Cisco 小さいセル コマンドの実行脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20140707-CVE-2014-3307 **初公開日 :** 2014-07-07 20:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCup47513	CVE-2014-3307

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 小さいセル製品の DHCP クライアント 実装の脆弱性は非認証、隣接した攻撃者がコマンドを実行し、可能性のある影響を受けたデバイスの完全な制御を引き継ぐことを可能にする可能性があります。

脆弱性は巧妙に細工された DHCP メッセージの不適当な解析が原因です。 攻撃者は影響を受けたデバイスへ巧妙に細工された DHCP メッセージを送信 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。 エクスプロイトは攻撃者がコマンドを実行し、可能性のある影響を受けたデバイスの完全な制御を引き継ぐことを可能にする可能性があります。

Cisco はセキュリティ通知の脆弱性を確認し、ソフトウェア アップデートをリリースしました。

この脆弱性を不正利用するために、攻撃者は影響を受けたソフトウェアに巧妙に細工された要求を送信 するために内部ネットワーク信頼されるへのアクセスを必要とするかもしれません。 このアクセス要件は正常なエクスプロイトの確率を制限する可能性があります。

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

顧客は影響を受けた製品バージョンの完全なリストのための Cisco バグ ID CSCup47513 を参照する必要があります。

脆弱性のある製品

このアラートが最初に送達された時; Cisco ユニバーサル小さいセル シリーズ ファームウェア

のバージョン R3.2、R3.3、R3.4、R3.5、R2.12、R2.13、R2.14、R2.15、R2.16 および R2.17 は脆弱でした。 Cisco ユニバーサル小さいセル シリーズ ファームウェアの他のバージョンはまた影響を受けるかもしれません。

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。

管理者は信頼されたユーザだけネットワーク アクセスをアクセスできることを許可するために助言されます。

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。

管理者は影響を受けた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-20140707-CVE-2014-3307

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2014-Jul-07

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。