

Cisco PIX 脆弱性

severity	アドバイザーID : cisco-sa-20031215-pix	CVE-2003-1004
	初公開日 : 2003-12-15 16:00	CVE-2003-1002
	バージョン 1.2 : Final	CVE-2003-1003
	回避策 : Yes	CVE-2003-1001
	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

この Cisco PIX Firewall のための諮問文書 2 脆弱性。これらの脆弱性は CSCeb20276 (SNMPv3) および CSCec20244 (VPNC) として文書化されています。

利用可能な回避策が CSCeb20276 (SNMPv3) の効果を軽減するためにあります。CSCec20244 (VPNC) のための対応策が見つからない場合。

このアドバイザーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20031215-pix> で掲示されます。

該当製品

修正済みソフトウェア

すべての Cisco PIX Firewall 実行するデバイスはこれらの脆弱性から下記に文書化されていますように影響を受けた Cisco PIX ファイアウォール ソフトウェア、影響を受けます。

- CSCeb20276 (SNMPv3)
6.3.1、6.2.2 およびそれ以前、6.1.4 およびそれ以前。 5.x.x およびそれ以前。
- CSCec20244 (VPNC)
6.2 (2.119) 6.2.3 に、含んだ両方。

6.3.x および 6.2.1 から 6.2 (2.118) 影響を受けてはなりません。

FireWall Service Module (FWSM) は SNMPv3 問題にまた脆弱で、[215-fwsm](#) として文書化されています。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。

ソフトウェアリビジョンを、型 `show version` コマンド・ライン プロンプトで確認するため。

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

リビジョン 1.2	2004- January- 26	リリースされたソフトウェアに影響を与えなかったため、CSCea28896 への取除かれた参照。SNMPv3 Workaround セクションへの追加された elaborative テキスト。
リビジョン 1.1	2003- Decembe r-17	ディセーブル SNMP サーバ対応策への追加されたクリア snmp-server コマンド。SNMPv3 詳細および回避策セクションへの追加された elaborative テキスト。
リビジョン 1.0	2003- Decembe r-15	初回公開リリース

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。本アドバイザリに関する情報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。