Cisco Firewall 製品の無意識パスワード修正脆弱性

severity

アドバイザリーID : cisco-sa-20060823-firewall

初公開日 : 2006-08-23 16:00

バージョン 1.0 : Final

回避策 : Yes

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 アプライアンスのためのソフトウェアのある特定のバージョン、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス（ASA）、および Firewall Services Module （FWSM）はユーザ 介入なしで変更されるべきスタートアップ コンフィギュレーションでローカルで定義されたユーザ名の EXECパスワード、パスワード、およびイネーブル パスワードを引き起こすかもしれないソフトウェアバグから影響を受けます。

許可されていないユーザはスタートアップ コンフィギュレーションのパスワードが変更された後リロードされたデバイスへのアクセス権を得ることを試みるのにこの不具合を利用できます。 さらに、許可されたユーザはロックアウトされ、影響を受けたデバイスを管理する機能を失う場合があります。

Cisco では、該当するお客様用に、この問題に対応するソフトウェアを無償で提供しております。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060823-firewall で掲示されます。

該当製品

修正済みソフトウェア

の次のソフトウェア バージョン実行するとき PIX 500 シリーズ セキュリティ アプライアンスおよび ASA 5500 シリーズは適応型セキュリティ アプライアンス（ASA）影響を受けています：

- 7.0(x) トレインのバージョン（を含む暫定バージョン）以前の 7.0(5)
- 7.1(2.4) 以前の 7.1(x) トレインのバージョン（を含む暫定バージョン）

Cisco Catalyst 6500 スイッチ用の FWSM は Cisco 7600 シリーズ ルータ次のソフトウェア バージョンを実行するとき影響を受けて、:

- 3.1(1.6) 以前の 3.1(x) トレインのバージョン（を含む暫定バージョン）

脆弱性を含んでいないことが確認された製品

の次のソフトウェア バージョン実行するとき PIX 500 シリーズ セキュリティ アプライアンスおよび ASA 5500 シリーズは適応型セキュリティ アプライアンス（ASA）*影響を受けていません*:

- ASA が pre-7.x コードを実行しないのでだけ pre-7.x バージョン（PIX）
- 7.2(1) およびそれ以降

Cisco Catalyst 6500 スイッチ用の FWSM は Cisco 7600 シリーズ ルータの次のソフトウェア バージョン実行するとき*影響を受けていないし*、:

- 1.x および 2.x バージョン
- 3.1(2) およびそれ以降

その他のCisco製品は現在この問題から影響を受けるために知られていません。

改訂履歴

リビジョン 1.0	2006-August-23	初回公開リリース

利用規約