Cisco Firewall サービス モジュール、PIX および ASA SIP メッセージ サービス拒否の脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20070214-CVE-2007-0961 **初公開日 :** 2007-02-14 23:02 **最終更新日 :** 2012-07-14 21:14 **バージョン 2.0 :** Final **CVSSスコア :** 3.3 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2007-0961

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 Firewall サービス モジュールにより、PIX セキュリティ アプライアンス モデルおよび ASA セキュリティ アプライアンス モデルは非認証を可能にする可能性があるサービス拒否（DoS）状態を引き起こすために脆弱性がリモート攻撃者含まれています。

SIP メッセージを処理する場合のエラーによる脆弱性存在。 非認証は影響を受けたデバイスへ形式が間違った SIP メッセージを送信 することによって、リモート攻撃者この脆弱性を不正利用する可能性があります。 この操作により影響を受けたデバイスは一時 DoS 状態に終って、リロードします可能性があります。 繰り返された不正侵入は耐久性がある DoS 状態という結果に終る場合があります。

Cisco は Security Advisory のこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

不正利用の成功は攻撃者により一時 DoS 状態とみなすことができる影響を受けたデバイスはリロードしますことを可能にします。 繰り返された不正侵入は耐久性があるサービス拒否状態という結果に終る可能性があります。

システムは SIP メッセージの強度のパケット インスペクションがイネーブルになっている場合その時だけ脆弱です。 これは FWSM 2.x および ASA/PIX 6.x の**フィックスアップ** コマンドによって処理され、これらのバージョンの SIP パケットのためにデフォルトでイネーブルになっています。 それは FWSM 3.x および ASA/PIX 両方 7.x の **inspect コマンド**によって処理されます。 inspect コマンドは FWSM 3.x でデフォルトでイネーブルになり、ASA/PIX 7.x でデフォルトでデ

ィセーブルにされます。

該当製品

Cisco は次のリンクで Cisco Firewall サービス モジュールの Cisco バグ ID CSCsg80915 をアドレス指定するために Security Advisory を再リリースしました: cisco-sa-20070214-fwsm

Cisco は次のリンクで Cisco PIX および ASA アプライアンスの Cisco バグ ID CSCse27708 および CSCsd97077 をアドレス指定するために Security Advisory をリリースしました: cisco-sa-20070214-pix

US-CERT は次のリンクで脆弱性に関する注記を発表しました: VU#430969

脆弱性のある製品

Cisco Firewall サービス モジュールの次のバージョンを稼動するシステムは脆弱です:

2.3(4.12) 以前の Cisco Firewall サービス モジュール
3.1(3.24) 以前の Cisco Firewall サービス モジュール

次のソフトウェア リリースを使用している場合 Cisco PIX 500 シリーズ セキュリティ アプライアンスおよび Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは脆弱です:

6.3(5.115) 前のバージョン 6.0
7.0(5.2) 前のバージョン 7.0
7.1(2.5) 前のバージョン 7.1

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

管理者は適切なパッチを加えるように助言されます。

管理者は影響を受けたシステムへのアクセスを制限するように助言されます。

管理者は SIP メッセージの強度のパケット インスペクションをディセーブルにすることを考えるかもしれません。 これはパススルーに許されるかもしれない別の方法で検出されるかもしれないいくつかの悪質なパケットとして SIP セッションを終了しているデバイスに影響を与えるかもしれません。

3.x FWSM システムまたは 7.x ASA/PIX デバイスの管理者は信頼できないホストからのトラフィックを拒否するように助言されます。 ただし、SIP が UDP ベース プロトコルであるので、スプ

ーフィングする IPソースアドレスが IPベース ACL をバイパスするのに使用できます。

Cisco によって加えられる知性チームは識別を管理者に指示するために次のドキュメントガイドを作成し、軽減はアップデートされたソフトウェアを加える前にこの脆弱性を不正利用するように試みます: cisco-air-20070214-firewall

修正済みソフトウェア

アクティブな契約を持つ Cisco カスタマは次のリンクで Software Center を通して更新を入手できます: Cisco。 契約のない Cisco カスタマは 1-800-553-2447 か 1-408-526-7209 でまたは tac@cisco.com で E メールで Cisco Technical Assistance Center にコンタクトをとってアップグレードを入手できます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20070214-CVE-2007-0961

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2007 年 2 月 14 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。