Cisco アクセスポイントの SSH 管理における特権昇格の脆弱性

アドバイザリーID : cisco-sa-cisco-ap-LLjsGxv
初公開日 : 2021-09-22 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCvw71885

CVE-2021-1419

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

複数の Cisco アクセスポイント（AP）プラットフォームの SSH 管理機能における脆弱性により、認証されたローカルのユーザが該当デバイスのファイルを変更し、昇格した権限を取得する可能性があります。

この脆弱性は、SSH 管理インターフェイス内のファイル操作のチェックが不適切なことに起因します。ネットワーク管理者ユーザは、SSH 管理を介して該当デバイスにアクセスし、設定を変更することで、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、攻撃者はルートユーザと同等の権限を取得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、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv

該当製品

脆弱性のある製品

この脆弱性は、アクセスポイントの SSH 管理機能が有効になっていて、脆弱性が存在するソフトウェア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
- ESW6300 シリーズ AP
- 1100 サービス統合型ルータでの統合アクセスポイント

SSH 管理が有効になっているかどうかの確認

注:SSH管理機能はデフォルトでは有効になっていません。

Cisco IOS XE ソフトウェアを使用しているお客様は、Cisco ワイヤレス LAN コントローラ の Web ベース管理インターフェイスで次の設定を確認することで、アクセスポイントで SSH 管理が有効になっているかどうかを確認できます。

[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [AP 参加（AP Join）] > [プロファイル名をクリック（Click on profile name）] > [SSH 設定の確認（Verify SSH Configuration）]

[SSH] ボックスがオンになっている場合、SSH 管理機能は有効になっています。

Cisco AireOS ソフトウェアを使用しているお客様は、[ワイヤレス（Wireless）] > [グローバル設定（Global Configuration）] を確認し、[グローバル Telnet SSH（Global Telnet SSH）] 設定を確認することで、管理対象アクセスポイントで SSH 管理がグローバルに有効になっているかどうかを確認できます。

また、show running-config コマンドを実行し、SSH State の値を調べることで、アクセスポイントで SSH 管理が有効になっているかどうかを確認できます。

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。

Cisco AireOS ソフトウェアまたは Cisco IOS XE ソフトウェアを実行する Cisco ワイヤレス LAN コントローラデバイスは、この脆弱性の影響を受けません。

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。Cisco IOS ソフトウェアを実行するアクセスポイントは、この脆弱性の影響を受けません。

詳細

この脆弱性をエクスプロイトするには、SSH 機能を有効にする必要があります。SSH 管理が有効になっていないデバイスは、エクスプロイトに対して脆弱ではありません。Cisco ワイヤレス LAN コントローラデバイスからアクセスポイントをリモートで管理する場合、SSH 管理機能は必要ありません。

影響を受けるアクセスポイントにログインしてこの脆弱性をエクスプロイトするためには、攻撃者はアクセスポイントでローカルに定義された SSH 管理ログイン情報を知っている必要があります。

回避策

この脆弱性に対処する回避策はありません。

ただし、SSH 管理機能を使用していないお客様は、この機能を無効にして、該当デバイスの攻撃ベクトルを閉じることができます。

この緩和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

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、管理者は 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。

次の表に示すように、該当する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。

ワイヤレス LAN コントローラで管理されるアクセスポイント

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
8.5 以前	影響なし。
8.10	8.10.151.0

Catalyst 9800 ワイヤレスコントローラで管理されるアクセスポイント

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
16.12	16.12.6
17.2 以前	修正済みリリースに移行。
17.3	17.3.3
17.4	修正済みリリースに移行。
17.5	影響なし。
17.6	影響なし。

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、この脆弱性の報告をしていただいた ITGL の Richard Atkin 氏に感謝いたします。

URL

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

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 9 月 22 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。