Cisco RV110W、RV130W、およびRV215Wルータコマンドシェルインジェクションの脆弱性

Medium	**アドバイザリーID :** cisco-sa-20160803-rv110_130w1 **初公開日 :** 2016-08-03 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.6 **回避策 :** No workarounds available **Cisco バグ ID :** CSCux73567 CSCuv90134 CSCux58161	CVE-2015-6396

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ルータのコマンドラインインターフェイス(CLI)コマンドパーサにおける脆弱性により、認証されたローカルの攻撃者が、デバイスで実行される任意のシェルコマンドを挿入する可能性があります。コマンドは、完全な管理者権限で実行されます。

この脆弱性は、CLIで入力されたユーザ制御入力パラメータの入力検証が不十分であることに起因します。攻撃者は、デバイスに認証され、特定のコマンドに巧妙に細工された入力パラメータを送信することで、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、認証された攻撃者が該当デバイスで任意のシェルコマンドまたはスクリプトを実行できる可能性があります。

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。 この脆弱性を軽減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-20160803-rv110_130w1

該当製品

脆弱性のある製品

次のシスコ製品は、最初の修正バージョンまで、すべてのファームウェアバージョンで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。

修正済みリリース

この脆弱性は、次のファームウェアバージョンで修正されています。

- RV110W Wireless-N VPNファイアウォール、リリース1.2.1.7
- RV130W Wireless-N多機能VPNルータ、リリース1.0.3.16
- RV215W Wireless-N VPNルータ、リリース1.3.0.8

ファームウェア アップデートは、Cisco.com の Software Center で、[製品（Products）] > [ルータ（Routers）] > [スモールビジネス向けルータ（Small Business Routers）] > [Small Business RVシリーズルータ（Small Business RV Series Routers）] の順に選択すればダウンロードできます。

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外部のセキュリティ研究者であるAdam Zielinski氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-rv110_130w1

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	â	Final	2016年8月3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。