

Cisco ISMの不正な認証ヘッダーパケットに関するDoS脆弱性

Medium	アドバイザーID : Cisco-SA-20130507-CVE-2013-1241	CVE-2013-1241
	初公開日 : 2013-05-07 20:20	
	バージョン 1.0 : Final	
	CVSSスコア : 6.3	
	回避策 : No Workarounds available	
	Cisco バグ ID : CSCub92025	

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

ISR G2用Cisco ISMモジュールでの認証ヘッダーパケット処理の脆弱性により、認証されたりモートの攻撃者が該当モジュールのリロードを引き起こす可能性があります。

この脆弱性は、不正な認証ヘッダーパケットの不適切な処理に起因します。攻撃者は、確立されたIPSecセキュリティアソシエーションを介して不正な認証ヘッダーパケットのストリームを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、攻撃者は該当モジュールのリロードを引き起こし、IPsecトラフィックのサービス妨害(DoS)状態を引き起こす可能性があります。

シスコは、セキュリティ通知の脆弱性を確認し、ソフトウェアアップデートが利用可能であることを確認しました。

この脆弱性をエクスプロイトするには、攻撃者がターゲットシステムに認証を行い、不正な認証ヘッダーパケットを送信する必要があります。このアクセス要件により、不正利用が成功する可能性が制限されます。

影響を受けるバージョンの最新リストについては、「ベンダーのお知らせ」セクションのバグレポートを参照してください。

シスコはCVSSスコアを通じて、機能不正利用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ているかどうかは不明です。

該当製品

シスコは、[CVE-2013-1241](#)のリンクで、バグID [CSCub92025](#)のセキュリティ通知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公開された時点では、Cisco IOSソフトウェアリリース15.3(200)T以前には脆弱性が存在していました。Cisco IOSソフトウェアの以降のリリースも影響を受け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、特権を持つユーザだけに管理システムまたは管理システムへのアクセスを許可することを推奨します。

デバイスへの特権管理アクセスを制限して、情報の漏えいと不正アクセスを防止します。管理プレーンやコントロールプレーン保護などのセキュリティ機能がデバイスに適用されていることを確認します。インタラクティブ管理セッションを保護するためのベストプラクティスについては、『[Cisco Guide to Harden Cisco IOS Devices](#)』を参照してください。

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

有効な契約を結んでいるシスコのお客様は、シスコのサポートチームに連絡して、この脆弱性の修正を含むソフトウェアバージョンへのアップグレードをサポートしてもらう必要があります。契約を結んでいないお客様は、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で連絡するか、tac@cisco.comに電子メールで連絡して支援を受けることができます。

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-20130507-CVE-2013-1241>

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	2013年5月7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。