

# Cisco RV340およびRV345デュアルWANギガビットVPNルータにおける認証されたリモートコード実行の脆弱性



アドバイザリーID : cisco-sa-sb-rv34x-rce-7pqFU2e [CVE-2024-20416](#)

初公開日 : 2024-07-17 16:00

バージョン 1.0 : Final

CVSSスコア : [6.5](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwk32012](#)

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およびRV345デュアルWANギガビットVPNルータのアップロードモジュールの脆弱性により、認証されたリモート攻撃者が該当デバイスで任意のコードを実行する可能性があります。

この脆弱性は、特定の HTTP リクエストを処理する際の境界チェック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、この脆弱性をエクスプロイトすることができます。エクスプロイトに成功すると、攻撃者はデバイスの基盤となるオペレーティングシステムでrootユーザとして任意のコードを実行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。

このアドバイザリーは、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-rv34x-rce-7pqFU2e>

## 該当製品

### 脆弱性のある製品

公開時点では、この脆弱性はCisco Small Businessルータファームウェアリリース1.0.03.24以降を実行している次のシスコ製品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。](#)

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。

- 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

## 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、今後もリリースする予定はありません。Cisco RV340およびRV345デュアル WANギガビットVPNルータは、サポート終了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

この脆弱性を報告していただいたVulnCheck, Inc.のJacob Baines氏に感謝いたします。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-7pqFU2e>

## 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7月17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、単独の転載や意識を施した場合、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。