Cisco RV110W、RV130W、およびRV215Wルータにおける HTTP要求バッファオーバーフローの脆弱性

Medium	**アドバイザリーID :** cisco-sa-20160615-rv3 **初公開日 :** 2016-06-15 16:00 **最終更新日 :** 2016-06-21 22:03 **バージョン 1.1 :** Final **CVSSスコア :** 6.8 **回避策 :** No workarounds available **Cisco バグ ID :** CSCux86669 CSCux86664 CSCux86675	CVE-2016-1398

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 RV110W Wireless-N VPNファイアウォール、Cisco RV130W Wireless-N多機能VPNルータ、およびCisco RV215W Wireless-N 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ターゲットシステムでバッファオーバーフローを引き起こし、その結果サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、ユーザがデバイスのWebベース管理インターフェイスを使用して該当デバイスを設定するときに送信されるHTTP要求のフィールドに対するユーザ入力の不適切なサニタイズに起因します。攻撃者は、巧妙に細工されたペイロードを含む設定コマンドを含むHTTP要求を送信することで、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、攻撃者はターゲットシステムでバッファオーバーフローを引き起こし、デバイスが予期せずリロードされ、DoS状態が発生する可能性があります。

シスコでは、本脆弱性に対処するファームウェア 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-20160615-rv3

該当製品

脆弱性のある製品

次のシスコ製品のすべてのリリースがこの脆弱性の影響を受けます。

- RV110W Wireless-N VPN ファイアウォール
- RV130W Wireless-N 多機能 VPN ルータ
- RV215W Wireless-N VPN ルータ

Webベースの管理インターフェイスは、ローカルLAN接続またはリモート管理機能を介してこれらのデバイスで使用できます。デフォルトでリモート管理機能は、影響を受けるデバイスでは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、デバイスのWebベース管理インターフェイスを開き、[Basic Settings] > [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

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

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

シスコでは、Cisco Bugsの修正済みソフトウェアに関する情報を提供しています。この情報には、 Cisco Bug Search Toolからアクセスできます。

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性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、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は新規リリースでも継続して適切なサポートが受けら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、この脆弱性を発見し、報告していただいたセキュリティ研究者のSamuel Huntley氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv3

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	修正済みリリースの提供状況を示すために更新されました。不具合検索ツールへのリンクを追加し、追加情報を取得。	修正済みソフトウェアの概要	Final	2016年6月21日
1.0	初回公開リリース	-	Final	2016年6月15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。