Cisco RV340、RV340W、RV345、およびRV345PデュアルWANギガビットVPNルータにおける任意のファイルアップロードの脆弱性

Medium	**アドバイザリーID :** cisco-sa-sb-rv-afu-EXxwA65V **初公開日 :** 2023-02-01 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 :** CSCwe04040	CVE-2023-20073

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 RV340、RV340W、RV345、およびRV345PデュアルWANギガビット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、認証されていないリモートの攻撃者が該当デバイスに任意のファイルをアップロードする可能性があります。

この脆弱性は、ファイルアップロードのコンテキストにおける承認の強制メカニズムが不十分であることが原因です。攻撃者は、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、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に任意のファイルをアップロードする可能性があります。

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-sb-rv-afu-EXxwA65V

該当製品

脆弱性のある製品

この脆弱性は、公開時点で、ファームウェアリリース1.0.03.29以前を実行している次のCisco RVシリーズSmall Businessルータに影響を与えました。

- 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 対応 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。

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。

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、管理者はデバイスにログインし、[Firewall] > [Basic Settings] で**RESTCONF**オプションを無効にすることで、Webベース管理インターフェイスの影響を受けるコンポーネント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、このアドバイザリで説明している脆弱性に対処するためのソフトウェアの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 RV340、RV340W、RV345、およびRV345PデュアルWANギガビット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 Small Business RV340およびRV345シリーズの販売終了およびサポート終了のお知らせ

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。

いずれの場合でも、新製品がお客様のネットワークニーズに十分対応していること、新規デバイスに十分なメモリが搭載されていること、および現在のハードウェアとソフトウェアの構成が新製品で引き続き適切にサポートされることを確認してください。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。

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X1cT34m LaboratoryのWangJincheng氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-afu-EXxwA65V

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2月1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。