Cisco Firewall サービス モジュールの多重 脆弱点

High	**アドバイザリーID :** cisco-sa-20100804-fwsm **初公開日 :** 2010-08-04 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-2010-2819 CVE-2010-2818 CVE-2010-2821 CVE-2010-2820

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

多重 脆弱点は 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）にあり、Cisco 7600 シリーズ ルータそれにより Cisco FWSM は巧妙に細工された SunRPC かある特定の TCP パケットを処理した後リロードしますかもしれません。 この脆弱性が繰り返し悪用されると、DoS 状態が続く可能性があります。

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。 回避策はこのアドバイザリで表われる脆弱性に利用できます。

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。

このアドバイザリは 804-fwsm で掲示されます。

注: Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスはこのアドバイザリに説明がある SunRPC インスペクション脆弱性から影響を受けます。 別途の Cisco Security Advisory は Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに影響を与える他の脆弱性およびこれを表わすために公開されました。 アドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100804-asa で利用できます。

該当製品

修正済みソフトウェア

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）は多重 脆弱点から Cisco 7600 シリーズ ルータ影響を受け。 Cisco FWSM ソフトウェアの影響を受けたバージョンは特定の脆弱性によって変わります。

SunRPC インスペクション サービス拒否の脆弱性

SunRPC インスペクションが有効に なるときだけ Cisco FWSM ソフトウェア バージョン 3.x および 4.x はこれらの脆弱性から影響を受けます。 SunRPC インスペクションはデフォルトで有効に なります。

SunRPC インスペクションが有効に なるかどうか確認するために、**show service ポリシーを**使用して下さい **| sunrpc** コマンドを**含み、**次の例に示すように、コマンドが出力を戻すことを確認して下さい:

```
fwsm#show service-policy | include sunrpc
      Inspect: sunrpc , packet 0, drop 0, reset-drop 0
```

また、有効に なる SunRPC インスペクションがあるデバイスに次と同じような設定があります:

```
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  ...
  inspect sunrpc
  ...
!
service-policy global_policy global
```

注: Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスはこのアドバイザリに説明がある SunRPC インスペクション脆弱性から影響を受けます。 別途の Cisco Security Advisory は Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに影響を与える他の脆弱性およびこれを表わすために公開されました。 アドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100804-asa で利用できます。

TCP サービス拒否の脆弱性

マルチモードで（仮想 な ファイアウォールと）および次の機能の何れかで設定されたとき Cisco FWSM ソフトウェア バージョン 3.x および 4.x はこの脆弱性から影響を受けます:

- ASDM 管理アクセス

- Telnet
- SSH

FWSM が多重 モードで動作しているかどうか確認するために、次の例に示すように**提示モード コマンドを**、使用して下さい:

```
FWSM(config)#show mode
Security context mode: multiple
The flash mode is the SAME as the running mode.
```

次のコマンドは HTTPS サーバをイネーブルに設定し、192.168.1.0/24 ネットワークのアドレスの内部インターフェイスのホストだけ ASDM、SSH または Telnet接続を作成するように使用されます:

```
asa(config)# http server enable
asa(config)# http 192.168.1.0 255.255.255.0 inside
asa(config)# telnet 192.168.1.0 255.255.255.0 inside
asa(config)# ssh 192.168.1.0 255.255.255.0 inside
```

ソフトウェア バージョンの判別

動作している Cisco FWSM ソフトウェアのバージョンを判別するために、どんなモジュールおよび補助的なモジュール システムでインストールされているか識別する Cisco IOSソフトウェアまたは Cisco Catalystオペレーティング システム システム・ソフトウェアからの **show module コマンドを**発行して下さい。

次の例はスロット 2 にインストールされる Cisco FWSM （ WS-SVC-FWM-1 ）とのシステムを示したものです:

```
switch>show module
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1   16  SFM-capable 16 port 1000mb GBIC        WS-X6516-GBIC      SAL06334NS9
  2    6  Firewall Module                        WS-SVC-FWM-1       SAD10360485
  3    8  Intrusion Detection System             WS-SVC-IDSM-2      SAD0932089Z
  4    4  SLB Application Processor Complex      WS-X6066-SLB-APC   SAD093004BD
  5    2  Supervisor Engine 720 (Active)         WS-SUP720-3B       SAL0934888E

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  1  0009.11e3.ade8 to 0009.11e3.adf7   5.1   6.3(1)       8.5(0.46)RFW Ok
  2  0018.ba41.5092 to 0018.ba41.5099   4.0   7.2(1)       3.2(2)10     Ok
  3  0014.a90c.9956 to 0014.a90c.995d   5.0   7.2(1)       5.1(6)E1     Ok
  4  0014.a90c.66e6 to 0014.a90c.66ed   1.7                4.2(3)       Ok
  5  0013.c42e.7fe0 to 0013.c42e.7fe3   4.4   8.1(3)       12.2(18)SXF1 Ok

[...]
```

正しいスロットを見つけた後、動作している次の例に示すようにソフトウェア バージョンを確認する **show module <slot 数 >** コマンドを発行して下さい:

```
switch>show module 2
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  2    6  Firewall Module                        WS-SVC-FWM-1       SAD10360485

Mod MAC addresses                       Hw    Fw           Sw           Status
```

```
--- -------------------------------- ------ ------------ ------------ -------
  2  0018.ba41.5092 to 0018.ba41.5099   4.0   7.2(1)       3.2(2)10     Ok

[...]
```

前述の例は FWSM が「Sw.」の下でカラムによって示されるようにソフトウェア バージョン 3.2(2)10 を実行していることを示します

注: Cisco IOSソフトウェア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** *数* **>** コマンドを実行することは必要ではないです。

1 およびスイッチ 2.を切り替えるために属する 2 つの物理的 な Cisco Catalyst 6500 シリーズ スイッチが単一論理的なバーチャル スイッチとして動作するように仮想 な 切り換えシステム（VSS）が使用される場合 **show module スイッチはすべての**コマンドすべての FWSMs のソフトウェア バージョンを表示することができます。 このコマンドからの出力は **show module <slot** *数*からの出力に類似した **>** ですが、ために VSS の各スイッチ モジュールのためのモジュール情報が含まれて下さい。

また、バージョン情報は次の例に示すように FWSM から show version コマンドによる直接、得ることができます:

```
FWSM> show version
FWSM Firewall Version 3.2(2)10
[...]
```

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。 バージョンの表記は次の例のようになります。

```
FWSM> show version
FWSM Firewall Version 3.2(2)10
[...]
```

脆弱性を含んでいないことが確認された製品

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスを除いて、その他のCisco製品は現在これらの脆弱性から影響を受けるために知られていません。

改訂履歴

リビジョン 1.0	2010-August-04	初回公開リリース

利用規約

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。