Cisco Small Business RVシリーズルータの複数の脆弱性

アドバイザリーID : cisco-sa-20141105-rv
初公開日 : 2014-11-05 16:00
最終更新日 : 2014-11-20 14:41
バージョン 1.1 : Final
CVSSスコア : 9.4
回避策 : No Workarounds available
Cisco バグ ID : CSCuh86998 CSCuh87126 CSCuh87145

CVE-2014-2179
CVE-2014-2177
CVE-2014-2178

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 RV120W Wireless-N VPNファイアウォール、Cisco RV180 VPNルータ、Cisco RV180W Wireless-N多機能VPNルータ、およびCisco RV220Wワイヤレスネットワークセキュリティファイアウォールは、次の脆弱性の影響を受けます。

- Cisco RVシリーズルータにおけるコマンドインジェクションの脆弱性
- Cisco RVシリーズルータのHTTP Refererヘッダーの脆弱性
- Cisco RVシリーズルータにおける安全でないファイルアップロードの脆弱性

これらの脆弱性は互いに独立しています。いずれかの脆弱性の影響を受けるリリースが、他の脆弱性の影響を受けることはありません。

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リリースしています。これらの脆弱性に対しては回避策があります。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-20141105-rv

該当製品

脆弱性のある製品

これらの脆弱性は、次のCisco Small Business RVシリーズルータに影響を与えます。

- 1.0.5.9より前のファームウェアが稼働しているCisco RV120W Wireless-N VPNファイア

ウォール
- 1.0.4.14より前のファームウェアバージョンを実行しているCisco RV180 VPNルータおよびCisco RV180W Wireless-N多機能VPNルータ
- 1.0.6.6より前のファームウェアバージョンを実行しているCisco RV220Wワイヤレスネットワークセキュリティファイアウォール

デバイスで実行されているシステムファームウェアのバージョンを確認するには、Web管理インターフェイスでデバイスにログインし、画面の右上隅にある Aboutをクリックします。新しいウィンドウが開き、ルータのタイプとファームウェアバージョンが表示されます。ファームウェアバージョンフィールドラベルのすぐ横にある番号は、システムファームウェアのバージョンです。たとえば、V1.0.3.10のようになります。

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。

詳細

Cisco RV120W Wireless-N VPNファイアウォール、Cisco RV180 VPNルータ、Cisco RV180W Wireless-N多機能VPNルータ、およびCisco RV220Wワイヤレスネットワークセキュリティファイアウォールは、使いやすく、柔軟性に優れた高性能デバイスで、小規模企業に最適です。複数のオフィスやリモートの従業員に、安全性の高いブロードバンド、有線、ワイヤレス接続を提供します。

Cisco RVシリーズルータにおけるコマンドインジェクションの脆弱性

Cisco RV120W Wireless-N VPNファイアウォール、Cisco RV180 VPNルータ、Cisco RV180W Wireless-N多機能VPNルータ、およびCisco RV220Wワイヤレスネットワークセキュリティファイアウォールのネットワーク診断管理ページにおける脆弱性により、認証されたリモートの攻撃者がデバイスで任意のコマンドを実行する可能性があります。

この脆弱性は、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、この脆弱性を不正利用する可能性があります。不正利用に成功すると、root 権限を使用してデバイス上で任意のコマンドを実行する恐れがあります。

この脆弱性は、Cisco Bug ID CSCuh87126(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2014-2177が割り当てられています。

Cisco RVシリーズルータのHTTP Refererヘッダーの脆弱性

Cisco RV120W Wireless-N VPNファイアウォール、Cisco RV180 VPNルータ、Cisco RV180W Wireless-N多機能VPNルータ、およびCisco RV220Wワイヤレスネットワークセキュリティファ

イアウォールの管理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クロスサイトリクエストフォージェリ(CSRF)攻撃を実行する可能性があります。

この脆弱性は、不十分なCSRF保護に起因します。攻撃者は、デバイスに対して認証されたユーザが悪意のあるリンクをクリックするように仕向けることで、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、攻撃者は認証されたユーザの権限を使用して、デバイスの管理Webページでアクションを実行できる可能性があります。

この脆弱性は、Cisco Bug ID CSCuh87145(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2014-2178が割り当てられています。

Cisco RVシリーズルータにおける安全でないファイルアップロードの脆弱性

Cisco RV120W Wireless-N VPNファイアウォール、Cisco RV180 VPNルータ、Cisco RV180W Wireless-N多機能VPNルータ、およびCisco RV220Wワイヤレスネットワークセキュリティファイアウォールのファイルアップロードルーチン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デバイス上の任意の場所にファイルをアップロードする可能性があります。

この脆弱性は、入力に対する不十分な検証に起因します。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、攻撃者はデバイス上の任意の場所にファイルをアップロードできる可能性があります。

この脆弱性は、Cisco Bug ID CSCuh86998(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2014-2179が割り当てられています。

回避策

次の緩和策は、これら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： WAN接続を介してデバイスを管理している場合は、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画面で Administration > Management Interface > Web Accessの順に選択して、この機能を無効にできます。 Remote Managementフィールドの Disabledチェックボックスにチェックマークを付けます。

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を悪用しようとする可能性があります。

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、デバイスを強化して、デフォルト設定の anyではなく、特定のIPアドレスによってのみデバイスにアクセスできるようにします。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

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照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、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。

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Cisco RV180 VPNルータおよびCisco RV180W Wireless-N多機能VPNルータの無償ソフトウェアアップデートを次のリンクでリリースしています。

Cisco RV180 VPNルータファームウェアリリース 1.0.4.14:http://software.cisco.com/download/release.html?mdfid=284005904&flowid=32282&softwareid=2
Cisco RV180W Wireless-N多機能VPNルータファームウェアリリース 1.0.4.14:http://software.cisco.com/download/release.html?mdfid=284005928&softwareid=282487380&rele
Cisco RV120W Wireless-N VPNファイアウォールファームウェアリリース 1.0.5.9:http://software.cisco.com/download/release.html?mdfid=282981372&flowid=796&softwareid=2824
Cisco RV220Wワイヤレスネットワークセキュリティファイアウォールリリース 1.0.6.6:http://software.cisco.com/download/release.html?mdfid=283118607&flowid=24581&softwareid=28

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

シスコは、これらの脆弱性を報告していただいたSecurify(www.securify.nl)のYorick Koster氏に感

謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141105-rv

改訂履歴

リビジョン 1.1	2014-November-20	RV220Wの修正済みソフトウェアの詳細を追加。
リビジョン 1.0	2014年11月5日	初回公開リリース

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。

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。