Cisco Unified Industrial Wireless Software for Ultra-Reliable Wireless Backhaul Access Pointのコマンドインジェクションの脆弱性

アドバイザリーID : cisco-sa-backhaul-ap-cmdinj-R7E28Ecs
CVE-2024-20418
初公開日 : 2024-11-06 16:00
バージョン 1.0 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID : CSCwk98052

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 Ultra-Reliable Wireless Backhaul(URWB)アクセスポイント向けCisco Unified Industrial Wireless SoftwareのWebベース管理インターフェイスにおける脆弱性により、認証されていないリモートの攻撃者が、基盤となるオペレーティングシステムに対するroot権限を使用してコマンドインジェクション攻撃を実行できる可能性があります。

この脆弱性は、Webベースの管理インターフェイスへの入力の検証が不適切なことに起因します。細工された HTTP 要求が該当システムの Web ベース管理インターフェイスに送信されると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、攻撃者は該当デバイスの基盤となるオペレーティングシステムでroot権限で任意のコマンドを実行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-backhaul-ap-cmdinj-R7E28Ecs

該当製品

脆弱性のある製品

この脆弱性は、脆弱性が存在するリリースを実行し、URWB動作モードが有効になっている次

のシスコ製品に影響を与えます。

- Catalyst IW9165Dヘビーデューティアクセスポイント
- Catalyst IW9165E高耐久性アクセスポイントおよびワイヤレスクライアント
- Catalyst IW9167Eヘビーデューティアクセスポイント

URWBモードで動作していないシスコ製品は、この脆弱性には該当しません。

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。

デバイス設定の確認

URWB動作モードが有効になっているかどうかを確認するには、show mpls-config CLIコマンドを使用します。コマンドが使用可能な場合、URWB動作モードが有効になり、デバイスはこの脆弱性の影響を受けます。コマンドが使用できない場合、URWB動作モードは無効になり、デバイスはこの脆弱性の影響を受けません。

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。

- 6300 シリーズ エンベデッド サービス アクセス ポイント
- Aironet 1540 シリーズ
- Aironet 1560 シリーズ
- Aironet 1810 シリーズ OfficeExtend アクセスポイント
- Aironet 1810w シリーズ アクセス ポイント
- Aironet 1815 シリーズ アクセス ポイント
- Aironet 1830 シリーズ アクセス ポイント
- Aironet 1850 シリーズ アクセス ポイント
- Aironet 2800 シリーズ アクセス ポイント
- Aironet 3800 シリーズ アクセス ポイント
- Aironet 4800 アクセスポイント
- Business 100シリーズアクセスポイントおよびメッシュエクステンダ
- Business 200シリーズアクセスポイント
- Catalyst 9100 シリーズ アクセスポイント
- Catalyst IW6300 Heavy Duty シリーズ アクセスポイント
- FMシリーズラジオトランシーバ
- IEC6400 エッジ コンピューティング アプライアンス
- ワイヤレス LAN コントローラ（WLC）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。

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。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右側の列は、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最初のリリースを示しています。このセクションの表に記載されている適切な修正済み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。

Cisco Unified Industrial Wireless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）
17.14 以前	修正済みリリースに移行。
17.15	17.15.1

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、シスコ内部でのセキュリティテスト中にシスコのDJ Coleによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-backhaul-ap-cmdinj-R7E28Ecs

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	2024年11月6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。