

Cisco Packet Data Network Gateway GTPv2トンネルの脆弱性



アドバイザリーID : Cisco-SA-20150715-[CVE-2015-4275](#)
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](#)

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 Packet Data Network Gateway(PGW)バージョン2(GTPv2)のGPRSトンネリングプロトコル(GTP)の脆弱性により、認証されていないリモートの攻撃者がGTPv2サービスの部分的なアベイラビリティを引き起こす可能性があります。

この脆弱性は、着信GTPv2パケットヘッダーの入力検証の欠如に起因します。攻撃者は、巧妙に細工された不正なGTPv2パケットを該当デバイスに送信することにより、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はGTPv2サービスの部分的なアベイラビリティ状態を引き起こす可能性があります。

シスコはこの脆弱性を確認し、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には、攻撃者は不正なGTPv2パケットをターゲットデバイスに送信できる必要があります。信頼できない送信元からのネットワークアクセスを制限する環境では不正利用がより困難になります。

シスコはCVSSスコアを通じて、機能的なエクスプロイトコードが存在することを示していますが、このコードが一般に公開されることは確認されていません。

該当製品

シスコは登録ユーザ向けにBug ID [CSCut11534](#)をリリースしました。このIDには、詳細情報と、影響を受ける製品バージョンの最新リストが含まれています。

脆弱性のある製品

このアラートが最初に発行された時点では、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に脆弱性が存在していました。Cisco ASR 5000シリーズソフトウェアの新しいリリースにも脆弱性が存在する可能性があります。

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

適切なアップデートを適用することを推奨します。

管理者は、信頼できるユーザだけにネットワークアクセスを許可することを推奨します。

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

契約が有効なシスコのお客様は、[Cisco](#)のSoftware Centerからアップデートを入手できます。契約をご利用でないお客様は、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)に連絡するか、tac@cisco.comの電子メールでアップグレードを入手できます。

推奨事項

```
$propertyAndFields.get("recommendations")
```

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150715-CVE-2015-4275>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2015年7月

バージョン	説明	セクション	ステータス	日付
	ース			15日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。