Cisco PIX および Cisco ASA の多重 脆弱点

High

アドバイザリーID : cisco-sa-20081022-asa

初公開日 : 2008-10-22 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : Yes

Cisco バグ ID :

CVE-2008-3815

CVE-2008-3816

CVE-2008-3817

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。 このアドバイザリは以下の脆弱性の要点について説明しています。

- Windows NT ドメイン 認証 バイパス の 脆弱性
- IPv6 サービス拒否の脆弱性
- 暗号アクセラレータ メモリリーク の 脆弱性

注： これらの脆弱性は相互に関連していません。 ある機器が 1 つの脆弱性の影響を受け、他の脆弱性の影響は受けない場合もあります。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 この中のいくつかの脆弱性には影響を軽減する回避策が存在します。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20081022-asa で掲示されます。

該当製品

修正済みソフトウェア

以下に本アドバザリの各脆弱性の詳細について示します。

Windows NT ドメイン 認証 バイパス の 脆弱性

Microsoft Windows NT ドメイン 認証が理由で Cisco ASA および Cisco PIXデバイスを VPN 認証 バイパス の 脆弱性に敏感であるかもしれないです発行して下さい。 Microsoft Windows NT ドメイン 認証を使用して IPSec か SSL ベース リモートアクセス VPN のために設定される Cisco ASA または Cisco PIX セキュリティ アプライアンス モデルは脆弱かもしれません。 外部認証（すなわち、LDAP、RADIUS、TACACS+、SDI、またはローカルデータベース）の他のどの型も使用しているデバイスはこの脆弱性から影響を受けません。

Windows NT ドメイン 認証が Cisco ASA の Command Line Interface （CLI）を使用してどのように設定されるか次の例に示されています:

```
aaa-server NTAuth protocol nt
 aaa-server NTAuth (inside) host 10.1.1.4
 nt-auth-domain-controller primary1
```

また、デバイスが Windows NT ドメイン 認証 使用のために **show running-config** 設定されるかどうか見るため **| nt auth ドメイン コントローラ** コマンドを**含んで下さい**。

IPv6 サービス拒否の脆弱性

ソフトウェア バージョン 7.2(4)9 か 7.2(4)10 を実行しているおよび IPv6 のために設定されて脆弱かもしれません Cisco ASA および Cisco PIX セキュリティ アプライアンス モデルは。 この脆弱性は IPv4 のためにだけ設定されるデバイスに影響を与えません。

注： IPv6 機能はデフォルトで消えます。

IPv6 は **IPv6 アドレス** interface コマンドを使用して Cisco ASA および Cisco PIX セキュリティ アプライアンス モデルで有効に なります。 デバイスが IPv6 使用のために **show running-config** 設定されるかどうか確認するため **| IPv6** コマンドを**含んで下さい**。

また、次の例に示すように特権EXECモードの**提示 IPv6 interface コマンド**を使用して IPv6 のために、設定されるインターフェイスのステータスを表示することができます:

```
hostname# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
dmz [up/up]
    unassigned
```

この例では、**外部**および **dmz** インターフェイスは IPv6 のために設定されません。

暗号アクセラレータ メモリリーク の 脆弱性

Cisco ASA 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。 このメモリリークはハードウェア暗号化アクセラレータのための初期化コードで行われます。 8.0.x のソフトウェア バージョンを実行しているデバイスはです脆弱リリースします。

注: 7.0 のソフトウェア バージョンを実行している Cisco ASA アプライアンス、7.1、および 7.2 リリースは脆弱ではないです。 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せん。

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

```
ASA# show version

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

[...]
```

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。

脆弱性を含んでいないことが確認された製品

Cisco Firewall サービス モジュール（FWSM）はこれらの脆弱性の何れかから影響を受けません。 バージョン 6.x を実行する Cisco PIX セキュリティ アプライアンス モデル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 1.0	2008-October-22	初版リリース

利用規約