Cisco Small Business RV シリーズルータのスタックオーバーフローによる任意のコード実行に対する脆弱性

High

アドバイザリーID : cisco-sa-rv-routers-stack-vUxHmnNz

初公開日 : 2020-06-17 16:00

バージョン 1.0 : Final

CVSSスコア : 7.2

回避策 : No workarounds available

Cisco バグ ID : CSCvt26525 CSCvt26555 CSCvt26643 CSCvt26705 CSCvt29416 CSCvt26659 CSCvt26725 CSCvt26619 CSCvt26718 CSCvt26729 CSCvt29381 CSCvt29400 CSCvt29423 CSCvt26591 CSCvt29403 CSCvt29414 CSCvt26663 CSCvt29385 CSCvt29396 CSCvt29398 CSCvt29388 CSCvt29421

CVE-2020-3291
CVE-2020-3290
CVE-2020-3293
CVE-2020-3292
CVE-2020-3288
CVE-2020-3287
CVE-2020-3289
CVE-2020-3295
CVE-2020-3294
CVE-2020-3286
CVE-2020-3296

概要

Cisco Small Business RV320 および RV325 シリーズルータと、Cisco Small Business RV016、RV042、RV082 ルータの Web ベースの管理インターフェイスで複数の脆弱性が確認されました。管理者権限を持つ認証されたリモートの攻撃者が、影響を受けるデバイスに対して任意のコマンドを実行する危険性があります。

この脆弱性は、Web ベース管理インターフェイスでの、スクリプトへのユーザ入力の境界制限が不適切なことに起因します。 Web ベースの管理インターフェイスにログインできる管理権限を持つ攻撃者は、影響を受けるデバイスに非常に容量の多い偽造リクエストを送信してスタックオーバーフローを起こすことで、各脆弱性をエクスプロイトする危険性があります。 攻撃者がエクスプロイトに成功すると、デバイスがクラッシュされたり、*ルート権限*を用いて基盤となるオペレーティングシステムに対して任意のコードが実行されたりする危険性があります。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 これら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-rv-routers-stack-vUxHmnNz

該当製品

脆弱性のある製品

これらの脆弱性は、以下の Cisco Small Business ルータおよびファームウェアのリリースに影響します。

- RV016 Multi-WAN VPN： 4.2.3.10 以前
- RV042 Dual WAN VPN： 4.2.3.10 以前
- RV042G デュアルギガビット WAN VPN： 4.2.3.10 以前
- RV082 Dual WAN VPN： 4.2.3.10 以前
- RV320 デュアルギガビット WAN VPN： 1.5.1.05 以前
- RV325 デュアルギガビット WAN VPN： 1.5.1.05 以前

これらのデバイスの 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経由で利用できます。 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、ローカル LAN 接

続で Web ベースの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、これらの脆弱性の影響を受けることが分かっています。

回避策

これら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

シスコでは、Cisco RV320 および 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 1.5.1.11 でこれらの脆弱性を修正しました。

シスコでは、Cisco RV016、RV042、および RV082 ルータのファームウェアリリース 4.2.3.14 でこれらの脆弱性を修正しました。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、このアドバイザリで説明されている脆弱性に対して概念実証段階のエクスプロイト コードが入手可能であることを認識しています。

Cisco PSIRT では、このアドバイザリに記載されている脆弱性のいかなる悪用も認識していません。

出典

これらの脆弱性を報告してくださった Kai Cheng 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-routers-stack-vUxHmnNz

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	2020 年 6 月17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。