Cisco Small Business RV110W、RV130、RV130W、および RV215W シリーズ ルータのコマンド シェル インジェクションの脆弱性

High

アドバイザリーID : cisco-sa-cmd-shell-injection-9jOQn9Dy
初公開日 : 2020-07-15 16:00
バージョン 1.0 : Final
CVSSスコア : 8.1
回避策 : No workarounds available
Cisco バグ ID : CSCvs50849 CSCvs50846 CSCvs50853

CVE-2020-3332

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 RV110W、RV130、RV130W、および RV215W シリーズ 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の攻撃者が該当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。

この脆弱性は、ユーザが指定したデータの入力の検証が不十分であることに起因します。攻撃者は、該当デバイスの Web ベース管理インターフェイスに巧妙に細工されたリクエストを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、攻撃者は該当デバイスにおいて任意のシェルコマンドまたはスクリプトをルート権限で実行す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-cmd-shell-injection-9jOQn9Dy

該当製品

脆弱性のある製品

この脆弱性は、脆弱性が存在するファームウェアリリースを実行している次の Cisco Small

Business ルータに影響を与えます。

- RV110W Wireless-N VPN ファイアウォール
- RV130 VPN ルータ
- RV130W Wireless-N 多機能 VPN ルータ
- RV215W Wireless-N VPN ルータ

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

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。

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、この脆弱性の影響を受けることが分かっています。

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。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、アクセスまたはその他の方法で使用した場合、お客様は https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載の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。

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、シスコ セキュリティ アドバイザリ 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アップグレード ソリューション一式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が新規リリースで引き続き正しくサポートされていることを十分に確認してください。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（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

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

次の表に示すように、該当する修正済みのソフトウェアリリースにアップグレードすることをお勧めします。

シスコ製品	First Fixed Release（修正された最初のリリース）
RV110W Wireless-N VPN ファイアウォール	1.2.2.8
RV130 VPN ルータ	1.0.3.55
RV130W Wireless-N 多機能 VPN ルータ	1.0.3.55
RV215W Wireless-N VPN ルータ	1.3.1.7

Cisco.comのSoftware Centerからソフトウェアをダウンロードするには、次の手順を実行します。

RV110W および RV215W

1. [すべてを参照（Browse All）] をクリックします。
2. Routers > Small Business Routers > Small Business RV Series Routers > RV110W Wireless-N VPN Firewall またはRV215W Wireless-N VPN Router > Wireless Router Firmwareの順に選択します。
3. [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）] ページの左ペインからリリースを選択します。

RV130 および RV130W

1. [すべてを参照（Browse All）] をクリックします。
2. [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）] > [RV130 VPNルータ（RV130 VPN Router）] または [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）] の順に選択します。
3. [RV130 VPNルータ（RV130 VPN Router）] または [RV130W Wireless-N多機能VPNルータ（RV130W Wireless-N Multifunction VPN Router）] ページの左ペインからリリースを選択します。

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

この脆弱性を報告していただいた XDSEC 社の Larryxi 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmd-shell-injection-9jOQn9Dy

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	2020 年 7 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。