Cisco Small Business RV340、RV340W、RV345、およびRV345PデュアルWANギガビットVPNルータにおける特権昇格とリモートコマンド実行の脆弱性

High

アドバイザリーID : cisco-sa-rv34x-privesc-rce-qE33TCms
初公開日 : 2024-10-02 16:00
バージョン 1.0 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCwm27935 CSCwk99655

CVE-2024-20393 CVE-2024-20470

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における複数の脆弱性により、認証されたリモート攻撃者が該当デバイスの基盤となるオペレーティングシステムで権限を昇格させ、任意のコマンドを実行する可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコは、これらの脆弱性に対応する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。これは、該当製品がソフトウェアメンテナンスリリースの終了日を過ぎているためです。Cisco Product Security Incident Response Team(PSIRT)は、これらの製品に影響を与えるセキュリティの脆弱性がサポート終了日に達するまで、それらの脆弱性の評価と開示を続けます。

これら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-rv34x-privesc-rce-qE33TCms

該当製品

脆弱性のある製品

これらの脆弱性は、次のCisco RVシリーズSmall Businessルータに影響を与えます。

- 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

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、これらの脆弱性の影響を受けることが分かっています。

シスコでは、これらの脆弱性が次の Cisco RV Series Small Business ルータには影響を与えないことを確認しています。

- 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

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために、他の脆弱性をエクスプロイトする必要はありません。

脆弱性の詳細は以下のとおりです。

CVE-2024-20393:Cisco RV340、RV340W、RV345、およびRV345PデュアルWANギガビットVPNルータにおける特権昇格の脆弱性

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で権限を昇格させる可能性があります。

この脆弱性は、Webベースの管理インターフェイスが機密情報を開示するために存在します。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、攻撃者は権限をguestからadminに昇格できるようになります。

この脆弱性に対処する回避策はありません。

バグID:CSCwm27935
CVE ID：CVE-2024-20393
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.8
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2024-20470: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の脆弱性

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における脆弱性により、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。この脆弱性を不正利用するには、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、Webベースの管理インターフェイスがユーザ入力を十分に検証していないことに起因しています。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。不正利用に成功すると、攻撃者は基盤となるオペレーティングシステム上でルート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。

バグID:CSCwk99655
CVE ID：CVE-2024-20470
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.7
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

回避策

これら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

Cisco Small Business RV340、RV340W、RV345、およびRV345PデュアルWANギガビットVPNルータは、ソフトウェアメンテナンスリリースの終了日が過ぎています。このため、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。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

Cisco RV 160、RV260、RV345P、RV340W、RV260W、RV260P、および RV160W VPN ルータ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 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とその公表は確認しておりません。

出典

シスコは、これらの脆弱性を報告していただいたWebin DBappSecurity社のH4lo氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms

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10月2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。