Cisco Webex Room PhoneおよびCisco Webex Share Link Layer Discovery Protocolのメモリリークの脆弱性

Medium	**アドバイザリーID :** cisco-sa-lldp-memlk-McOecPT **初公開日 :** 2023-01-11 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.5 **回避策 :** No workarounds available **Cisco バグ ID :** CSCwb22136 CSCwb25580	CVE-2023-20047

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 Webex Room PhoneおよびCisco Webex Shareデバイスの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、リソースの割り当てが不十分であることに起因します。攻撃者は、巧妙に細工されたLLDPトラフィックを該当デバ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、攻撃者は該当デバイスのメモリリソースを使い果たし、LLDPプロセスがクラッシュする可能性があります。該当するデバイスがLLDPのみをサポートするように設定されている場合、着信および発信コールが中断される可能性があります。デフォルトでは、これらのデバイスはCisco Discovery ProtocolとLLDPの両方をサポートするように設定されています。動作状態を回復するには、影響を受けるデバイスを手動で再起動する必要があります。

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-lldp-memlk-McOecPT

該当製品

脆弱性のある製品

この脆弱性は、次のシスコ製品でファームウェアの脆弱性が存在するリリースを実行していて、LLDP機能が有効になっている場合に、公開時点で影響を受けました。LLDP機能はデフォルトで有効になっています。

- Webex Room Phone
- Webex Share

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。

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。

回避策

この脆弱性に対処する回避策はありません。ただし、ネイバー探索でCisco Discovery ProtocolとLLDPの両方をサポートする展開では、この脆弱性に対処する緩和策があります。影響を受けるデバイスでLLDPを無効にすることができます。その後、デバイスはCisco Discovery Protocolを使用して、音声VLAN、電源ネゴシエーションなどの設定データを検出します。これは些細な変更ではなく、デバイスに対する潜在的な影響を評価し、この変更を社内に導入するための最適なアプローチを評価するために、企業に代わって努力する必要があります。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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。

修正済みリリース

発行時点では、次の表に示す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。

左側の列にはシスコソフトウェアリリース、右側の列に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が示されています。

Cisco Webex Room PhoneおよびCisco Webex Shareファームウェアリリース	First Fixed Release（修正された最初のリリース）
1.2.0 以前	1.2.0SR3

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。

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

シスコは、この脆弱性を報告していただいたQI-ANXIN GroupのCodesafe Team of LegendsecのQian Chen氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lldp-memlk-McOecPT

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	2023年1月11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。