# Cisco RV340、RV340W、RV345、およびRV345PデュアルWANギガビットVPNルータにおけるリモートコード実行およびDoS脆弱性

| | | |
|---|---|---|
| Medium | **アドバイザリーID :** cisco-sa-sb-rv-rcedos-7HjP74jD<br>**初公開日 :** 2023-01-11 16:00<br>**最終更新日 :** 2023-01-12 16:07<br>**バージョン 1.1 :** Final<br>**CVSSスコア :** 4.7<br>**回避策 :** No workarounds available<br>**Cisco バグ ID :** CSCwc84443 | CVE-2023-20007 |

**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 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の脆弱性により、認証されたリモート攻撃者が任意のコードを実行したり、デバイスのWebベース管理プロセスを予期せず再起動させたりして、サービス妨害(DoS)状態が発生する可能性があります。攻撃者は有効な管理者クレデンシャルを持っている必要があります。

この脆弱性は、ユーザーが Web ベースの管理インターフェイスで行った入力の検証が不十分であることに起因します。攻撃者は、細工された HTTP 入力を該当デバイスに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、攻撃者は基盤となるオペレーティングシステム上で*root*ユーザとして任意のコードを実行したり、Webベースの管理プロセスを再起動させて、DoS状態を引き起こす可能性があります。

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-sb-rv-rcedos-7HjP74jD

## 該当製品

### 脆弱性のある製品

この脆弱性は、公開時点で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

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。

#### デバイス設定の確認

これらのデバイスの Web ベース管理インターフェイスは、無効にできないローカル LAN 接続、またはリモート管理機能が有効になっている場合は WAN 接続を介して利用できます。デフォルトでは、リモート管理機能は、これらのデバイスで無効になっています。

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、Web ベース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。

- 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

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。

### 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 RV340およびRV345シリーズルータリリース | First Fixed Release（修正された最初のリリース） |
|---|---|
| 1.0.03.29 より前 | 1.0.03.29 |

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

シスコは、この脆弱性を報告していただいたMoyunSec TopBreaker LabsのLawhackzz氏とMoyunSecのBing Liu氏に感謝いたします。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 1.1 | ソースを更新。 | 出典 | Final | 2023年1月12日 |
| 1.0 | 初回公開リリース | - | Final | 2023年1月11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。