Cisco Aironet アクセスポイントにおける FlexConnect マルチキャスト DNS のサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-aironet-mdns-dos-E6KwYuMx
CVE-2021-1439
初公開日 : 2021-03-24 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 : CSCvw63560

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 シリーズ アクセス ポイント ソフトウェアのマルチキャスト DNS（mDNS）機能の脆弱性により、認証されていない隣接する攻撃者が該当デバイスでサービス妨害（DoS）状態を引き起こす可能性があります。

この脆弱性は、mDNS の受信トラフィックの入力検証が不十分であることに起因します。攻撃者は、FlexConnect ローカルスイッチングモードで設定されたワイヤレスネットワーク、または設定された mDNS VLAN 上の有線ネットワークを介して、巧妙に細工された mDNS パケットを該当デバイスに送信することにより、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、攻撃者はアクセスポイント（AP）を再起動させ、DoS 状態を引き起こす可能性があります。

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-aironet-mdns-dos-E6KwYuMx

該当製品

脆弱性のある製品

この脆弱性は、Cisco Aironet シリーズ アクセス ポイント ソフトウェアの脆弱性が存在するリ

リースを実行しており、少なくとも 1 つのワイヤレスネットワークが FlexConnect ローカルスイッチングモードで設定されていて、そのワイヤレスネットワークのワイヤレスコントローラ、またはそのネットワークに関連付けられている有線 VLAN のいずれかで mDNS ゲートウェイ機能が有効になっている場合、次のシスコ製品に影響を及ぼします。

- 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
- Catalyst IW 6300 AP
- 1100 サービス統合型ルータでの統合 AP
- 6300 シリーズ エンベデッド サービス AP（ESW6300）

FlexConnect ローカルスイッチングモードのステータスの確認

ワイヤレスネットワークが FlexConnect ローカルスイッチングモードで実行されているかどうかを確認するには、次の手順を実行します。

1. ワイヤレスコントローラの管理 Web インターフェイスにアクセスします。
2. [設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [ポリシー（Policy）] を選択し、ワイヤレスネットワークに関連付けられているプロファイルを開きます。
3. [全般（General）] タブで、[中央スイッチング（Central Switching）] パラメータのステータスを確認します。

[中央スイッチング（Central Switching）] が無効になっている場合、ネットワークは FlexConnect ローカルスイッチングモードで動作しています。

mDNS ゲートウェイ機能のステータスの確認

mDNS ゲートウェイがワイヤレスネットワークで有効になっているかどうかを確認するには、次の手順を実行します。

1. ワイヤレスコントローラの管理 Web インターフェイスにアクセスします。
2. [設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [WLAN（WLANs）] の順に選択し、ワイヤレスネットワークを選択します。
3. [詳細設定（Advanced）] タブで、[mDNS モード（mDNS Mode）]ドロップダウンリストで選択した値を確認します。

mDNS ゲートウェイが有線 VLAN で有効になっているかどうかを確認するには、次の手順を実行します。

1. ワイヤレスコントローラの管理 Web インターフェイスにアクセスします。
2. [設定（Configuration）] > [サービス（Services）] > [mDNS] を選択します。
3. [mDNS Flex プロファイル（mDNS Flex Profile）] セクションで、プロファイル名をクリックします。
4. [VLAN（VLANs）] フィールドで、有効になっている VLAN を確認します。

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。

また、シスコ ワイヤレス コントローラおよび Cisco Mobility Express は、FlexConnect ワイヤレスネットワークでの mDNS ゲートウェイ機能の有効化をサポートしていないため、この脆弱性の影響を受けないことも確認しています。

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 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、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。

次の表に示す適切な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。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。お客様におかれましては、これらも考慮したうえでアップグレード ソリューション全体をご確認ください。

- cisco-sa-aironet-info-disk-BfWqghj:Cisco AironetアクセスポイントのFlexConnectアップグレードにおける情報漏えいの脆弱性
- cisco-sa-aironet-mdns-dos-E6KwYuMx:Cisco AironetアクセスポイントのFlexConnectマルチキャストDNSにおけるDoS脆弱性
- cisco-sa-ap-privesc-wEVfp8Ud:Ciscoアクセスポイントソフトウェアにおける任意のコード実行の脆弱性

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によって管理されているシスコアクセスポイント

Cisco Catalyst 9800 ワイヤレスコントローラ ソフトウェア リリース	この脆弱性に対する最初の修正リリース	アドバイザリ集に記載されているすべての脆弱性に対する最初の修正済みリリース
17.2 以前	脆弱性なし	修正済みリリースに移行。
17.3	17.3.3	17.3.3
17.4	修正済みリリースに移行。	17.5.1（2021 年 3 月）
17.5 以降	脆弱性なし	脆弱性なし

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

シスコ ワイヤレス コントローラおよび Cisco Mobility Express は、FlexConnect ワイヤレスネットワークでの mDNS ゲートウェイ機能の有効化をサポートしていないため、これらのアクセスポイントはこの脆弱性の影響を受けません。

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aironet-mdns-dos-E6KwYuMx

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 3 月 24 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。