Cisco ASR 5000およびASR 5500 TACACSのDoS脆弱性

Medium	**アドバイザリーID :** cisco-sa-20151012-asr **初公開日 :** 2015-10-12 22:20 **バージョン 1.0 :** Final **CVSSスコア :** 5.0 **回避策 :** No workarounds available **Cisco バグ ID :** CSCuw01984 CSCuw01985	CVE-2015-6334

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アグリゲーションサービスルータ(ASR)5000およびASR 5500(ASR5K)システムソフトウェアのTACACSプロトコル実装における脆弱性により、認証されていないリモートの攻撃者が、*vpnmgr*プロセスの再起動により部分的なサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、TACACSパケットヘッダーの不適切な入力検証に起因します。攻撃者は、巧妙に細工されたTACACSパケットをデバイスに送信することで、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、攻撃者は巧妙に細工されたTACACSパケットを解析するときに*vpnmgr*プロセスを再起動する可能性があるため、部分的なDoS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に対処するソフトウェアアップデートをリリースしています。この脆弱性を軽減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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151012-asr

該当製品

脆弱性のある製品

Cisco ASR 5000シリーズシステムソフトウェアリリース18.0.0.57828および19.0.M0.61045が稼働しているCisco ASR 5000およびCisco ASR 5500デバイスには脆弱性が存在します。

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。

セキュリティ侵害の痕跡

ASR5Kは *vpnmgr*プロセスのコアファイルを書き込みます。これは、 **show crash**コマンドライン インターフェイス(CLI)コマンドを使用して表示できます。

 # show crash <#>

=== ================== ======== ========== ==============
======================

Time Process Card/CPU/SW HW_SER_NUM
PIDバージョンMIO/クラッシュカード

=== ================== ======== ========== ==============
======================

1 2010-Feb-16+07:56:37 vpnmgr 05/0/15340 19.0.M0.61045 ####################

回避策

回避策はありません。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

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-20151012-asr

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	初回公開リリース	-	Final	2015年10月12日

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。

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。