Cisco RV110W、RV130W、および RV215W ルータの管理インターフェイスにおけるサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-20190619-rvrouters-dos

初公開日 : 2019-06-19 16:00

バージョン 1.0 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvo21850 CSCvo39082 CSCvo39087

CVE-2019-1843

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における脆弱性により、認証されていないリモートの攻撃者が該当デバイスをリロードして、サービス妨害（DoS）状態を発生させる可能性があります。

この脆弱性は、Web ベース管理インターフェイスでユーザが指定したデータの検証が不適切なことに起因します。 攻撃者は、悪意のある HTTP 要求をターゲット 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、該当デバイスをリロードして、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ました。 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190619-rvrouters-dos

該当製品

脆弱性のある製品

この脆弱性は、次のシスコ製品について修正済みリリースにリストされているものより前のすべてのリリースに影響します。

- 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

これらのデバイスの Web ベース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経由で利用できます。 デフォルトで、リモート管理機能はこれらの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、管理者が 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。

中小企業向けルータのファームウェア リリースの特定

中小企業向けルータにインストールされているファームウェア リリースは、管理者が Web ベース管理インターフェイスにログインし、右上隅の **[バージョン情報（About）]** リンクをクリックすることで特定できます。 ポップアップ ウィンドウが開き、中小企業向けルータに現在インストールされているファームウェアの情報が表示されます。

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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 アップデートを提供しています。 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。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

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際には、Cisco Security Advisories and Alerts 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ご利用いただいていない場合、また、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場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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、次のリリースで修正されています。

- RV110W Wireless-N VPN ファイアウォール： 1.2.2.4 以降
- RV130W Wireless-N 多機能 VPN ルータ： 1.0.3.51 以降
- RV215W Wireless-N VPN ルータ： 1.3.1.4 以降

このソフトウェアは Cisco.com の Software Center にアクセスし、[すべて参照（Browse All）] をクリックして次の手順でダウンロードできます。

RV110W および RV215W

1. [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）] > [RV110W Wireless-N VPNファイアウォール（RV110W Wireless-N VPN Firewall）] または [RV215W Wireless-N VPNルータ（RV215W Wireless-N VPN Router）] > [ワイヤレスルータのファームウェア（Wireless Router Firmware）] を選択します。
2. [RV110W Wireless-N VPNファイアウォール（RV110W Wireless-N VPN Firewall）] または

[RV215W Wireless-N VPNルータ（RV215W Wireless-N VPN Router）] ページの左側のペインにあるリリースにアクセスします。

RV130W

1. [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）] > [RV130W Wireless-N多機能VPNルータ（RV130W Wireless-N Multifunction VPN Router）] > [スモールビジネス向けルータのファームウェア（Small Business Router Firmware）] を選択します。
2. [RV130W Wireless-N多機能VPNルータ（RV130W Wireless-N Multifunction VPN Router）] ページの左側のペインにあるリリースにアクセスします。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

シスコは、この脆弱性をご報告いただいた Pen Test Partners LLP の T. Shiomitsu 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190619-rvrouters-dos

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019 年 6 月 19 日

利用規約