

Cisco PIX Firewall Authentication Denial of Serviceの脆弱性

severity アドバイザリーID : cisco-sa-20011003-pix-firewall-auth-flood
初公開日 : 2001-10-03 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

バージョン 4.0 で導入される Cisco Secure PIX Firewall AAA認証 機能はシステムの認証ユーザによって始められるサービス拒絶 (DoS) 攻撃に脆弱です。この脆弱性は特定のコンフィギュレーションに影響を与え、PIXファイアウォールのリリースバージョンで解決されました。

この脆弱性は Cisco バグ ID CSCdt92339 を割り当てられました。

完全な表記は <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20011003-pix-firewall-auth-flood> で利用できます。

該当製品

修正済みソフトウェア

4.4(8)、5.0(3) 以前のソフトウェア バージョン 4.0 との CiscoセキュアPIX ファイアウォールのすべてのユーザは、5.1(3)、AAA認証を使用してコンフィギュレーションと 5.2(2) および 5.3(1) 危険な状態にあります。

影響を受けたコンフィギュレーションに始まる設定行があります:

```
pixfirewall# aaa authentication ...
```

脆弱性を含んでいないことが確認された製品

AAA認証を含むコンフィギュレーションはない影響を受けていません。PIXファイアウォールソフトウェア バージョン 6.0(1) および それ以降は影響を受けていません。

IOS Firewall 機能セットは上記の問題から影響を受けません。

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

リビジョン 1.0	2001-October-03	一般公開に関しては。
--------------	-----------------	------------

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。