

Cisco CVR100W Wireless-N VPNルータユニバーサルプラグアンドプレイバッファオーバーフローの脆弱性

Critical アドバイザリーID : cisco-sa-20170503-cvr100w1 [CVE-2017-3882](#)
初公開日 : 2017-05-03 16:00
最終更新日 : 2017-05-04 15:30
バージョン 1.1 : Final
CVSSスコア : [9.6](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCuz72642](#)

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 CVR100W Wireless-N VPNルータのユニバーサルプラグアンドプレイ(UPnP)実装における脆弱性により、認証されていないレイヤ2隣接の攻撃者が任意のコードを実行したり、サービス妨害(DoS)状態を引き起こしたりする可能性があります。リモートコード実行は、*root*権限で発生する可能性があります。

この脆弱性は、UPnP入力データの不完全な範囲チェックに起因し、これによりバッファオーバーフローが発生する可能性があります。攻撃者は、ターゲットデバイスのUPnPリスニングポートに悪意のある要求を送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はデバイスのリロードを引き起こしたり、*root*権限で任意のコードを実行したりする可能性があります。

シスコはこの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-20170503-cvr100w1>

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1.0.1.22より前のCisco CVR100W Wireless-N VPNルータのすべてのファームウェアリリースに影響します。管理者は、[http\(s\):// system-ip](http(s)://system-ip)アクセスURLを使用してWebインターフェイスにログインすることで、どのファームウェアリリースが実行されているかを確認できます。ファームウェアのリリースが初期画面に表示されます。次の例では、ルータでファームウェアリリース 1.0.1.21が実行されています。

```
Cisco Small Business  
CVR100W Wireless-N VPN Router  
Version 1.0.1.21
```

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

シスコは、他のSmall Business RVシリーズルータがこの脆弱性の影響を受けないことを確認しました。

回避策

こ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した場合、お客様は

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

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。

http://www.cisco.com/c/ja_jp/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

この脆弱性は、Cisco CVR100W Wireless-N VPNルータファームウェアリリース1.0.1.22以降で対応されています。ファームウェアアップデートは、Cisco.comの[Software Center](#)からダウンロードできます。**[製品(Products)] > [ルータ(Routers)] > [Small Businessルータ(Small Business Routers)] > [Small Business RVシリーズルータ(Small Business RV Series Routers)] > [CVR100W Wireless-N VPNルータ(CVR100W Wireless-N VPN Router)]** の順に移動してください。

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、この脆弱性を発見し、報告していただいたGeekPwn社のChaitin Tech社のセキュリティ研究者に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170503-cvr100w1>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	ソース・クレジット・テキストを更新します。	出典	Final	2017年5月4日
1.0	初回公開リリース	-	Final	2017年5月3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。