Cisco RV180 VPNおよびRV180W Wireless-N多機能VPNルータにおける不正アクセスの脆弱性

High

アドバイザリーID : cisco-sa-20160803-rv180_1

初公開日 : 2016-08-03 16:00

バージョン 1.0 : Final

CVSSスコア : 7.1

回避策 : Yes

Cisco バグ ID : CSCuz43023

CVE-2016-1429

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 RV180 VPNルータおよびCisco RV180W Wireless-N多機能VPNルータのWeb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システム上の任意のファイルにアクセスする可能性があります。この脆弱性により、攻撃者はディレクトリトラバーサルを実行できます。

この脆弱性は、ユーザ入力ディレクトリパスの適切な入力検証とサニタイズが行われていないことに起因します。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、攻撃者は制限する必要があるシステム上の任意のファイルを読み取る可能性があります。

シスコはこの脆弱性に対処するためのファーム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。この脆弱性に対する緩和策が利用可能です。

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-20160803-rv180_1

該当製品

脆弱性のある製品

Cisco RV180 VPNルータおよびRV180W Wireless-N多機能VPNルータのすべてのファームウ

ェアバージョンに脆弱性が存在します。

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。

回避策

この脆弱性に対処する回避策はありません。 次の2つの緩和策が、この脆弱性の発現を制限するのに役立ちます。

リモート管理の無効化

注意：デバイスがWAN接続を介して管理されている場合は、リモート管理を無効にしないでください。その結果、デバイスへの管理接続が失われます。この機能を無効にすると、Cisco QuickVPNアクセスができなくなります。

リモート管理はデフォルトで無効になっています。有効になっている場合、管理者は[Web Access] 画面([Administration] > [Management Interface] > [Web Access])を使用して無効にできます。[Remote Management] フィールドの[Disabled] チェックボックスをオンにします。

リモート管理を無効にすると、LAN上のユーザだけがこの脆弱性の不正利用を試みることができます。デバイスでは、リモート管理はデフォルトでは有効になっていません。

リモート管理アクセスを特定のIPアドレスに制限する

リモート管理が必要な場合は、デフォルトのany設定ではなく、特定のIPアドレスによってのみアクセスできるようにデバイスを強化します。設定画面([Administration] > [Management Interface] > [Web Access])にアクセスすると、管理者は[Remote IP address] フィールドを変更して、指定したIPアドレスを持つデバイスだけがデバイスにアクセスできるようにすることができます。

修正済みソフトウェア

シスコはこのアドバイザリで説明している脆弱性に対処するためのファームウェアの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。Cisco RV180ルータとCisco RV180Wルータは、サポート終了(EoL)プロセスに入っています。次の製品のEoL通知を参照してください。

- Cisco RV180W Wireless-N多機能VPNルータの販売終了およびサポート終了のお知らせ
- Cisco RV180 VPNルータの販売終了およびサポート終了のお知らせ

Cisco RV130W Wireless-N多機能VPNルータへの移行をお勧めします。

デバイスの移行を検討する際は、 http://www.cisco.com/go/psirtにあるCisco Security Advisories and Responsesアーカイブを参照し、後続のアドバイザリを確認して、侵害の可能性と完全なア

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、お客様は新しいデバイスがネットワークのニーズに十分に対応できることを確認する必要があります。新しいデバイスには十分なメモリが搭載され、現在のハードウェアおよびソフトウェア構成は新しい製品でも引き続き適切にサポートされます。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

この脆弱性は、セキュリティ研究者のHarri Kuosmanen氏によって発見され、シスコに報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-rv180_1

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	2016年8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。