Cisco Small Business RV042、RV042G、RV320、およびRV325ルータのサービス拒否およびリモートコード実行の脆弱性

Medium

アドバイザリーID : cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV
初公開日 : 2024-10-02 16:00
バージョン 1.0 : Final
CVSSスコア : 6.8
回避策 : No workarounds available
Cisco バグ ID : CSCwm48770

CVE-2024-20520
CVE-2024-20522
CVE-2024-20521
CVE-2024-20524
CVE-2024-20523
CVE-2024-20517
CVE-2024-20516
CVE-2024-20519
CVE-2024-20518

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 RV042、RV042G、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複数の脆弱性により、リモート攻撃者が該当デバイスの基盤となるオペレーティングシステムで任意のコマンドを実行したり、サービス妨害(DoS)状態を引き起こす可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコは、これらの脆弱性に対応するソフトウェアアップデートをリリースしておらず、リリースする予定もありません。これは、該当製品がソフトウェアメンテナンスリリースの終了日を過ぎているためです。Cisco Product Security Incident Response Team(PSIRT)は、これらの製品に

影響を与えるセキュリティの脆弱性がサポート終了日に達するまで、それらの脆弱性の評価と開示を続けます。

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性は次のCisco Small Business RVシリーズルータのすべてのソフトウェアリリースに影響を与えていました。

- RV042 Dual WAN VPN ルータ
- RV042G デュアルギガビット 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、これら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、これらの脆弱性が次のCisco Small Business RVシリーズ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

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。

脆弱性の詳細は以下のとおりです。

CVE-2024-20516、CVE-2024-20517、CVE-2024-20522、CVE-2024-20523、およびCVE-2024-20524:Cisco Small Business RV042、RV042G、RV320、およびRV325のサービス拒否の脆弱性

Cisco Small Business RV042、RV042G、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複数の脆弱性により、認証された 管理者レベルのリモート攻撃者が該当デバイスの予期しないリロードを引き起こし、その結果、サービス妨害(DoS)状態が発生する可能性があります。これらの脆弱性を不正利用するには、攻撃者は該当デバイスの有効な管理者ログイン情報を持っている必要があります。

これらの脆弱性は、着信HTTPパケットでの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、該当デバイスのWebベースの管理インターフェイスに巧妙に細工されたHTTP要求を送信することにより、これらの脆弱性を不正利用する可能性があります。攻撃者は、エクスプロイトに成功すると、予期していないデバイスのリロードを引き起こし、DoS 状態を引き起こせるようになります。

これらの脆弱性に対処する回避策はありません。

バグID:CSCwm48770
CVE ID:CVE-2024-20516、CVE-2024-20517、CVE-2024-20522、CVE-2024-20523、CVE-2024-20524
SIR：中
CVSS ベーススコア：6.8
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H

CVE-2024-20518、CVE-2024-20519、CVE-2024-20520、およびCVE-2024-20521:Cisco Small Business RV042、RV042G、RV320、およびRV325のリモートコマンド実行の脆弱性

Cisco Small Business RV042、RV042G、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複数の脆弱性により、認証された 管理者レベルのリモート攻撃者が、 rootユーザとして任意のコードを実行する可能性があります。これらの脆弱性を不正利用するには、攻撃者は該当デバイスの有効な管理者ログイン情報を持っている必要があります。

これらの脆弱性は、Web ベースの管理インターフェイスへの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、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、これら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、攻撃者はルートユーザーとして、基盤となるオペレーティングシステムで任意のコードを実行する可能性があります。

これらの脆弱性に対処する回避策はありません。

バグID:CSCwm48770
CVE ID:CVE-2024-20518、CVE-2024-20519、CVE-2024-20520、CVE-2024-20521
SIR：中
CVSS ベーススコア：6.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

回避策

これらの脆弱性に対処する回避策はありません。ただし、攻撃対象領域を縮小するために、管理者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できます。影響を受けるルータは、この緩和策が実装された後も、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。

この緩和策の実装手順については、次の項を参照してください。

リモート管理の無効化

リモート管理を無効にするには、次の手順に従います。

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

ポート443および60443へのアクセスをブロックするには、最初に、ポート60443のデバイスのアクセスルールに新しいサービスを追加する必要があります。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、追加する必要はありません。ポート60443のアクセスルールに新しいサービスを追加する手順は、次のとおりです。

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. [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する必要があります。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、次の手順を使用します。

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

Cisco Small Business RV042、RV042G、RV320、およびRV325ルータは、ソフトウェアメンテナンスリリースの終了日が経過しています。このため、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ソフトウェアアップデートをリリースしておらず、リリースする予定もありません。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 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
「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 PSIRT では、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とその公表は確認しておりません。

出典

シスコは、これらの脆弱性を報告していただいたSecdriver Labのk0mor3b1に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV

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10月2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。