

PROTOS SIP テスト スイートによって発見されるマルチプル製品の脆弱性

severity	アドバイザーID : cisco-sa-20030221-protos	CVE-2003-1109
	初公開日 : 2003-02-21 17:00	CVE-2003-1114
	バージョン 1.0 : Final	CVE-2003-1115
	回避策 : Yes	CVE-2003-1112
	Cisco バグ ID :	CVE-2003-1113
		CVE-2003-1110
		CVE-2003-1111

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

複数のシスコ製品はセッション開始プロトコル (SIP) の処理で脆弱性が誘いますメッセージが含まれています。これらの脆弱性は SIP のための University of Oulu セキュア プログラム グループ (OUSPG) 「PROTOS」テスト スイートによって識別され、サービス拒否を生成 するのに繰り返し不正利用することができます。

このアドバイザーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030221-protos> で利用できます。

該当製品

修正済みソフトウェア

脆弱性を含む製品は次のとおりです。

- Cisco IP Phone モデル 4.2 前の 7940/7960 の実行 SIP イメージ
- Cisco IOS 12.2T および 12.2 つの Xトレインを実行する Cisco ルータ
- SIP サポートと、バージョン 5.2(1)にはじまっておよびバージョン 6.2(2)、6.1(4)、6.0(4) および 5.2(9) を含んでまで、しかし新しいソフトウェア バージョンを実行する Cisco PIX Firewall

脆弱性を含んでいないことが確認された製品

SIP プロトコルを動作させないか、または SIP プロトコルにネットワーク アドレス変換 (NAT) フィックスアップ サービスを提供しないシスコ製品は影響を受けていません。

改訂履歴

リビジョン 1.0	2003-February-21	初版リリース
--------------	------------------	--------

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。