Ciscoアクセスポイントソフトウェアの制御されないリソース消費の脆弱性

Medium

アドバイザリーID : cisco-sa-ap-dos-capwap-DDMCZS4m
初公開日 : 2023-09-27 16:00
バージョン 1.0 : Final
CVSSスコア : 4.7
回避策 : No workarounds available
Cisco バグ ID : CSCwe75371

CVE-2023-20268

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アクセスポイント(AP)ソフトウェアのパケット処理機能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リソースを枯渇させる可能性があります。

この脆弱性は、特定のタイプのトラフィックを処理する際のリソース管理が不十分であることに起因します。攻撃者は、一連の特定のワイヤレスパケットを該当デバイスに送信することで、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、攻撃者は該当デバイスのリソースを消費する可能性があります。攻撃が継続すると、Control and Provisioning of Wireless Access Points(CAPWAP)トンネルが中断され、ワイヤレスクライアントトラフィックが断続的に失われ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-ap-dos-capwap-DDMCZS4m

該当製品

脆弱性のある製品

この脆弱性は、公開時点で、脆弱性のあるソフトウェアリリースを実行してい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 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
- Business 150および151 APとメッシュエクステンダ
- Catalyst 9100 AP
- Catalyst IW6300 Heavy Duty シリーズ AP
- 1100 サービス統合型ルータ（ISR）での統合 AP

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。

シスコでは、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 AP シリーズは、この脆弱性の影響を受けないことを確認しています。

回避策

この脆弱性に対処する回避策はありません。

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

公開時点では、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。

左の列はシスコソフトウェアリリースを示し、右の列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を示しています。

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、適切な修正済み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。

ワイヤレスLANコントローラまたはMobility Expressで管理されるAP

シスコワイヤレス LAN コントローラ ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
8.9 以前	修正済みリリースに移行。
8.10	8.10.190.0（2023年9月）

Catalyst 9800ワイヤレスコントローラまたは組み込みワイヤレスコントローラで管理されるAP

Cisco Catalyst 9800 ワイヤレス コントローラ ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
17.2 以前	修正済みリリースに移行。
17.3	17.3.8（2023年9月）
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	17.6.6
17.8	修正済みリリースに移行。
17.9	17.9.4
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	脆弱性なし

ビジネスワイヤレスAPソフトウェア

Cisco Business 150シリーズAPソフトウェアリリース	First Fixed Release（修正された最初のリリース）
10.5.2 以前	修正済みリリースに移行。
10.6.2	10.6.2.0（2023年9月）

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-dos-capwap-DDMCZS4m

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9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。