

# Catalyst アクセスポイント用 Cisco Embedded Wireless Controller のサービス妨害 ( DoS ) の脆弱性



アドバイザーID : cisco-sa-ap-ip-flood-dos-6hxxENVQ

[CVE-2022-20622](#)

初公開日 : 2022-04-13 16:00

バージョン 1.0 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvx88847](#)

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

Catalyst アクセスポイント用 Cisco Embedded Wireless Controller ( EWC ) ソフトウェアの IP 入力パケット処理の脆弱性により、認証されていないリモートの攻撃者がデバイスの予期せぬリロードを引き起こし、サービス拒否 ( DoS ) 状態に繋がる可能性があります。予期せぬリロードの前に、デバイスのトラフィック処理のパフォーマンスが低下したり、CPU 使用率が高くなったりすることがあります。

この脆弱性は、管理インターフェイスでの IP パケットの不適切なレート制限に起因します。攻撃者は、安定した IP トラフィックのストリームを高いレートで標的デバイスの管理インターフェイスに送信することで、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、攻撃者は標的デバイスのリロードを引き起こすことができるようになります。

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-ip-flood-dos-6hxxENVQ>

## 該当製品

### 脆弱性のある製品

この脆弱性は、Catalyst アクセスポイント用 Cisco Embedded Wireless Controller ソフトウエ

Aの脆弱性のあるリリースを実行しているシスコデバイスに影響を与えます。

注：脆弱性が存在するには、デバイスがデフォルト設定である必要があります。

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。

## 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。

- 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
- IOS ソフトウェア
- IOS XE 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。

## 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 [Cisco Support and Downloads 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](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。

### 修正済みリリース

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 アクセスポイント用 Cisco Embedded Wireless Controller ソフトウェアのリリース	First Fixed Release ( 修正された最初のリリース )
16.12 以前	影響なし。
17.2	影響なし。
17.3	17.3.4
17.4	修正済みリリースに移行。
17.5	修正済みリリースに移行。
17.6	17.6.1

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

この脆弱性は、シスコ内部でセキュリティテストを実施中、シスコのミロスラフ・ポポヴィッチによって発見されました。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-ip-flood-dos-6hxxENVQ>

## 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	2022年 4 月 13 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。