FWSM URL フィルタリング な ソリューション TCP ACL バイパス の 脆弱性

severity	**アドバイザリーID :** cisco-sa-20050511-url	CVE-2005-1517
	初公開日 : 2005-05-11 16:00	
	バージョン 1.0 : Final	
	回避策 : Yes	
	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 Firewall サービス モジュール（FWSM）は Catalyst 6500 シリーズ スイッチ用の高速、統合ファイアウォール モジュールおよび Cisco 7600 シリーズ ルータです。 受信 TCP パケットが明示的にそれらをフィルタリングするように意図されているアクセス リストエントリをバイパスできる URL、FTP、または HTTPS フィルタリングが有効に なる場合の Cisco Firewall サービス モジュールで存在 する脆弱性。

Cisco はこの脆弱性に対処するためにフリーソフトを使用できるようにしました。 この脆弱性に対しては、影響を緩和するための回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050511-url で掲示されます。

該当製品

修正済みソフトウェア

コンテンツフィルタリングのための例外を許可するために設定されたとき Firewall Services Module （FWSM）の Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ インターネット ルータだけバージョン 2.3.1 の実行をインストールするか、または前に影響を受けています。

内部ホストが別のネットワークにアクセスするようにするフィルタ 例外の設定例はあるかもしれません

```
FWSM#show filter
filter https except 0.0.0.0 0.0.0.0 10.1.3.0 255.255.255.0
filter ftp except 0.0.0.0 0.0.0.0 10.1.3.0 255.255.255.0
filter url except 0.0.0.0 0.0.0.0 10.1.3.0 255.255.255.0
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter ftp 21 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter https 443 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

、このアドバイザリで説明されている脆弱性に敏感かもしれない**以外**結果として生じる出力が引数の**フィルタ** コマンドがの含まれていれば。

脆弱性のあるバージョンの FWSM ソフトウェアが稼働しているかどうかを判別するには、IOS か CatOS で **show module** コマンドを実行して、システムにインストールされているモジュールとサブモジュールを確認します。

次の例は、ファイアウォール サービス モジュール（WS-SVC-FWM-1）がスロット 4 にインストールされたシステムを示しています。

```
6506-B#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
```

正しいスロットを見つけたら、**show module <スロット番号>** コマンドを実行して、稼働しているソフトウェアのバージョンを確認します。

```
6506-B#sho 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)       2.3(1)       Ok
```

この例では、上記の「Sw」列に示されているように、FWSM ではバージョン 2.3(1) が動作しています。

また、情報はまた **show version コマンド**によって FWSM から直接得られるかもしれません:

```
FWSM#show version

FWSM Firewall Version 2.3(1)
```

PIX Device Manager （PDM）によって FWSM を管理している顧客向けにアプリケーションに単にログイン すれば、バージョンは Login ウィンドウの表またはに類似した ラベルによって示される PDM ウィンドウの左上 の コーナーで見つけられるかもしれません:

FWSM Version: 2.3(1)

脆弱性を含んでいないことが確認された製品

同じような機能を用いる製品は、Cisco PIX セキュリティ アプライアンス モデルおよび Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA） 5500 シリーズのような、影響を受けていません。

この脆弱性に該当するその他の Cisco 製品は現在のところ見つかっていません。

改訂履歴

リビジョン 1.0	2005-May-11	初回公開リリース

利用規約