

Cisco IOSソフトウェアインターネットキーエクスチェンジバージョン2(IKEv2)アンチリプレイ保護が無効にされた脆弱性

Medium

アドバイザリーID : Cisco-SA-20131030-CVE-2013-5548

[CVE-2013-5548](#)

初公開日 : 2013-10-30 19:26

最終更新日 : 2015-02-24 21:39

バージョン 2.0 : Final

CVSSスコア : [5.0](#)

回避策 : No Workarounds available

Cisco バグ ID : [CSCuj47795](#)

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 IOSソフトウェアのインターネットキーエクスチェンジバージョン2(IKEv2)プロトコルの実装における脆弱性により、IPSecのアンチリプレイ機能が無効になる場合があります。この問題は、フェーズ2 IPSecセキュリティアソシエーション(SA)に対して、高度暗号化規格(AES)Galois/カウンタモード(AES-GCM)またはAES Galoisメッセージ認証コード(AES-GMAC)アルゴリズムを使用している場合にのみ発生します。

この脆弱性は、IPsecフェーズ2 SAのアンチリプレイ機能を有効または無効にするために必要なロジックの不適切なコーディングに起因します。攻撃者は、IPsecトンネルを通過するトラフィックを送信することで、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、トラフィックを消費するアプリケーションが独自のシーケンスまたはアンチリプレイチェックを実装していない限り、攻撃者は以前に送信されたトラフィックをリプレイできる可能性があります。IPSecの機密性および認証機能は、この脆弱性の影響を受けません。

シスコは、セキュリティ通知で脆弱性を確認し、ソフトウェアアップデートをリリースしました。

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

影響を受ける製品バージョンの完全なリストについては、Cisco Bug ID [CSCuj47795](#)を参照してください。

脆弱性のある製品

Cisco IOSバージョン15.3(3)M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。

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。

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。

IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけに該当システムへのアクセスを許可することを検討することもできます。

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

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で電子メールを介してサポート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-20131030-CVE-2013-5548>

改訂履歴

バ ー ジ ン	説 明	セ ク シ ョ ン	ス テ ー ス	日 付

ヨ ン		ヨ ン	タ ス	
1 . 0	Cisco IOSソフトウェアには、認証されていないリモートの攻撃者がターゲットデバイスのIPsecのアンチリプレイ機能を変更できる可能性のある脆弱性が存在します。更新プログラムが利用可能です。	適 用 外	F i n a l	20 13 年 10 月 30 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。