ファイアウォール サービス モジュールの複数の脆弱性

High

アドバイザリーID : cisco-sa-20071017-fwsm
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-2007-5570
CVE-2007-5571
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 Firewall Services Module（FWSM; ファイアウォール サービス モジュール）には、細工を施されたパケットに関連する脆弱性が 2 つ存在し、FWSM のリロードの原因となる場合があります。 これらの脆弱性は、HTTPS 要求の処理中や 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）パケットの処理中に引き起こされる可能性があります。

3 番目の脆弱性は、アクセス リストが操作された後、Access Control List（ACL; アクセス コントロール リスト）のエントリが評価されない原因となる場合があります。

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 017-fwsm で掲示されます。

該当製品

修正済みソフトウェア

FWSM 上の HTTPS サーバが有効になっていて、ソフトウェア バージョン 3.1(5) 以前または 3.2(1) が稼働している場合、FWSM は細工を施された HTTPS 要求の脆弱性に該当します。 バージョン 2.3.x は該当しません。 デフォルトでは HTTPS サーバは有効になっていません。

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、デバイスでソフトウェア バージョン 3.1(5) 以前が稼働している場合、FWSM は細工を施された MGCP パケットの脆弱性に該当します。 バージョン 2.3.x および 3.2.x は該当しません。 デフォルトでは MGCP の検査は有効になっていません。

FWSM は、ACL が正常に動作しない原因となる場合がある、アクセス コントロール リスト破損の脆弱性に該当します。つまり、ACL によって、通常であれば拒否されるトラフィックが許可されたり、通常であれば許可されるトラフィックが拒否されたりする場合があります。 該当するバージョンには、3.1(6) 以前と 3.2(2) 以前が含まれます。 バージョン 2.3.x は該当しません。

FWSM に加えて、細工を施された MGCP のパケットの脆弱性は、PIX 500 シリーズ セキュリティ アプライアンスおよび Cisco ASA 5500 適応型セキュリティ アプライアンスにも該当します。 PIX および ASA に影響を与える脆弱性に関する詳細は http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20071017-asa にある関連アドバイザリで見つけることができます。

脆弱性のあるバージョンの FWSM ソフトウェアを実行しているのかどうかを判断するには、Cisco IOS または Cisco CatOS から **show module** 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、どのモジュールとサブモジュールがシステムにインストールされているのかを確認します。

次の例は、スロット 4 にファイアウォール サービス モジュール（WS-SVC-FWM-1）が搭載されたシステムを示しています。

```
switch#show module
 Mod Ports Card Type                                Model              Serial No.
 --- ----- -------------------------------------- ------------------ -----------
 1   48    SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAxxxxxxxxx
 4    6    Firewall Module                        WS-SVC-FWM-1       SAxxxxxxxxx
 5    2    Supervisor Engine 720 (Active)         WS-SUP720-BASE     SAxxxxxxxxx
 6    2    Supervisor Engine 720 (Hot)            WS-SUP720-BASE     SAxxxxxxxxx
```

正しいスロットの場所を確認した後、**show module <slot number>** コマンドを発行して、実行されているソフトウェア バージョンを識別します。

```
switch#show module 4
 Mod Ports Card Type                                Model              Serial No.
 --- ----- -------------------------------------- ------------------ -----------
 4    6    Firewall Module                        WS-SVC-FWM-1       SAxxxxxxxxx

 Mod MAC addresses                       Hw     Fw           Sw           Status
 --- ----------------------------------- ------ ------------ ------------ -------
 4   0003.e4xx.xxxx to 0003.e4xx.xxxx    3.0    7.2(1)       3.1(3)       Ok
```

この例は、「Sw」の下のカラムに示されているように、FWSM によってバージョン 3.1(3) が実行されていることを示しています。

注： Cisco IOS の最近のバージョンは **show module コマンド**からの出力で各モジュールのソ

フトウェア バージョンを示します; 従って、**show module <slot number>** コマンドを実行することは必要ではないです。

あるいは、次に示すように、**show version** コマンドを使用して FWSM から情報が直接取得される場合もあります。

```
FWSM#show version
FWSM Firewall Version 3.1(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。

```
FWSM Version: 3.1(3)
```

[脆弱性を含んでいないことが確認された製品](#)

Cisco PIX 500 シリーズ セキュリティ アプライアンスと Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス以外には、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。

脆弱性を含んでいないことが確認された製品

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 1.1	2007 年 10 月 31 日	FWSM バージョン 3.2(3) の配布予定日を更新
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