Cisco Small Business RV016、RV042、RV042G、RV082、RV320、およびRV325ルータのクロスサイトスクリプティングの脆弱性

アドバイザリーID : cisco-sa-sbiz-rv-xss-OQeRTup
CVE-2024-20362
初公開日 : 2024-04-03 16:00
バージョン 1.0 : Final
CVSSスコア : 6.1
回避策 : No workarounds available
Cisco バグ ID : CSCwj24997 CSCwj31685

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 RV016、RV042、RV042G、RV082、RV320、およびRV325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、インターフェイスのユーザに対してクロスサイトスクリプティング(XSS)攻撃を仕掛ける可能性があります。

この脆弱性は、Webベースの管理インターフェイスによる不十分な入力検証に起因します。攻撃者は、悪意のあるペイロードを含む特定のWebページにアクセスするようにユーザを誘導することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスする可能性があります。

シスコでは、本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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbiz-rv-xss-OQeRTup

該当製品

脆弱性のある製品

この脆弱性は、次のCisco RVシリーズSmall Businessルータのすべてのソフトウェアリリース

に影響を与えます。

- RV016 Multi-WAN VPN ルータ
- RV042 Dual WAN VPN ルータ
- RV042G デュアルギガビット WAN VPN ルータ
- RV082 Dual WAN VPN ルータ
- RV320 デュアルギガビット WAN VPN ルータ
- RV325 デュアルギガビット WAN VPN ルータ

最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

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。

シスコは、この脆弱性が次のCisco RVシリーズSmall Businessルータには影響を与えないことを確認しました。

- RV160 VPN ルータ
- RV160W Wireless-AC VPN ルータ
- RV260 VPN ルータ
- PoE 対応 RV260P VPN ルータ
- RV260W Wireless-AC VPN ルータ
- RV340 デュアル WAN ギガビット VPN ルータ
- RV340W デュアル WAN ギガビット Wireless-AC VPN ルータ
- RV345 デュアル WAN ギガビット VPN ルータ
- RV345P デュアル WAN ギガビット PoE 対応 VPN ルータ

回避策

この脆弱性に対処する回避策はありません。

Cisco Small Business RV320およびRV325ルータでこの脆弱性を緩和するには、リモート管理を無効にします。Cisco Small Business RV016、RV042、RV042G、およびRV082ルータでこの脆弱性を緩和するには、リモート管理を無効にして、ポート443および60443へのアクセスをブロックします。軽減策が実装された後も、ルータには LAN インターフェイスを介して引き続きアクセスできます。

リモート管理の無効化

リモート管理を無効化するには、次の手順を実行します。

1. デバイスの Web ベースの管理インターフェイスにログインします。
2. [ファイアウォール（Firewall）] > [全般（General）] を選択します。
3. [リモート管理（Remote Management）] チェックボックスをオフにします。

ポート 443 および 60443 へのアクセスをブロックする

まず、新しいサービスをポート 60443 に対するデバイスのアクセスルールに追加します。ポート443のサービスはサービスリストで事前に定義されているため、このサービスを作成する必要はありません。

1. デバイスの Web ベースの管理インターフェイスにログインします。
2. [ファイアウォール（Firewall）] > [アクセスルール（Access Rules）] を選択します。
3. [サービス管理（Service Management）] をクリックします。
4. [サービス名（Service Name）]フィールドに [TCP-60443] を入力します。
5. [プロトコル（Protocol）] ドロップダウンリストから [TCP] を選択します。
6. [ポート範囲（Port Range）] フィールドの両方に [60443] と入力します。
7. [リストに追加（Add to List）] をクリックします。
8. [OK] をクリックします。

次に、ポート 443 および 60443 をブロックするアクセスルールを作成します。ポート 443 をブロックするアクセスルールを作成するには、次の手順を実行します。

1. デバイスの Web ベースの管理インターフェイスにログインします。
2. [ファイアウォール（Firewall）] > [アクセスルール（Access Rules）] を選択します。
3. [Add] をクリックします。
4. [アクション（Action）] ドロップダウンリストから [拒否（Deny）] を選択します。
5. [サービス（Service）] ドロップダウンリストから [HTTPS (TCP 443-443）] を選択します。
6. [ログ（Log）] ドロップダウンリストから [このルールに一致するパケットをログ（Log packets match this rule）] を選択します。
7. [ソースインターフェイス（Source Interface）] ドロップダウンリストから、デバイスの WAN 接続に一致するオプションを選択します。
8. [送信元IP（Source IP）] ドロップダウンリストから [任意（Any）] を選択します。
9. [宛先IP（Destination IP）] ドロップダウンリストから [単一（Single）] を選択します。
10. [宛先IP（Destination IP）] の両方のフィールドに、WAN IP アドレスを入力します。
11. [Save] をクリックします。

ポート 60443 をブロックするアクセスルールを作成するには、前の手順を繰り返しますが、手順5では[サービス（Service）] ドロップダウンリストから [HTTPS (TCP 60443-60443)] を 選択します。

注：2番目のWANポートを使用している場合は、2番目のWANポートのWAN番号とIPアドレスを使用して、さらに2つのアクセスコントロールリスト(ACL)ルールを設定する必要があります。

これらの緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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ためのソフトウェア アップデートをリリースしておらず、今後もリリースする予定はありません。Cisco Small Business RV016、RV042、RV042G、およびRV082ルータは、サポート終了プロセスに入っています。お客様には、これらの製品のサポート終了通知を参照することをお勧めします。

Cisco RV016 Multi-WAN VPN ルータの販売終了とサポート終了のご案内
Cisco RV042 および RV042G VPN ルータ（全モデル）の販売終了とサポート終了のご案内
Cisco RV082 Dual WAN VPN ルータの販売終了とサポート終了のご案内
「End-of-Sale and End-of-Life Announcement for the Cisco RV320 and RV325 Dual Gigabit WAN VPN Router」

デバイスの移行を検討する際は、[シスコ セキュリティ アドバイザリ（Cisco Security Advisories）] 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の有無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。

いずれの場合でも、新製品がお客様のネットワークニーズに十分対応していること、新規デバイスに十分なメモリが搭載されていること、および現在のハードウェアとソフトウェアの構成が新製品で引き続き適切にサポートさ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。

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

シスコは、この脆弱性を報告していただいたLeetsun氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbiz-rv-xss-OQeRTup

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	2024年4月3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。