Cisco PIX および ASA アプライアンスの複数の脆弱性

High	**アドバイザリーID :** cisco-sa-20071017-asa **初公開日 :** 2007-10-17 16:00 **バージョン 1.1 :** Final **CVSSスコア :** 7.8 **回避策 :** Yes **Cisco バグ ID :**	CVE-2007-5569 CVE-2007-5568

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（PIX）および Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）には、偽造パケットによる 2 つの脆弱性が存在し、デバイスのリロードが発生する場合があります。 これらの脆弱性は、Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）パケットの処理中や、PIX または ASA セキュリティ アプライアンス上で終端する Transport Layer Security（TLS）トラフィックの処理中に引き起こされる可能性があります。

注: これらの脆弱性は、互いに独立して存在します。 デバイスは 1 つとない他から影響を受けるかもしれません。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20071017-asa で掲示されます。

該当製品

修正済みソフトウェア

MGCP アプリケーション レイヤ プロトコルの検査が有効になっていて、デバイスで特定の 7.x ソフトウェア バージョンが稼働している場合、Cisco PIX および ASA セキュリティ アプライアンスは偽造 MGCP パケットの脆弱性に該当します。 バージョン 6.3.x への影響はありません。 デフォルトでは MGCP の検査は有効になっていません。 該当する具体的なバージョンについては、「ソフトウェア バージョンと修正」セクションを参照してください。

PIX および ASA セキュリティ アプライアンスは、PIX および ASA セキュリティ アプライアンス上で TLS セッションが終端する原因となる 1 つ以上の機能がソフトウェアに設定されている場合、特定の 7.x ソフトウェア バージョンが実行されているデバイスに影響する、偽造 TLS パケットの脆弱性による影響も受けます。 これらの機能には、クライアントレス WebVPN、AnyConnect および SSL VPN クライアントを使用したクライアント接続、HTTPS 管理、ネットワーク アクセスのカットスルー プロキシ、および暗号化された音声検査の TLS プロキシなどがあります（これらの機能に限りません）。 バージョン 6.3.x への影響はありません。 TLS セッションが PIX および ASA セキュリティ アプライアンス上で終端する原因となる機能は、デフォルトでは有効になっていません。 該当する具体的なバージョンについては、「ソフトウェア バージョンと修正」セクションを参照してください。

PIX および ASA セキュリティ アプライアンスに加え、偽造 MGCP パケットの脆弱性は、Cisco Firewall Services Module（FWSM; ファイアウォール サービス モジュール）にも該当します。 FWSM に関する詳細は関連アドバイザリ 017-fwsm で見つけることができます。

脆弱性のある Cisco PIX または ASA ソフトウェアのバージョンを実行しているかどうかを判断するには、**show version** Command-Line Interface（CLI; コマンドライン インターフェイス）コマンドを発行します。

次の例は、ソフトウェア リリース 7.2(3) を実行している Cisco ASA セキュリティ アプライアンスを示しています。

```
ASA# show version

Cisco Adaptive Security Appliance Software Version 7.2(3)

[...]
```

Cisco Adaptive Security Device Manager（ASDM）を使用してデバイスを管理している場合は、ログイン ウィンドウの表、または ASDM ウィンドウの左上にソフトウェアのバージョンが表示されます。 バージョンは次のように表示されます。

```
PIX Version 7.2(3)
```

脆弱性を含んでいないことが確認された製品

FWSM を除き、このアドバイザリで説明されている問題の脆弱性があると判明している Cisco 製品はありません。

改訂履歴

リビジョン 1.1	2007 年 10 月	AnyConnect および SSL VPN クライアントによるクライアント接続を含めるようにクライアントレス WebVPN を変更

	19日	
リビジョン 1.0	2007年10月17日	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、単独の転載や意訳を施した場合、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。