

ASR 5000 シリーズ ルータ IPsec VPN トンネル サービス拒否の脆弱性のための Cisco StarOS

Medium	アドバイザリーID : cisco-sa-20170621-asr	CVE-2017-3865
m	送達される : 2017-06-21 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 5.8	
	回避策 : Yes	
	Cisco バグ ID : CSCvc21129	

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 5000 シリーズ ルータのための Cisco StarOS の IPsec コンポーネントの脆弱性はすべてのアクティブIPsec VPN トンネルを終え、サービス拒否 (DoS) 状態に終って非認証、リモート攻撃者が可能にする可能性があります新しいトンネルが、確立することを防ぐことを。

脆弱性はインターネット キー エクスチェンジ (IKE) メッセージの不適切な処理が原因です。攻撃者は影響を受けたルータの方に巧妙に細工された IKE メッセージの送信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 *ipsecmgr* サービスはリロードしますことを可能にする可能性があります。サービスが再起動するまで終わるすべての IPsec VPN トンネルという結果に *ipsecmgr* サービスのリロードは終り、DoS 状態に終って可能性があります新しいトンネルが、確立されることを防ぐ。

この脆弱性に対処する回避策がありません。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-asr>

影響を受ける製品

脆弱性が存在する製品

この脆弱性は以下のシスコ製品に影響を及ぼします:

- ASR 5000 シリーズ ルータ
- 仮想パケットコア (VPC) ソフトウェア

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。

脆弱性が存在しない製品

この脆弱性に影響されるその他のシスコ製品は現在のところ見つかりません。

細部

回避策

この脆弱性に対処する回避策がありません。

固定ソフトウェア

修正済み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。

ソフトウェアのアップグレードを検討する際には、[Cisco Security Advisories and Alerts ページ](#)で入手できるシスコ製品のアドバイザリを定期的に参照して、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、顧客はアップグレードされるべきデバイスが十分なメモリが含まれ、現在のハードウェア および ソフトウェア構成が新しいリリースによってきちんとサポートされ続けることを確認するようする必要があります。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製品 のセキュリティ上の問題に対する回答チーム (PSIRT) はこのアドバイザリに説明がある脆弱性の公示が不正利用に気づいていません。

ソース

この脆弱性は内部 保全テストの間に発見されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-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	初版リリース		FINAL	2017-June-21

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。