Cisco PIX および ASA TTL 脆弱性

High

アドバイザリーID : cisco-sa-20080123-asa
初公開日 : 2008-01-23 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-2008-0028

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

デバイスのリロードという結果に終るかもしれない Cisco 5500 シリーズ 存在 する 巧妙に細工された IPパケット脆弱性（ASA）および適応型セキュリティ アプライアンス（ASA）ソフトウェア Cisco PIX 500 シリーズ セキュリティ アプライアンス モデル（PIX）で。 この脆弱性は巧妙に細工された IPパケットの処理の間に Time To Live （TTL）デクリメント機能が有効に なるとき引き起こされます。

よくある脆弱性および公開（CVE）識別子 CVE-2008-0028 はこの脆弱性に割り当てられました。

シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。 この脆弱性に対しては回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080123-asa で掲示されます。

該当製品

修正済みソフトウェア

TTL 減少機能はバージョン 7.2(2)で導入され、デフォルトでディセーブルにされます。 Cisco に PIX および 7.2(3)006 前にソフトウェア バージョンをか 8.0(3) およびそれ実行する ASA セキュリティ アプライアンス モデルに有効に なる TTL デクリメント機能がです脆弱あります。

デフォルトで PIX および ASA セキュリティ アプライアンス モデル ソフトウェアは一時パケットの TTL を減少しません。 一時パケットの TTL を減少する機能は選択的なかグローバルに

policy-map クラスコンフィギュレーションモードで**一定接続デクリメント TTL** コマンドを使用することによって有効に することができます。 この機能 使用を**一定接続デクリメント TTL** コマンドのための **show running-config コマンド**および検索実行しているかどうか判別するため。 次の通りまたこのコマンドを捜すのに含引数を使用できます:

```
ASA#show running-config  |  include decrement-ttl
set connection decrement-ttl
ASA#
```

一定接続デクリメント TTL コマンドは設定された class-map の一部です。 実施されるこのコマンドのためにそれは policy-map を使用して適用する必要があります（グローバルにまたはインターフェイスに割り当てられる）。 Cisco ASA および PIX のモジュラ 政策の枠組に関する詳細については次のリンクを参照して下さい:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/mpc.html

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。 バージョン表示法は次に類似したです:

```
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

TTL デクリメント機能をサポートしないし、それのために明示的に設定されない ASA セキュリティ アプライアンス モデルおよび Cisco は PIX 脆弱ではないです。

注: TTL 減少機能はバージョン 7.2(2)で導入され、デフォルトでディセーブルにされます。 Cisco Firewall サービス モジュール（FWSM）は脆弱ではないです。

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。

改訂履歴

リビジョン 1.2	2008-April-25	CSCsk48199 への更新済 CVSS リンク。
リビジョン 1.0	2008-January-23	初版リリース

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。