# Ciscoアクセスポイントソフトウェアの断続的なIPv6ゲートウェイ変更の脆弱性

Medium

アドバイザリーID : cisco-sa-ap-ipv6-gw-tUAzpn9O
CVE-2025-20365
初公開日 : 2025-09-24 16:00
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : No workarounds available
Cisco バグ ID : CSCwm13005

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

シスコアクセスポイントソフトウェアのIPv6ルータアドバタイズメント(RA)パケット処理における脆弱性により、認証されていない隣接する攻撃者が該当デバイスのIPv6ゲートウェイを変更できる可能性があります。

この脆弱性は、ワイヤレスクライアントから受信するIPv6 RAパケットの処理における論理エラーに起因します。攻撃者は、ワイヤレスネットワークに関連付けて、巧妙に細工された一連のIPv6 RAパケットを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IPv6ゲートウェイを一時的に変更できる可能性があります。また、影響を受けるデバイスに関連付けられたワイヤレスクライアントでパケットが断続的に失われる可能性もあります。

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-ap-ipv6-gw-tUAzpn9O

## 該当製品

### 脆弱性のある製品

公開時点で、これらの脆弱性は、デバイス設定に関係なく、Ciscoアクセスポイントソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えました。

- 6300シリーズエンベデッドサービスアクセスポイント(AP)
- Aironet 1540 シリーズ AP
- Aironet 1560 シリーズ AP
- Aironet 1800 シリーズ AP
- Aironet 2800 シリーズの AP
- Aironet 3800 シリーズの AP
- Aironet 4800 AP
- Catalyst 9100 AP
- Catalyst IW6300 Heavy Duty シリーズ AP
- 1100サービス統合型ルータ(ISR)の統合型AP

このアドバイザリの公開時点で脆弱性が存在するシスコ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。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ないCiscoアクセスポイントシリーズには影響を与えないことを確認しました。

## 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

シスコでは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策は一時的な解決策であると考えています。この脆弱性を完全に修復し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明されている修正済みソフトウェアにアップグレードすることを強く推奨します。

### 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。

アクセスポイント（AP）のアップグレードプロセスでは、管理者は AP が登録されているワイヤレスコントローラをアップグレードする必要があります。次の表に示すように、該当する修正済みのソフトウェア リリースにアップグレードすることをお勧めします。

Catalyst 9800ワイヤレスコントローラまたはEmbedded Wireless Controller(EWC)によって管理されるアクセスポイント

| Cisco WLC IOS XEソフトウェア | First Fixed Release（修正された最初のリリース） |
|---|---|
| 17.8 以前 | 修正済みリリースに移行。 |
| 17.9 | 17.9.7 |
| 17.10 | 修正済みリリースに移行。 |
| 17.11 | 修正済みリリースに移行。 |
| 17.12 | 17.12.5 |
| 17.13 | 修正済みリリースに移行。 |
| 17.14 | 修正済みリリースに移行。 |
| 17.15 | 17.15.2 |
| 17.16 | 脆弱性なし |
| 17.17 | 脆弱性なし |
| 17.18 | 脆弱性なし |

シスコの 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済みリリース情報のみを検証します。

ワイヤレスLANコントローラ(WLC)またはMobility Express(ME)で管理されるアクセスポイント

Cisco WLC 3504、5520、8540、Mobility Express(ME)、および仮想WLCについては、ソフトウェアメンテナンスリリースの終了日がそれぞれで終了しています。このため、シスコは、このアドバイザリで説明している脆弱性に対処するためのソフトウェアのアップデートをリリースしておらず、今後もリリースする予定はありません。お客様には、これらの製品のサポート終了通知を参照することをお勧めします。

Ciscoワイヤレスソフトウェアバージョン8.10のサポート終了のお知らせ
3504ワイヤレスコントローラのサポート終了のお知らせ
5520ワイヤレスコントローラのサポート終了のお知らせ
8540ワイヤレスコントローラのサポート終了通知
Virtual Wireless Controllerのサポート終了のお知らせ

デバイスの移行を検討する際は、[シスコセキュリティアドバイザリ（Cisco Security Advisories）] 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

可能性の有無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、新しい製品がネットワークニーズに十分であること、新しい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しい製品で引き続き適切にサポートされることを確認する必要があります。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。

## 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 Technical Assistance Center(TAC)の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-ap-ipv6-gw-tUAzpn9O

## 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9月24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。