

Cisco Firewall サービス モジュールの多重 脆弱点

High	アドバイザーID : cisco-sa-20100804-fwsm	CVE-2010-2819
	初公開日 : 2010-08-04 16:00	CVE-2010-2818
	バージョン 1.0 : Final	CVE-2010-2821
	CVSSスコア : 7.8	CVE-2010-2820
	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

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 がある特定の 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ー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。

このアドバイザーは [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ーに説明がある SunRPC インспек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。アドバイザーは <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:

```
fwsм#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せん:

```
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

[...]

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

本アドバイザー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。本アドバイザー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、単独の転載や意識を施した場合、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。