Cisco Aironetアクセスポイントソフトウェアのリソース枯渇に関するDoS脆弱性

Medium

アドバイザリーID : cisco-sa-airo-ap-dos-PPPtcVW
初公開日 : 2024-03-27 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 : CSCwh81027

CVE-2024-20354

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 Aironetアクセスポイント(AP)ソフトウェアの暗号化されたワイヤレスフレームの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、特定の不正なフレームをドロップする際のリソースの不完全なクリーンアップに起因します。攻撃者は、ワイヤレスクライアントとして該当APに接続し、ワイヤレス接続を介して特定の不正なフレ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、攻撃者は他のクライアントへのサービスの低下を引き起こし、完全なDoS状態につなが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-airo-ap-dos-PPPtcVW

該当製品

脆弱性のある製品

公開時点では、この脆弱性は、Cisco Aironet APソフトウェアの脆弱性のある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。

- 800および1900シリーズISR統合型AP

- Aironet 1530 シリーズ屋外用 AP
- Aironet 1552屋外AP
- Aironet 1570 シリーズ屋外用 AP
- Aironet 1700 シリーズ AP
- Aironet 2700 シリーズ AP
- Aironet 3700 シリーズ AP
- Industrial Wireless 3700シリーズ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。

- 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 100 シリーズ AP およびメッシュエクステンダ
- Business 200 シリーズ 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）での統合 AP
- Meraki AP
- 産業用ルータ用Wide Pluggable Form Factor Wi-Fi 6 APモジュール

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。

左の列にはシスコソフトウェアリリースが、右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、およびこれら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。

APをアップグレードするプロセスでは、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。

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）
8.4 以前	脆弱性なし
8.5.171.0よりも前の8.5リリース	脆弱性なし
8.5.171.0 以降	修正済みリリースに移行。
8.6	脆弱性なし
8.7	脆弱性なし
8.8	脆弱性なし
8.9	脆弱性なし
8.10.130.0よりも前の8.10リリース	脆弱性なし
8.10.130.0 以降	8.10.190.81

1.この修正は、特別なエンジニアリングイメージにのみ含まれています。このイメージは、TACサービスリクエストを通じてCisco TACから入手できます。

Catalyst 9800 Wireless Controller(WLC)またはEmbedded Wireless Controller(EWC)によって管理される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）
16.11 以前	脆弱性なし
16.12.4aよりも前の16.12リリース	脆弱性なし

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）
16.12.4a以降	修正済みリリースに移行。
17.1	脆弱性なし
17.2	脆弱性なし
17.3	17.3.9
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	17.6.7
17.7	修正済みリリースに移行。
17.8	修正済みリリースに移行。
17.9	17.9.5
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	17.12.2
17.13	脆弱性なし

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

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-airo-ap-dos-PPPtcVW

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。