

# Cisco PIX および ASA TCPトラフィック インспекション サービス拒否の脆弱性

Medium	アドバイザーID : Cisco-SA-20070214-CVE-2007-0959	<a href="#">CVE-2007-0959</a>
	初公開日 : 2007-02-14 21:57	
	バージョン 1.0 : Final	
	CVSSスコア : <a href="#">3.3</a>	
	回避策 : <a href="#">Yes</a>	
	Cisco バグ ID :	

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 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 (ASA) は非認証を可能にする可能性があるサービス拒否 (DoS) 状態を引き起こす影響を受けたデバイスによりクラッシュするために脆弱性がリモート攻撃者含まれています。

不正な TCP パケットの不十分な処理によるこの脆弱性存在は流れます。非認証は影響を受けたデバイスへ巧妙に細工された一続きのパケット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。これは攻撃者が DoS 状態に終ってデバイスを、クラッシュすることを可能にする可能性があります。

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。

脆弱であるシステムに関しては TCP ベースのプロトコルのインスペクション用の設定する必要があります。A は TCP プロトコルを使用するアプリケーションをおよび inspect コマンドと規定するを使用してこれされます。基づく TCP、インスペクション用にデフォルトで設定される A はこれ FTP および HTTP が含まれています。A によって影響を受けるデバイスはデフォルト設定で脆弱です。

影響を受けたデバイスが企業のサイトの境界に沿って一般的に配置されるので、信頼できないユーザからのトラフィックのために開いたポートがある場合攻撃に脆弱かもしれません。A はこれトラフィックが Web か FTP サーバ。A に幸いにもアクセスするようすが含まれていますこの問題を解決する回避策があります。A はすべての管理者この回避策をなるべく早く設定するため

に助言されます。

## 該当製品

### 修正済みソフトウェア

ソフトウェアのリリースバージョン 7.2.2 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。

### 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。

## 改訂履歴

バージョン	説明	Section	ステータス	日付
1.0	<a href="#">初版リリース</a>	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。