Cisco IOS XE ワイヤレス コントローラ ソフトウェアの Cisco Discovery Protocol におけるサービス妨害（DoS）の脆弱性

アドバイザリーID : cisco-sa-ewlc-cdp-dos-fpeks9K
CVE-2025-20202
初公開日 : 2025-05-07 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 : CSCwm14282

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 XE ワイヤレス コントローラ ソフトウェアの脆弱性により、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、アクセスポイント（AP）の Cisco Discovery Protocol（CDP）ネイバーレポートがワイヤレスコントローラで処理される際の入力検証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 CDP パケットを AP に送信することにより、この脆弱性をエクスプロイト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 AP を管理するワイヤレスコントローラの予期しないリロードを引き起こし、その結果、ワイヤレスネットワークに影響を与える DoS 状態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-ewlc-cdp-dos-fpeks9K

このアドバイザリは、2025 年 5 月に公開された Cisco IOS ソフトウェアおよび IOS XE ソフトウェアリリースのセキュリティ 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: May 2025 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

この脆弱性は、Cisco 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、AP CDP が有効になっている、以下のシスコ製品に影響を与えます。

- クラウド向け Catalyst 9800-CL ワイヤレスコントローラ
- Catalyst 9300、9400、9500 シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ
- Catalyst 9800 シリーズ ワイヤレス コントローラ
- Catalyst AP上の組み込みワイヤレスコントローラ

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

デバイスによって管理されている任意の AP に対して CDP が有効になっている場合、そのデバイスはこの脆弱性の影響を受けます。CDP はデフォルトで有効になっており、ワイヤレスコントローラの [AP参加プロファイル (AP Join Profile)] セクションから設定できます。

デバイスが影響を受けるかどうかを判断するには、Administrator 権限を持つユーザーがデバイスの CLI に接続し、show running-config | section ap profile コマンドを発行します。デバイスに設定されているすべての AP 参加プロファイルの出力に no cdp の行が含まれている場合、そのデバイスは影響を受けません。1 つ以上の AP 参加プロファイルの出力にこの行が含まれていない場合、その AP 参加プロファイルの下にあるすべての AP に対して CDP が有効になり、デバイスが影響を受けます。

以下の例では、new-ap-profile で CDP が無効になっていますが、default-ap-profile で CDP が有効になっています。したがって、デバイスは影響を受けます。

<#root>

```
WLC#show running-config | section ap profile
ap profile new-ap-profile

no cdp


 ntp ip 0.0.0.0
 syslog host 255.255.255.255
ap profile default-ap-profile
 description "default ap profile"
 ntp ip 0.0.0.0
 syslog host 255.255.255.255
```

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。

- IOS ソフトウェア
- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア
- ワイヤレス LAN コントローラ（WLC）AireOS 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。

ただし、AP で CDP が必要ない場合は、管理者は Web ベースの管理 GUI または CLI から、すべての AP プロファイルで CDP を無効にすることができます。

Web ベースの管理 GUI からの AP CDP の無効化

Web ベースの管理 GUI から AP CDP を無効にするには、以下の手順を実行します。

1. [設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [AP参加（AP Join）] の順に選択します。
2. デバイスに設定されているすべての AP プロファイルに対して、プロファイル名をクリックしてから、[管理（Management）] > [CDPインターフェイス（CDP Interface）] の順に選択します。
3. [CDP状態（CDP State）] を [無効（Disabled）] に設定します。

管理 CLI からの AP CDP の無効化

ワイヤレスコントローラの管理 CLI から AP CDP を無効にするには、以下の手順を実行します。

1. 以下の例に示すように、show ap ap-join-profile summary コマンドを使用して AP プロファイル名を確認します。
   <#root>

```
WLC#

show ap ap-join-profile summary



Number of AP Profiles: 2
```

```
AP Profile Name                  Description
------------------------------------------------------------------------
new-ap-profile
default-ap-profile               default ap profile
```

2. コンフィギュレーション モードに切り替えます。以下の例に示すように、各 AP 参加プロファイルに対して、no cdp コマンドを入力します。
<#root>

```
WLC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
WLC(config)#ap profile new-ap-profile
WLC(config-ap-profile)#
```

no cdp

```
WLC(config-ap-profile)#ap profile default-ap-profile
WLC(config-ap-profile)#
```

no cdp

```
WLC(config-ap-profile)#end
```

設定を確認するには、このアドバイザリの「脆弱性のある製品」セクションの手順を参照してください。

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシ

スコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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完全なアップグレード ソリューション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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS 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。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。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. リリース番号（例：15.9(3)M2、17.3.3）を入力します。
3. [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

Enter release number | Check

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-ewlc-cdp-dos-fpeks9K

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	2025 年 5 月 7 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。