Cisco RVS4000 および WRVS4400N ギガビット セキュリティ ルータ ファームウェア SSL キー公開脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20110525-CVE-2011-1647 **初公開日 :** 2011-05-25 15:16 **最終更新日 :** 2012-07-14 12:57 **バージョン 2.0 :** Final **CVSSスコア :** 5.0 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2011-1647

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 RVS4000 4 ポート ギガビット セキュリティ ルータおよび WRVS4400N ワイヤレスN ギガビット セキュリティ ルータのファームウェアは非認証を可能にする可能性がある目標とされたデバイスから機密情報にアクセスするために脆弱性がリモート攻撃者含まれています。

脆弱性は影響を受けたデバイスの SSL 証明書 プライベートキーの不適当な機密保持が原因です。Â は非認証、遠隔目標とされたデバイスから SSL Certificate 鍵情報を検索するのにこの脆弱性を不正利用する可能性があります。、攻撃者成功すれば Â はさらなる攻撃で使用する可能性がある機密情報にアクセスする可能性があります。

Cisco はこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

リモート管理機能がイネーブルになっていなければ、攻撃者は不正利用のための可能性を制限する内部ネットワークからのこの脆弱性を不正利用するただ可能性があります。Â 遠隔管理はデフォルトでディセーブルにされます。

Cisco は CVSS スコアを通してその機能エクスプロイト コード存在を示します; ただし、コードは共用利用可能であると知られていません。

該当製品

Cisco は次のリンクで Cisco バグ ID CSCtn23871 のための Security Advisory を再リリースしました: cisco-sa-20110525-rvs4000

脆弱性のある製品

Cisco 次のファームウェアは影響を受けています:

- 1.3.3.5 前の RVS4000v1 ファームウェア
- 2.0.2.7 前の RVS4000v2 ファームウェア
- 2.0.2.1 前の WRVS4400Nv2 ファームウェア

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

管理者は適切な更新を加えるように助言されます。

管理者は影響を受けたデバイスからバックアップ ファイルを取除くように助言されます。

管理者は信頼された システムだけ影響を受けたシステムにアクセスするように IPベース アクセス コントロール リスト（ACL）を使用することを考えるかもしれません。

管理者は重要なシステムを監視するように助言されます。

修正済みソフトウェア

アクティブな契約を持つ Cisco カスタマは次のリンクで Software Center を通して更新を入手できます: Cisco。 契約のない Cisco カスタマは 1-800-553-2447 か 1-408-526-7209 でまたは tac@cisco.com で E メールで Cisco Technical Assistance Center にコンタクトをとってアップグレードを入手できます。

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やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20110525-CVE-2011-1647

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2011-May-25

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。