

# Cisco Aironet アクセスポイントにおける不正アクセスの脆弱性



アドバイザリーID : [cisco-sa-20191016-airo-CVE-2019-](#)

unauth-access

[15260](#)

初公開日 : 2019-10-16 16:00

バージョン 1.0 : Final

CVSSスコア : [9.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvm54888](#)

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 ) ソフトウェアに含まれる脆弱性により、認証されていないリモートの攻撃者が、昇格された権限を使用してターゲットデバイスに不正にアクセスする可能性があります。

この脆弱性は、該当デバイス上での特定の URL に対する不十分なアクセス制御に起因します。攻撃者は、該当 AP から特定の URL を要求することにより、この脆弱性を 익스プロイトする可能性があります。 익스プロイトにより、攻撃者が昇格された権限を使用してデバイスにアクセスする危険性があります。攻撃者はすべての可能な設定オプションへのアクセスを許可されるわけではありませんが、機密情報を表示したり、一部のオプション ( ワイヤレスネットワーク設定など ) を任意の値で置き換えることが可能になる場合があります。また、攻撃者が AP を無効にして、AP に関連付けられたクライアントにサービス拒否 ( DoS ) 状態を発生させることも可能になります。

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。

このアドバイザリーは、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-unauth-access>

## 該当製品

脆弱性のある製品

この脆弱性は、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

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。](#)

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 9100 AP

## 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。

[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
8.0 以前	脆弱性なし	8.5.151.0
8.0	脆弱性なし	8.5.151.0
8.1	脆弱性なし	8.5.151.0
8.2	脆弱性なし	8.5.151.0
8.3	脆弱性なし	8.5.151.0
8.4	脆弱性なし	8.5.151.0
8.5	8.5.151.0	8.5.151.0
8.6	脆弱性なし	8.8.125.0
8.7	脆弱性なし	8.8.125.0
8.8	8.8.120.0	8.8.125.0
8.9	脆弱性なし	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 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-20191016-airo-unauth-access>

## 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。

本アドバイザー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。