Cisco PIX および ASA TCPトラフィック インスペクション サービス拒否の脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20070214-CVE-2007-0959 **初公開日 :** 2007-02-14 21:57 **バージョン 1.0 :** Final **CVSSスコア :** 3.3 **回避策 :** Yes **Cisco バグ ID :**	CVE-2007-0959

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。Â 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 コマンドこと**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 Â はこれ FTP および HTTP が含まれています。Â 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。Â はこれトラフィックが Web か FTP サーバ。Â に幸いにもアクセスするように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。Â 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	初版リリース	該当なし	Final	2007 年 2 月 14 日

利用規約

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。