シスコ 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

High

アドバイザリーID : cisco-sa-ap-privesc-wEVfp8Ud

CVE-2021-1449

初公開日 : 2021-03-24 16:00

バージョン 1.0 : Final

CVSSスコア : 6.7

回避策 : No workarounds available

Cisco バグ ID : CSCvw45507

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

シスコ アクセス ポイント ソフトウェアの起動ロジックの脆弱性により、認証されたローカルの攻撃者が起動時に署名されていないコードを実行する可能性があります。

この脆弱性は、システムのスタートアッププロセスを管理するコードの領域によって実行される不適切なチェックに起因します。攻撃者は、システムに保存されている特定のファイルを変更することで、この脆弱性をエクスプロイトし、既存の保護をバイパスする可能性があります。エクスプロイトに成功すると、攻撃者は起動時に署名されていないコードを実行し、該当デバイスのセキュアブートプロセスのソフトウェアイメージ検証チェック部分をバイパスする可能性があります。

注：この脆弱性をエクスプロイトするには、攻撃者はデバイスの開発シェル（devshell）にアクセスする必要があります。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-privesc-wEVfp8Ud

該当製品

脆弱性のある製品

この脆弱性は、シスコ 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いる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）

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。

詳細

Cisco AP-COS オペレーティングシステムを実行している AP には、devshell と呼ばれるデバッグおよびトラブルシューティング機能が含まれています。この機能は、基盤となる Linux オペレーティングシステムおよびデバッグ情報に、安全かつ管理された方法でアクセスできるように設計されています。

devshell 機能を使用することで、既存の **show または debug コマンドではアクセスできない情報を提供できます。**シスコの開発エンジニアは、デバイスで実行しているソフトウェアを更新することなく、devshell 機能を介して低レベルの情報を要求できます。また、再起動せずにデータを収集できるなどの利点もあります。再起動すると、エラー状態の問題を示す重要な値が失われて問題解決が遅れる可能性があります。

シスコの開発エンジニアによる devshell 機能へのアクセスは、お客様によって明示的に許可されている必要があります。お客様の同意なしにシスコの担当者がこの機能にアクセスすることはできません。

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 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

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-disc-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 アクセスポイントにおける FlexConnect マルチキャスト DNS のサービス妨害の脆弱性
- cisco-sa-ap-privesc-wEVfp8Ud：シスコ 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

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 LAN 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
8.5 以前	8.5.171.0	8.5.171.0
8.6 ~ 8.9	修正済みリリースに移行。	8.10.151.0
8.10	8.10.150.0	8.10.151.0

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
16.12 以前	16.12.5	16.12.5
17.1	修正済みリリースに移行。	17.3.3
17.2	修正済みリリースに移行。	17.3.3
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

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-privesc-wEVfp8Ud

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	—	最終版	2021 年 3 月 24 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。