Cisco Aironet アクセスポイントの WLAN 制御プロトコルにおけるパケットバッファリークに関するサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-airo-wpa-pktleak-dos-uSTyGrL
初公開日 : 2021-09-22 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 : CSCvu98674

CVE-2021-34740

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 WLAN 制御プロトコル（WCP）実装の脆弱性により、認証されていない隣接する攻撃者が該当デバイスのリロードを引き起こし、サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、該当デバイスが予期しない 802.11 フレームを受信した場合の誤ったエラー処理に起因します。攻撃者は、該当する AP のインターフェイスにワイヤレスネットワーク経由で特定の 802.11 フレームを送信することで、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、攻撃者はパケットバッファリークを引き起こす可能性があります。これにより、最終的にバッファ割り当てが失敗し、該当デバイスのリロードがトリガーさ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-airo-wpa-pktleak-dos-uSTyGrL

該当製品

脆弱性のある製品

この脆弱性は、Cisco Aironet AP ソフトウェアの脆弱性が存在す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す。

- 6300 シリーズ エンベデッド サービス AP
- Aironet 1540 シリーズ
- Aironet 1560 シリーズ
- Aironet 1800 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）での統合 AP

脆弱性が存在するのは、8.10、17.2、および 17.3 のコードトレインだけです。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シスコ アクセス ポイント シリーズには、この脆弱性が影響しないことを確認しました。

セキュリティ侵害の痕跡

この脆弱性がエクスプロイトされると、WCP デーモンプロセスが予期せず再起動し、AP がリロードされます。このイベントは、次の Syslog メッセージで示されます。

```
systemd[1]: wcpd.service: main process exited, code=dumped, status=6/ABRT
systemd[1]: Unit wcpd.service entered failed state.
systemd[1]: wcpd.service failed.
```

これらの Syslog メッセージを表示するには、show logging CLI コマンドを使用します。AP が予期せずリロードされ、これらの Syslog メッセージが存在する場合は、Cisco Technical Assistance Center（TAC）に連絡して、この脆弱性がデバイスでエクスプロイトされたか確認してください。

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。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ます。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。

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。

修正済みリリース

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。

ワイヤレス LAN コントローラまたは Mobility Express で管理されているアクセスポイント

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	脆弱性なし
8.10	8.10.162.01

1. 脆弱性が存在する最初のリリースはリリース 8.10.121.0 です。

Catalyst 9800 ワイヤレスコントローラまたは Catalyst アクセスポイントの組み込みワイヤレスコントローラ（EWC）で管理されているアクセスポイント

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 以前	脆弱性なし
17.2	修正済みリリースに移行します。[1]。
17.3	IOS XE アクセス ポイント サービス パック 17.03.04.CSCvz17868[2]
17.4 以降	脆弱性なし

1. 脆弱性が存在する最初のリリースはリリース 17.2.1 です。
2.この脆弱性に対する最初の修正リリースは、リリース17.3.4です。ただし、この脆弱性とCSCvz08781を修正するには、リリース17.3.4にアップグレードし、IOS XEアクセスポイントService Pack 17.03.04.CSCvz17868をインストールすることを推奨します。

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-airo-wpa-pktleak-dos-uSTyGrL

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	2021 年 9 月 22 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。