Cisco ASA の多重 脆弱点 適応型セキュリティ アプライアンス (ASA) ソフトウェアおよび Cisco PIX セキュリティ アプライアンス モデル

High	**アドバイザリーID :** cisco-sa-20090408-asa **初公開日 :** 2009-04-08 16:00 **バージョン 1.2 :** Final **CVSSスコア :** 7.8 **回避策 :** Yes **Cisco バグ ID :**	CVE-2009-1155 CVE-2009-1159 CVE-2009-1158 CVE-2009-1157 CVE-2009-1156 CVE-2009-1160

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 ASA 5500 シリーズ 適応型セキュリティアプライアンスおよび Cisco PIX セキュリティアプライアンスに複数の脆弱性が存在しています。 この Security Advisory はこれらの脆弱性の詳細を概説します:

- アカウント 上書きする 機能が使用された脆弱性である場合の VPN 認証 バイパス
- 巧妙に細工された HTTP パケット サービス拒否 （ DoS ）脆弱性
- 巧妙に細工された TCPパケット DoS 脆弱性
- 巧妙に細工された H.323 パケット DoS 脆弱性

- SQL*Net パケット DoS 脆弱性
- Access Control List（ACL）バイパス の 脆弱性

回避策はいくつかの脆弱性に利用できます。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090408-asa で掲示されます。

該当製品

修正済みソフトウェア

以下はこのアドバイザリ内の詳細に記述されているように各脆弱性の該当製品のリストです。

VPN 認証 バイパス の 脆弱性

IPsec か SSL ベース リモートアクセス VPN のために設定され、有効に なる 上書きする アカウントによってディセーブルにされる機能がある Cisco ASA または Cisco PIX セキュリティ アプライアンス モデルはこの脆弱性から影響を受けます。

注: 上書きする アカウントによってディセーブルにされた機能は Cisco ASA ソフトウェア バージョン 7.1(1) で導入されました。 Cisco ASA および PIXソフトウェアバージョン 7.1、7.2、8.0、および 8.1 はこの脆弱性から影響を受けます。 この機能はデフォルトでディセーブルにされます。

巧妙に細工された HTTP パケット DoS 脆弱性

Cisco ASA セキュリティ アプライアンス モデルに一連の巧妙に細工された HTTP パケットによって引き起こすことができるデバイスのリロードが生じるかもしれません SSL VPN のために設定されたときまたは Cisco Adaptive Security Device Manager（ASDM）接続を許可するために設定されたとき。 Cisco ASA ソフトウェア バージョンだけ 8.0 および 8.1 この脆弱性から影響を受けます。

巧妙に細工された TCPパケット DoS 脆弱性

Cisco ASA および Cisco PIX セキュリティ アプライアンス モデルは一連の巧妙に細工された TCP パケットによって引き起こすことができるメモリリークを経験するかもしれません。 バージョン 7.0、7.1、7.2、8.0、および 8.1 を実行する Cisco ASA および Cisco PIX セキュリティ アプライアンス モデルは次の機能の何れかのために設定されたとき影響を受けています:

- SSL VPN
- ASDM 管理アクセス
- Telnet 経由のアクセス
- SSH アクセス
- リモートアクセス VPN のための Cisco トンネリング 制御プロトコル（cTCP）
- 仮想 Telnet
- バーチャルHTTP
- 暗号化された音声 インスペクション用の Transport Layer Security（TLS）プロキシ
- ネットワーク アクセスのカットスルー プロキシ
- TCP インターセプト

巧妙に細工された H.323 パケット DoS 脆弱性

H.323 インスペクションが有効に なるとき Cisco ASA および Cisco PIX セキュリティ アプライアンス モデルに H.323 一連の巧妙に細工されたパケットによって引き起こすことができるデバイスのリロードが生じるかもしれません。 H.323 インスペクションはデフォルトで有効になります。 Cisco ASA および Cisco PIXソフトウェアバージョン 7.0、7.1、7.2、8.0、および 8.1 はこの脆弱性から影響を受けます。

SQL*Net パケット DoS 脆弱性

SQL*Net インスペクションが有効に なるとき Cisco ASA および Cisco PIX セキュリティ アプライアンス モデルに一連の SQL*Net パケットによって引き起こすことができるデバイスのリロードが生じるかもしれません。 SQL*Net インスペクションはデフォルトで有効に なります。 Cisco ASA および Cisco PIXソフトウェアバージョン 7.2、8.0、および 8.1 はこの脆弱性から影響を受けます。

アクセス制御リスト バイパス の 脆弱性

トラフィックがデバイスの内で設定される ACL の終わりに暗黙の deny 動作をバイパスするようにするかもしれない Cisco ASA および Cisco PIX セキュリティ アプライアンス モデルで存在 する脆弱性。 Cisco ASA および Cisco PIXソフトウェアバージョン 7.0、7.1、7.2、および 8.0 はこの脆弱性から影響を受けます。

ソフトウェア バージョンの判断

show version Command Line Interface（CLI）コマンドが Cisco PIX または Cisco ASA ソフトウェアの脆弱なバージョンが動作しているかどうか判別するのに使用することができます。 ソフトウェア バージョン 8.0(4) を実行する次の例は Cisco ASA を適応型セキュリティ アプライアンス（ASA）ソフトウェア示したものです:

```
ASA#show version
```

```
    Cisco Adaptive Security Appliance Software Version 8.0(4)
    Device Manager Version 6.0(1)

<output truncated>
```

次の例はソフトウェア バージョン 8.0(4) を実行する Cisco PIX セキュリティ アプライアンス モデルを示したものです:

```
PIX#show version

Cisco PIX Security Appliance Software Version 8.0(4)
Device Manager Version 5.2(3)

<output truncated>
```

Cisco ASDM をデバイスを管理するのに使用する顧客はソフトウェア バージョンを Login ウィンドウまたは ASDM ウィンドウの左上のコーナーの表で表示する見つけることができます。

脆弱性を含んでいないことが確認された製品

Cisco Catalyst 6500 シリーズ スイッチ用の Cisco Firewall サービス モジュール（FWSM）および Cisco 7600 シリーズ ルータおよび Cisco VPN 3000 シリーズ コンセントレータはこれらの脆弱性の何れかから影響を受けません。 Cisco PIX セキュリティ アプライアンス モデル ソフトウェア バージョン 6.x はこれらの脆弱性の何れかから影響を受けません。 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。

改訂履歴

リビジョン 1.2	2009-April-13	8.1(2)16 からのソフトウェア テーブルの巧妙に細工された HTTP パケット DoS 脆弱性セクションの 8.1(2)19 への変更された推奨されるリリース。
リビジョン 1.1	2009-April-08	不正利用事例と公式発表 アップデート。
リビジョン 1.0	2009-April-08	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。