Cisco PIX および ASA ローカル メソッド 特権拡大脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20070214-CVE-2007-0960 **初公開日 :** 2007-02-14 23:06 **バージョン 1.0 :** Final **CVSSスコア :** 6.0 **回避策 :** Yes **Cisco バグ ID :**	CVE-2007-0960

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) は認証される可能にする可能性があるデバイスの高い特権を得るために脆弱性がリモート攻撃者含まれています。

ユーザ認証におけるローカル メソッドを使用してデバイスで存在 するただ脆弱性。 攻撃者はまたゼロの特権のローカルデータベースでデバイスに認証定義され、できる必要があります。 これらの条件が満たされる場合、攻撃者は彼ら自身に管理権限を与える可能性があります。

ベンダーはこの問題に機能エクスプロイト コードのアベイラビリティを反映するために CVSS スコアを与えました; ただし、コードは共用利用可能であると知られていません。

Cisco はこの脆弱性を確認し、更新済ソフトウェアは利用できます。

この脆弱性を不正利用するために、攻撃者はゼロの特権レベルが付いているローカルデータベースで影響を受けたデバイスに認証定義され、できる必要があります。 これらの条件は信頼されたユーザだけローカルデータベースで定義する必要があるように、不正侵入の確率を大幅に下げます。 影響を受けたデバイスがデフォルト 設定で脆弱ではないことにまた注意する必要があります。

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