

ワイヤレスLANコントローラ用Cisco IOS XEソフトウェアのマルチキャストDNSにおけるDoS脆弱性



アドバイザリーID : cisco-sa-wlc-mdns-dos- [CVE-2024-4hv6pBGf](#) [20303](#)

初公開日 : 2024-03-27 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 : [CSCwf53124](#)

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

ワイヤレスLANコントローラ(WLC)用のCisco IOS XEソフトウェアのマルチキャストDNS(mDNS)ゲートウェイ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、mDNSクライアントエントリの不適切な管理に起因します。攻撃者は、ワイヤレスネットワークに接続し、特定のmDNSパケットの連続ストリームを送信することで、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、攻撃者はワイヤレスコントローラのCPU使用率を高め、アクセスポイント(AP)がコントローラへの接続を失ってDoS状態を引き起こす可能性があります。

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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-mdns-dos-4hv6pBGf>

このアドバイザリーは、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ーバンドル公開の2024年3月リリースの一部です。アドバイザリーとリンクの一覧については、『[Cisco Event Response: March 2024 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、mDNSゲートウェイ機能を有効にし、FlexConnectモードでAPを管理している次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

FlexConnectモードのAPがあるかどうかを確認するには、ワイヤレスコントローラに接続し、`show ap status | i Flex` CLIコマンド。

次の例は、FlexConnectモードのAPを使用するワイヤレスコントローラでこのコマンドを発行した場合の出力を示しています。

```
<#root>
```

```
C9800#show ap status | i Flex
```

```
my_ap_name          Enabled    FlexConnect      ES
```

出力がない場合、FlexConnectモードのAPはありません。

mDNSゲートウェイ機能が有効になっているかどうかを確認するには、ワイヤレスコントローラに接続し、`show mdns-sd summary` CLIコマンドを使用します。そのコマンドの出力に「mDNS Gateway: Enabled」と表示されている場合は、次の例に示すように、mDNSゲートウェイ機能が有効になっています。

```
<#root>
```

```
C9800#show mdns-sd summary
```

```
mDNS Gateway:
```

```
Enabled
```

Active Query: Enabled
Periodicity (in minutes): 30
Transport Type: Both IPv4 and IPv6

両方のコマンドの出力が前述の例と同様の場合、デバイスはこの脆弱性の影響を受けます。

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 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
- 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。

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ン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です。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。

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 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 (15.9(3)M2、17.3.3 など) 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

オン

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-wlc-mdns-dos-4hv6pBGf>

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3月27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、単独の転載や意識を施した場合、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。