# Cisco RV110W、RV130W、およびRV215Wルータのスタティッククレデンシャルの脆弱性

**Critical**

**アドバイザリーID :** cisco-sa-20160803-rv110_130w2

**初公開日 :** 2016-08-03 16:00

**バージョン 1.0 :** Final

**CVSSスコア :** 9.0

**回避策 :** No workarounds available

**Cisco バグ ID :** CSCux73557 CSCuv90139 CSCux58175

CVE-2015-6397

**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ルータの特定の設定でdefaultアカウントの脆弱性を使用すると、認証されたリモート攻撃者がデバイスに *root*アクセスする可能性があります。認証時に、アカウントに誤って *root*権限が付与される可能性があります。

この脆弱性は、デフォルトアカウントの不適切なロールベースアクセスコントロール(RBAC)に起因します。デフォルトのアカウントには *ルート*権限を付与してはならず、すべての場合で読み取り専用にする必要があります。攻撃者は、デフォルトアカウントを使用してターゲットデバイスにログインすることにより、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はデフォルトアカウントを使用してデバイスに認証され、 *ルート*権限が割り当てられ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_130w2

## 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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。このようなソフトウェアアップグレードをインストール、ダウンロード、アクセス、またはその他の方法で使用することにより、お客様はシスコのソフトウェアライセンス(http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html)の条項に従うことに同意したことになります。

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

**サービス契約をご利用でないお客様**

シスコから直接購入したがシスコのサービス契約を結んでいないお客様、およびサードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できないお客様は、Cisco Technical Assistance Center(TAC)(http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html)に連絡してアップグレードを入手する必要があります。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

**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_130w2

## 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。