Cisco ASR 5500 システムアーキテクチャ関連ゲートウェイ GPRS Tunneling Protocol（GTP）サービス拒否の脆弱性

Medium	**アドバイザリーID :** cisco-sa-20170906-asr **初公開日 :** 2017-09-06 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 5.8 **回避策 :** Yes **Cisco バグ ID :** CSCve07119	CVE-2017-12217

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 ASR 5500 システムアーキテクチャ関連（SAE）ゲートウェイの General Packet Radio Service（GPRS）トンネリング プロトコル 入力 パケットハンドラの脆弱性はリモート攻撃者非認証により影響を受けたデバイスの部分的なサービス拒否（DoS）状態を引き起こすようにする可能性があります。

脆弱性はパケットヘッダーの不適当な入力の検証が GPRS Tunneling Protocol（GTP）原因です。 攻撃者は影響を受けたデバイスへ不正 な パケットを GPRS Tunneling Protocol（GTP） 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。 正常なエクスプロイトは攻撃者により影響を受けたデバイスの GTPUMGR プロセスは部分的な DoS 状態に終って、予想に反して再起動しますことを可能にする可能性があります。 GTPUMGR プロセスが再起動する場合、デバイスを通るトラフィックに簡潔な影響があ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-20170906-asr

該当製品

修正済みソフトウェア

この脆弱性は最初の修正済みリリース前にソフトウェア リリースを実行して、GPRS

Tunneling Protocol（GTP）使用するために設定される Cisco ASR 5500 システムアーキテクチャ関連（SAE）ゲートウェイに影響を与えます。 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

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。

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017-September-06

利用規約