Cisco パケット データ ネットワーク ゲートウェイ GTPv2 トンネル脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20150715-CVE-2015-4275 **初公開日 :** 2015-07-15 13:03 **バージョン 1.0 :** Final **CVSSスコア :** 5.0 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCut11534	CVE-2015-4275

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 パケット データ ネットワーク ゲートウェイ（PGW）のバージョン 2（GTPv2）のための脆弱性はリモート攻撃者 GPRS Tunneling Protocol（GTP）非認証により GTPv2 サービスの部分的なアベイラビリティを引き起こすようにする可能性があります。

脆弱性は着信 GTPv2 パケットヘッダーの入力の検証の欠けて当然です。 攻撃者は影響を受けたデバイスへ巧妙に細工された、不正 な GTPv2 パケットを送信 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により GTPv2 サービスの条件部分的なアベイラビリティの引き起こすことを可能にする可能性があります。

Cisco は脆弱性およびリリースされたソフトウェア アップデートを確認しました。

この脆弱性を不正利用するために、攻撃者は不正利用を信頼できないソースからネットワーク アクセスを制限する環境でさらに困難にする目標とされたデバイスに不正 な GTPv2 パケットを送信できる必要があります。

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

Cisco は影響を受けた製品バージョンの追加詳細および最新リストが含まれている登録ユーザ向けのバグID CSCut11534 をリリースしました。

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 ASR 5000 シリーズ ソフトウェア リリース 18.0.0.59167 および 18.0.0.59211 は脆弱でした。 Cisco ASR 5000 シリーズ ソフトウェアの新しいリリースはまた脆弱かもしれません。

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-20150715-CVE-2015-4275

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2015-Jul-15

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。