CiscoワイヤレスLANコントローラのAireOSソフトウェアにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-cbw-dos-YSmbUqX3
CVE-2023-20251
初公開日 : 2023-09-27 16:00
バージョン 1.0 : Final
CVSSスコア : 6.1
回避策 : Yes
Cisco バグ ID : CSCwe32125

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 Wireless LAN Controller(WLC)AireOSソフトウェアのメモリバッファの脆弱性により、認証されていない隣接する攻撃者がメモリリークを引き起こし、最終的にデバイスのリブートが発生する可能性があります。

この脆弱性は、特定の条件下で接続している複数のクライアントによって引き起こされるメモリリークに起因します。攻撃者は、複数のワイヤレスクライアントを該当デバイスのアクセスポイント(AP)に接続させることで、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ブートを長時間にわたって引き起こし、その結果サービス妨害(DoS)状態が発生す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で確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-dos-YSmbUqX3

該当製品

脆弱性のある製品

公開時点で、この脆弱性は、Cisco WLC AireOS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て、ランダムMACフィルタリング機能が有効になっている次のシスコデバイスに影響を与えました。

- Mobility Express
- 仮想ワイヤレスLANコントローラ(vWLC)

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。

ランダムMACフィルタリングが有効になっているかどうかの確認

該当するデバイスでランダムMACフィルタリングが有効になっているかどうかを確認するには、デバイスにログインしてshow wlan idコマンドを使用します。

次の例は、ランダムMACフィルタリングがwlan 1で有効になっているCisco 3500シリーズワイヤレスコントローラでのshow wlan idコマンドの出力を示しています。

<#root>

```
(3500-3-AX) >show wlan 1


WLAN Identifier.................................. 1
Profile Name..................................... wpa2-dot1x
Network Name (SSID).............................. wpa2-dot1x
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled

Random MAC Filtering............................. Enabled
```

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。

- 2504ワイヤレスコントローラ
- 3504ワイヤレスコントローラ
- 5508ワイヤレスコントローラ
- 5520ワイヤレスコントローラ
- 8510ワイヤレスコントローラ
- 8540ワイヤレスコントローラ
- Flex 7510ワイヤレスコントローラ
- IOS ソフトウェア

- IOS XE ソフトウェア
- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

回避策

この脆弱性に対処する回避策はありません。管理者は、次のCLIコマンドを使用して、該当するデバイスでランダムMACフィルタリング機能を無効にすることができます。

```
3500-3-AX (config-wlan)# no local-admin-mac deny
```

この回避策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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

発行時点では、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。

Cisco WLC AireOS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
8.10.101 ~ 8.10.142.0	脆弱性なし

Cisco WLC AireOS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）
8.10.150 ~ 8.10.185	8.10.190.0

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-cbw-dos-YSmbUqX3

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

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。