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）] の下にある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。

# 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-lldp-dos-sBnuHSjT

## 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 | 2021 年 9 月 22 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。