Ciscoワイヤレスレジデンシャルゲートウェイのリモートコード実行の脆弱性

Critical

アドバイザリーID : ciscosa-20140716-cm

CVE-2014-3306

初公開日 : 2014-07-16 16:00

最終更新日 : 2014-07-18 17:55

バージョン 1.1 : Final

CVSSスコア : 10.0

回避策 : No Workarounds available

Cisco バグ ID : CSCup40808

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

複数のCiscoワイヤレスレジデンシャルゲートウェイ製品で使用されるWebサーバの脆弱性により、認証されていないリモートの攻撃者がバッファオーバーフローを不正利用して任意のコードを実行する可能性があります。

この脆弱性は、HTTP要求の入力検証が正しく行われ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。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。この脆弱性を軽減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/ciscosa-20140716-cm

該当製品

シスコは、BFC 5.5.2以前に基づくソフトウェアを実行している「脆弱性が存在する製品」セクションに記載されている製品のみが脆弱性の影響を受けることを確認しました。BFC 5.5.2以前のバージョンのソフトウェアを実行している場合は、「修正済みソフトウェアの入手」セクションに記載されている手順に従ってソフトウェアのアップデートを入手できます。すべてのBFC 5.5.3ベースのソフトウェア以降には、この脆弱性は含まれていません。

脆弱性のある製品

次のシスコ製品がこの脆弱性の影響を受けます。

- Cisco DPC3212 VoIPケーブルモデム
- Cisco DPC3825 8x4 DOCSIS 3.0ワイヤレスレジデンシャルゲートウェイ
- Cisco EPC3212 VoIPケーブルモデム
- Cisco EPC3825 8x4 DOCSIS 3.0ワイヤレスレジデンシャルゲートウェイ
- Cisco Model DPC3010 DOCSIS 3.0 8x4ケーブルモデム
- Cisco Model DPC3925 8x4 DOCSIS 3.0 with Wireless Residential Gateway with EDVA
- Cisco Model DPQ3925 8x4 DOCSIS 3.0ワイヤレスレジデンシャルゲートウェイ（EDVA付き）
- Cisco Model EPC3010 DOCSIS 3.0ケーブルモデム
- Cisco Model EPC3925 8x4 DOCSIS 3.0 with Wireless Residential Gateway with EDVA

脆弱性を含んでいないことが確認された製品

- Cisco Model DCP2100 DOCSIS 2.0ケーブルモデム
- Cisco Model DPC3008 DOCSIS 3.0 8x4ケーブルモデム
- Cisco Model DPC3208 8x4 DOCSIS 3.0ケーブルモデム
- Cisco Model DPC3828 DOCSIS 3.0 8x4レジデンシャルワイヤレスゲートウェイ
- Cisco Model DPC3928 DOCSIS 3.0 8x4ワイヤレスレジデンシャルゲートウェイ
- Cisco Model EPC2425 EuroDOCSIS 2.0ケーブルモデム
- Cisco Model EPC3008 EuroDOCSIS 3.0 8x4 VoIPケーブルモデム
- Cisco Model EPC3208 8x4 DOCSIS 3.0ケーブルモデム
- Cisco Model EPC3828 EuroDOCSIS 3.0 8x4レジデンシャルワイヤレスゲートウェイ
- Cisco Model EPC3928 EuroDOCSIS 3.0 8x4ワイヤレスレジデンシャルゲートウェイ
- Scientific Atlanta DPR2320ケーブルモデム
- Scientific Atlanta DPX 2000ケーブルモデム
- Scientific Atlanta EPC2203 VoIPケーブルモデム
- WebSTAR DPX2100ケーブルモデム
- WebSTAR DPX2203C VoIPケーブルモデム
- WebSTAR EPC2100R2ケーブルモデム
- WebSTAR EPR2325 EuroDOCSISレジデンシャルゲートウェイ（ワイヤレスアクセスポイント搭載）

詳細

複数のCiscoワイヤレスレジデンシャルゲートウェイ製品で使用されるWebサーバの脆弱性により、認証されていないリモートの攻撃者がバッファオーバーフローを不正利用して任意のコードを実行する可能性があります。

この脆弱性は、HTTP要求の入力検証が正しく行われ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。不正利用に成功すると、攻撃者はWebサーバをクラッシュさせ、権限を昇格させて任意のコードを実行する可能性があります。この脆弱性は、デバイスがルータモードとゲートウ

ェイモードのどちらで設定されているかに関係なく存在します。

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サービスプロバイダーカスタマーにリリースしました。Cisco TACに連絡する前に、お客様のサービスプロバイダーに連絡して、この脆弱性に対処する修正が含まれているかどうかを確認することをお勧めします。

この脆弱性は、Cisco Bug ID CSCup40808(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-2014-3306が割り当てられています。

回避策

現在のところ、この脆弱性に対する既知の回避策はありません。

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。

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。

この脆弱性は、Tech AnalysisのChris Watts氏によってシスコに報告されました。シスコは、この問題をCisco PSIRTに報告していただいたことに感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-20140716-cm

改訂履歴

リビジョン 1.1	2014年7月18日	「脆弱性のある製品」セクションに修正済みバージョン情報を追加。
リビジョ	2014年7月16日	初回公開リリース

ン 1.0		

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。