Cisco Aironet アクセスポイントおよび Catalyst 9100 アクセスポイント CAPWAP のサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-20191016-airo-capwap-dos
CVE-2019-15264
初公開日 : 2019-10-16 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 : CSCvo40697

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 および Catalyst 9100 アクセスポイント（AP）の Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルの実装に含まれる脆弱性により、隣接する認証されていない攻撃者が該当デバイスの予期しない再起動を引き起こし、その結果、サービス拒否（DoS）状態が発生する可能性があります。

この脆弱性は、CAPWAP メッセージ処理中の不適切なリソース管理に起因します。攻撃者は、短時間に大量の正当なワイヤレス管理フレームを該当デバ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、攻撃者はデバイスの再起動を引き起こし、AP に関連付けられたクライアントの DoS 状態が発生する危険性があります。

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-20191016-airo-capwap-dos

該当製品

脆弱性のある製品

本脆弱性は、Cisco NX-OS ソフトウェアの該当リリースを実行する次のシスコ製品に影響を与えます。

- 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

注：Catalyst 9100 APの場合、リリース8.9.100.0が最初にサポートされるリリースです。

脆弱性が存在するソフトウェア 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」の項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。

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、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] 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、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 Cisco Service Contract 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 POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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

この項の表に示すように、適切なリリースにアップグレードすることをお勧めします。本アドバイザリは以下のアドバイザリを含むコレクションの一部です。これらも考慮した上、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。

- cisco-sa-20191016-airo-capwap-dos:Cisco AironetアクセスポイントおよびCatalyst 9100アクセスポイントのCAPWAPにおけるサービス妨害の脆弱性
- cisco-sa-20191016-airo-pptp-dos:Cisco AironetアクセスポイントのポイントツーポイントトンネリングプロトコルにおけるDoS脆弱性
- cisco-sa-20191016-airoo-unauth-access:Cisco Aironetアクセスポイントの不正アクセスの脆弱性
- cisco-sa-20191016-wlc-ssh-dos:CiscoワイヤレスLANコントローラのセキュアシェルにおけるDoS脆弱性

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。中央の列は、リリースがこのアドバイザリに記載されている脆弱性に該当するかどうか、および、この脆弱性に対する修正を含む最初のリリースを示しています。右の列は、リリースがこのアドバイザリ集に記載された何らかの脆弱性に該当するかどうか、および、それらすべての脆弱性に対する修正を含む最初のリリースを示しています。

Cisco Aironet AP ソフトウェアのメジャー リリース	この脆弱性に対する最初の修正リリース	このアドバイザリ集で説明している脆弱性すべてに対する推奨リリース
8.2	8.5.151.0	8.5.151.0
8.3	8.5.151.0	8.5.151.0
8.4	8.5.151.0	8.5.151.0
8.5	8.5.151.0	8.5.151.0

Cisco Aironet AP ソフトウェアのメジャー リリース	この脆弱性に対する最初の修正リリース	このアドバイザリ集で説明している脆弱性すべてに対する推奨リリース
8.6	8.8.125.0	8.8.125.0
8.7	8.8.125.0	8.8.125.0
8.8	8.8.125.0	8.8.125.0
8.9	8.9.111.0	8.9.111.0
8.10	脆弱性なし	脆弱性なし

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、シスコ内部でセキュリティテストを実施中に Xiaomei Jia によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-airo-capwap-dos

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	2019 年 10 月 16 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。