Cisco Small Business RV160およびRV260シリーズVPNルータにおけるリモートコマンド実行の脆弱性

Medium	**アドバイザリーID :** cisco-sa-rv-cmd-exe-n47kJQLE **初公開日 :** 2023-01-11 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 4.9 **回避策 :** No workarounds available **Cisco バグ ID :** CSCwd62514	CVE-2023-20045

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 Small Business RV160およびRV260シリーズVPNルータのWebベース管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、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任意のコマンドを実行する可能性があります。

この脆弱性は、ユーザ入力の検証が不十分であることに起因します。攻撃者は、該当デバイスのWeb ベース管理インターフェイスに巧妙に細工されたリクエストを送信することにより、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、攻撃者は該当デバイスで*root*レベルの権限を使用して任意のコマンドを実行できる可能性があります。この脆弱性をエクスプロイトするには、攻撃者が該当デバイスで有効な*管理者レベルのクレデンシャルを持っている必要があります。*

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-rv-cmd-exe-n47kJQLE

該当製品

脆弱性のある製品

この脆弱性は、公開時点で、リリース1.0.01.04より前のファームウェアリリースを実行している次のCisco Small Business RVシリーズルータに影響を与えました。

- RV160 VPN ルータ
- RV160W Wireless-AC VPN ルータ
- RV260 VPN ルータ
- PoE 対応 RV260P VPN ルータ
- RV260W Wireless-AC VPN ルータ

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。

注：これらのルータのWebベース管理インターフェイスは、デフォルトではローカルLAN接続を介して使用でき、そこで無効にすることはできません。インターフェイスは、リモート管理機能を有効にすることで、WAN インターフェイスを介して使用可能にすることもできます。デフォルトでは、リモート管理機能は、影響を受けるデバイスで無効になっています。

デバイス設定の確認

デバイスでリモート管理機能が有効になっているかどうかを確認するには、ローカル LAN 接続で Web ベースの管理インターフェイスを開き、**[基本設定 (Basic Settings)] > [リモート管理 (Remote Management)]** を選択します。[有効 (Enable)] **チェック ボックスがオンになっている場合、そのデバイスではリモート管理が有効になっています。**

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。

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。

- RV340 デュアル WAN ギガビット VPN ルータ
- RV340W デュアル WAN ギガビット Wireless-AC VPN ルータ
- RV345 デュアル WAN ギガビット VPN ルータ
- RV345PデュアルWANギガビットPoE VPNルータ

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ている脆弱性に対処するためのソフトウェアアップデートをリリースしておらず、リリースする予定もありません。Cisco Small Business RV160、

RV160W、RV260、RV260P、およびRV260W VPNルータは、サポート終了のプロセスに入っています。お客様には、これらの製品のサポート終了通知を参照することをお勧めします。

Cisco RV160およびRV260 VPNルータの販売終了およびサポート終了のお知らせ（全モデル）

デバイスの移行を検討する際は、[シスコ セキュリティ アドバイザリ（Cisco Security Advisories）] 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の有無と完全なアップグレード ソリューションを確認してください。

いずれの場合も、お客様は、新しい製品がネットワークのニーズを満たすのに十分であること、新しいデバイスに十分なメモリが搭載されていること、現在のハードウェアおよびソフトウェア構成が新しい製品によって引き続き適切にサポートされていることを確認する必要があります。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。

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Rivaille氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-cmd-exe-n47kJQLE

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	2023年1月11日

利用規約

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。