

Cisco Small Business RV320/RV325 ルータで確認された、コマンド インジェクションの脆弱性



アドバイザリーID : cisco-sa-20190123-rv-inject [CVE-2019-1652](#)

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 : [7.2](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvm78058](#)

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 および RV325 デュアル ギガビット WAN VPN ルータの Web ベースの管理インターフェイスの脆弱性により、影響を受けるデバイスに対する管理者権限を持つ認証されたりモートの攻撃者が任意のコマンドを実行する可能性があります。

この脆弱性は、ユーザ入力の検証が不適切なことに起因します。攻撃者は影響を受けるデバイスの Web ベースの管理インターフェイスに悪意のある HTTP POST 要求を送信することで、この脆弱性をエクスプロイトすることができます。エクスプロイトに成功すると、攻撃者はルートとして基盤となる Linux シェルで任意のコマンドを実行できます。

2019年4月4日更新 : この脆弱性に対する初期修正が不完全である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 アップデートが、現在提供されています。この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-inject>

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。

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 IP アドレスが割り当てられた Web ベースの管理インターフェイス (WAN ポート経由で到達可能) 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了場合、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です。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、[シスコのセキュリティアドバイザリおよびアラート (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 Cisco Service Contract 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 POS 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)] > [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

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

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-inject>

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.2	完全な修正に関するお知らせのためを更新。	「要約」、「脆弱性のある製品」および「修正済リリース」	Final	2019 年 4 月 4 日
2.1	緩和のための推奨事項を追加	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	Final	2019 年 1 月 25 日
1.0	初回公開リリース	—	Final	2019 年 1 月 23 日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。

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。