Cisco スモール ビジネス RV320 および RV325 ルータ弱いクレデンシャル暗号化脆弱性

Medium	**アドバイザリーID :** cisco-sa-20190404-rv-weak-encrypt **初公開日 :** 2019-04-04 14:00 **バージョン 1.0 :** Final **CVSSスコア :** 5.9 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvp09573	CVE-2019-1828

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 スモール ビジネス RV320 および RV325 二重ギガビットのウェブベースの管理インターフェイスの脆弱性は WAN VPN ルータ リモート攻撃者非認証が管理資格情報にアクセスするようにする可能性があります。

影響を受けたデバイスがユーザーの資格情報のために弱い暗号化アルゴリズムを使用するので存在 する脆弱性。 攻撃者は man-in-the-middle攻撃を行ない、代行受信された資格情報を復号化することによってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が*アドミニストレーター特権*の影響を受けたデバイスへのアクセス権を得ることを可能にする可能性があります。

この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190404-rv-weak-encrypt

該当製品

脆弱性のある製品

この脆弱性は Cisco スモール ビジネス RV320 および RV325 二重ギガビット WAN に VPN ルータ影響を与えます。 該当するソフトウェア リリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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

修正済みソフトウェア リリースの詳細については、本アドバイザリ上部の Cisco Bug ID を参照ください。

ソフトウェアのアップグレードを検討する際には、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は新規リリースでも継続して適切なサポートが受けら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製品のセキュリティ上の問題に対する回答チーム（PSIRT）はこのアドバイザリに説明がある脆弱性の公示か不正利用に気づいています。

出典

Cisco はこの脆弱性を報告するために GitHub ユーザ 0x27 に感謝することを望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190404-rv-weak-encrypt

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019-April-04

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。