Cisco Small Business RV320/RV325 ルータで確認された情報開示の脆弱性

High

アドバイザリーID : cisco-sa-20190123-rv-info

初公開日 : 2019-01-23 16:00

最終更新日 : 2019-04-04 14:00

バージョン 2.2 : Final

CVSSスコア : 7.5

回避策 : No workarounds available

Cisco バグ ID : CSCvg85922

CVE-2019-1653

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 RV320/RV325 デュアル ギガビット WAN VPN ルータでは、Web ベースの管理インターフェイスで脆弱性が確認されました。認証されていないリモートの攻撃者が機密情報を取得できる危険性があります。

この脆弱性は、不適切な URL アクセス管理に起因しています。 攻撃者は影響を受けるデバイスに HTTP または HTTPS 経由で接続し、特定の URL を要求することで、この脆弱性をエクスプロイトできます。 エクスプロイトに成功すると、ルータの設定や詳細な診断情報をダウンロードできます。

2019 年 4 月 4 日更新： この脆弱性の初期の修正が完全でないことが判明しました。 この脆弱性は、ファームウェア リリース 1.4.2.22 で完全に修正されました。

この脆弱性に対処するファームウェア アップデートは、現在提供されていません。 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-20190123-rv-info

該当製品

脆弱性のある製品

この脆弱性は、ファームウェア リリース 1.4.2.15 ~ 1.4.2.20 を実行している Cisco Small Business RV320/RV325 デュアル ギガビット WAN VPN ルータに影響を及ぼします。

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。

リモート管理機能が有効の場合、それを無効化して露出を低減することを推奨します。 この機能は **[ファイアウォール (Firewall)] > [全般 (General)]** で設定しますが、デフォルトで無効化されています。 これによって、WAN ポート経由で到達可能な、WAN IP アドレスの Web ベースの管理インターフェイスが無効化されます。 Web ベースの管理インターフェイスは LAN IP アドレスで引き続き使用可能となり、LAN ポート経由で到達可能です。

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

RV320/RV325 デュアル ギガビット WAN VPN ルータのファームウェア リリース 1.4.2.22 以降では本脆弱性が修正済みです。

このソフトウェアは Cisco.com の Software Center にアクセスし、次の手順でダウンロードできます。

1. [すべて参照（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）] > [RV320デュアルギガビットWAN VPNルータ（RV320 Dual Gigabit WAN VPN Router）] または [RV325デュアルギガビット WAN VPNルータ（RV325 Dual Gigabit WAN 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）] にアクセスします。
3. [RV320 デュアルギガビットWAN VPNルータ（RV320 Dual Gigabit WAN VPN Router）] または [RV325デュアルギガビットWAN VPNルータ（RV325 Dual Gigabit WAN VPN Router）] ページの左側のペインを使用して、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）は、このアドバイザリに記載されている脆弱性を対象としたネットワーク スキャンが活発に行われていることだけではなく、この脆弱性をエクスプロイトするコードが公開されていることを認識しています。

出典

本脆弱性の報告に関し RedTeam Pentesting GmbH に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-info

改訂履歴

バージ	説明	セクション	ステー	Da

ョン			タス	te
2.2	完全な修正に関するお知らせのために更新	「要約」、「脆弱性のある製品」および「修正済リリース」	最終版	2019年4月4日
2.1	緩和のための推奨事項も追加されました。	回避策	Interim	2019年3月28日
2.0	完了していない初期の修正の更新情報	「要約」、「脆弱性のある製品」および「修正済リリース」	Interim	2019年3月27日
1.1	不正利用事例に関する公開情報を更新	不正利用事例と公式発表	最終版	2019年1月25日
1.0	初回公開リリース		最終版	2019年1月23日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。