Cisco Aironetアクセスポイントにおける任意のファイル上書きの脆弱性

Medium

アドバイザリーID : cisco-sa-ap-foverwrt-HyVXvrtb
CVE-2021-1423
初公開日 : 2021-03-24 16:00
バージョン 1.0 : Final
CVSSスコア : 4.4
回避策 : No workarounds available
Cisco バグ ID : CSCvu98274

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)におけるCLIコマンドの実装における脆弱性により、認証されたローカルの攻撃者がデバイスのフラッシュメモリ内のファイルを上書きする可能性があります。

この脆弱性は、特定のコマンドに対する不十分な入力検証に起因します。攻撃者は、巧妙に細工された引数を使用してコマンドを発行することにより、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でホストされている他のファイルにすでに存在するデータでファイルを上書きまたは作成でき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、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-foverwrt-HyVXvrtb

該当製品

脆弱性のある製品

公開時点では、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いる次のシスコ製品に影響を与えました。

- 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）

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。

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。

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

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、次の表に記載されている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。

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
8.4 以前	修正済みリリースに移行。
8.5	8.5.171.0
8.6 ~ 8.9	修正済みリリースに移行。
8.10	8.10.130.0

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
16.11 以前	修正済みリリースに移行。
16.12	16.12.5
17.1 - 17-2	修正済みリリースに移行。
17.3 以降	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

シスコは、この脆弱性を報告していただいたAtredis PartnersのChris Beores氏とRumbleのHD Moore氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-foverwrt-HyVXvrtb

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

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。