Cisco IEC6400ワイヤレスバックホールエッジコンピューティングソフトウェアのSSHにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-iec6400-Pem5uQ7v
初公開日 : 2026-01-21 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCws02393

CVE-2026-20080

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 IEC6400ワイヤレスバックホールエッジコンピューティングソフトウェアのSSHサービスの脆弱性により、認証されていないリモートの攻撃者がSSHサービスの応答を停止させる可能性があります。

この脆弱性は、SSHサービスに効果的なフラッド保護がないために存在します。攻撃者は、SSHポートに対してサービス拒否(DoS)攻撃を開始することにより、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DoS攻撃中にSSHサービスを応答不能にできる可能性があります。その他の動作はすべて、攻撃中は安定しています。

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-iec6400-Pem5uQ7v

該当製品

脆弱性のある製品

公開時点で、SSHサービスが有効になっているCisco IEC6400ワイヤレスバックホールエッジコンピューティングソフトウェアがこの脆弱性の影響を受けました。SSHサービスはデフォルトで有効になっています。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が他のCisco Ultra-Reliable Wireless Backhaulプラットフォームには影響を与え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。ただし、緩和策として、SSHサービスを必要としないお客様は、ssh-server disable CLIコマンドを使用するか、Web UIのMisc SettingsページでSSHのチェックボックスをオフにすることで、SSHサービスを無効にすることができます。

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、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策（適用可能な場合）を一時的な解決策と見なします。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正済みリリース

発行時点では、次の表に示す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。

左側の列にはシスコソフトウェアリリース、右側の列に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が示されています。

Cisco IEC6400ワイヤレスバックホールエッジコンピューティングソフトウェア	First Fixed Release（修正された最初のリリース）
1.1.0 以前	1.2.0

シスコの 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済み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

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-iec6400-Pem5uQ7v

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	2026年1月21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。