Cisco PIXおよびASAの存続可能時間(TTL)の脆弱性

High

アドバイザリーID : cisco-sa-20080123-asa CVE-2008-0028
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 : No Workarounds available
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

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、巧妙に細工されたIPパケットの脆弱性が存在し、デバイスのリロードを引き起こす可能性があります。この脆弱性は、Time-to-Live（TTL；存続可能時間）の減少機能が有効になっている場合に、巧妙に細工されたIPパケットの処理中にトリガーされます。

この脆弱性には、Common Vulnerabilities and Exposures（CVE）識別子 CVE-2008-0028 が割り当てられています。

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ています。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、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080123-asa で公開されています。

該当製品

脆弱性のある製品

TTLの減分機能はバージョン7.2(2)で導入され、デフォルトでは無効になっています。7.2(3)006または8.0(3)より前のソフトウェアバージョンを実行し、TTL減少機能が有効になっているCisco PIXおよびASAセキュリティアプライアンスには、脆弱性が存在します。

デフォルトでは、PIXおよびASAセキュリティアプライアンスソフトウェアは一時的なパケットのTTLを減らしません。一時的なパケットのTTLを減分する機能は、選択的またはグローバ

ルにイネーブルにできます。これを行うには、policy-mapクラスコンフィギュレーションモードでset connection decrement-ttlコマンドを使用します。この機能が実行されているかどうかを判別するには、show running-configコマンドを使用して、set connection decrement-ttlコマンドを検索します。または、include引数を使用して、次のコマンドを検索することもできます。

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

set connection decrement-ttlコマンドは、設定されたクラスマップの一部です。このコマンドを有効にするには、（グローバルまたはインターフェイスに割り当てられた）ポリシーマップを使用して適用する必要があります。Cisco ASAおよびPIXのモジュラポリシーフレームワークの詳細については、次のリンクを参照してください。
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。バージョンの表記法は次のようになります。

```
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

Cisco PIXおよびASAセキュリティアプライアンスでTTLの減少機能がサポートされていないか、明示的に設定されていない場合は、この脆弱性の影響を受けません。

注：TTL減分機能はバージョン7.2(2)で導入され、デフォルトでは無効になっています。Cisco Firewall Services Module(FWSM)には脆弱性はありません。

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。

詳細

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、巧妙に細工されたIPパケットの脆弱性が存在し、デバイスのリロードを引き起こす可能性があります。この脆弱性は、Time-to-Live（TTL；存続可能時間）の減少機能が有効になっている場合に、巧妙に細工されたIPパケットの処理中にトリガーされます。この脆弱性は、Cisco Bug ID CSCsk48199(登録ユーザ専用)に記載されています。

回避策

クラスコンフィギュレーションモードでno set connection decrement-ttlコマンドを使用して、TTLデクリメント機能を無効にします。

```
ASA(config)#policy-map localpolicy1
ASA(config-pmap)#class local_server
ASA(config-pmap-c)#no set connection decrement-ttl
ASA(config-pmap-c)#exit
```

TTLベースの攻撃を識別して緩和する方法の詳細については、Cisco適用インテリジェンスホワイトペーパー『TTL Expiry Attack Identification and Mitigation』(http://cisco.com/web/about/security/intelligence/ttl-expiry.html)を参照してください。

修正済みソフトウェア

この脆弱性は、ソフトウェアバージョン7.2(3)6または8.0(3)以降で修正されています。

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080123-asa

改訂履歴

リビジョン 1.2	2008年4月25日	CSCsk48199のCVSSリンクを更新。
リビジョン 1.0	2008年1月23日	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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。