ファイアウォール サービス モジュールの複数の脆弱性

severity

アドバイザリーID : cisco-sa-20070214-fwsm

初公開日 : 2007-02-14 16:00

バージョン 1.4 : Final

回避策 : No Workarounds available

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 Cisco Firewall Services Module（FWSM; ファイアウォール サービス モジュール）には、複数の脆弱性が存在します。これらの脆弱性は、特定の Hypertext Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）、セキュア HTTP（HTTPS）、Session Initiation Protocol（SIP; セッション開始プロトコル）、および Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラフィックの処理で発生します。デバッグ目的で詳細なロギングが有効になっている場合は、FWSM が自分宛のパケットを処理する際に脆弱性が存在します。これらすべての脆弱性では、デバイスがリロードされる可能性があります。

さらに、このアドバイザリでは、オブジェクト グループを使用する Access Control List（ACL; アクセス コントロール リスト）を操作する際に ACL が破壊され、望ましくないトラフィックが許可されて、望ましいトラフィックがブロックされるような状況になる可能性がある別の脆弱性についても説明しています。

これらの脆弱性は相互に独立したものです。1 つの脆弱性に該当するリリースが必ずしもその他の脆弱性に該当するとは限りません。

このアドバイザリで公開される脆弱性の一部には回避策があります。

Cisco では、該当するお客様用に、この問題に対応するソフトウェアを無償で提供しております。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070214-fwsm で公開されています。

該当製品

このドキュメントで説明されている脆弱性は、FWSM に該当します。このドキュメントに関連するアドバイザリ (https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070214-pix) では、Cisco 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 シリーズ適応型セキュリティ アプライアンスに該当する同様の脆弱性について説明されています。

脆弱性のある製品

次の表には、Cisco FWSM のどのソフトウェア リリースがどのような条件で該当するかが示されています。

脆弱性の名前	該当する条件	デフォルトで脆弱性があるか	該当するバージョン	Cisco Bug ID
1.不正なHTTPトラフィックの拡張検査によりリロードが発生する可能性	**inspect http *<appfw>* コマンドで、HTTP トラフィックの拡張検査が有効になっている**	No	3.1(3.24) より前のすべての 3.x ソフトウェア リリース	CSCsd75794
2.不正なSIPメッセージの検査によりリロードが発生する場合がある	**fixup protocol sip *<ポート番号>* コマンドや fixup protocol sip udp *<ポート番号>* コマンド (FWSM ソフトウェア 2.x 以前の場合) または inspect sip** コマンド (FWSM ソフトウェア 3.x 以降の場合) で、SIP 検査が有効になっている	Yes	2.3(4.12) より前のすべてのソフトウェア リリースおよび 3.1(3.24) より前のすべての 3.x リリース	CSCsg80915
3. FWSM宛ての	(ロギングの宛	No	3.1(3.	C

パケットの処理によりリロードが発生する場合がある	先にかかわらず）「デバッグ」レベルでロギングし、syslog メッセージ 710006 が有効になっている		3) より前のすべての 3.x ソフトウェアリリース	CSCse85707
4.不正なHTTPSトラフィックの処理によりリロードが発生する場合がある	**aaa authentication match** コマンドまたは **aaa authentication include** コマンドで、ネットワーク アクセス認証が有効になっている	No	3.1(3.18) より前のすべての 3.x ソフトウェアリリース	CSCsg50228
5.長いHTTP要求の処理によりリロードが発生する場合がある	**aaa authentication match** コマンドまたは **aaa authentication include** コマンドで、ネットワーク アクセス認証が有効になっている	No	3.1(2) より前のすべての 3.x リリース	CSCsd91268
6. HTTPSトラフィックを処理するとリロードが発生する場合がある	**http server enable** コマンドで、HTTPS サーバーが有効になっている	No	3.1(3.11) より前のすべての 3.x リリース	CSCsf29974
7.不正なSNMP要求の処理によりリロードが発生する可能性	**snmp-server host *<インターフェイス名> <SNMP サーバの IP アドレス>* コマンドにより、特定の IP アドレスからの SNMP トラフィックが許可されている**	No	3.1(3.1) より前のすべての 3.x リリース	CSCse52679
8. ACL の操作により ACL が破損する場合がある	ACL でオブジェクト グループが使用されており、管理者が ACL	No	2.3(4.7) より前のすべて	CSCs

	を操作している		のソフトウェア リリースおよび 3.1(3.1) より前のすべての 3.x リリース	e60868、CSCse99740、および CSCsd50667

次の表には、このアドバイザリで説明されている脆弱性と Cisco 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 シリーズ適応型セキュリティ アプライアンスにある同等の脆弱性との関係が説明されています。このドキュメントで説明されている脆弱性が表にない場合、Cisco 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 シリーズ適応型セキュリティ アプライアンスには、その脆弱性は*該当しません*。

脆弱性	**PIX/ASA Bug ID**	**FWSM Bug ID**
不正形式 HTTP トラフィックの拡張検査によりリロードが発生する場合がある	CSCsd75794	CSCsd75794
不正形式 SIP メッセージの検査によりリロードが発生する場合がある	CSCse27708 および CSCsd97077	CSCsg80915

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。

注：最近のバージョンのIOSでは、show moduleコマンドの出力に各モジュールのソフトウェアバージョンが表示されるため、**show module <slot number>**コマンドを実行する必要はありません。

別の方法として、**show version** コマンドで、FWSM から情報を直接取得することもできます。

```
FWSM#show version

FWSM Firewall Version 2.3(1)
```

PIX Device Manager（PDM）や Cisco Adaptive Security Device Manager（ASDM）で FWSM を管理しているお客様は、アプリケーションにログインすれば、ログイン ウィンドウの表か PDM や ASDM のウィンドウの左上に、次のようなラベルでバージョンが表示されます。

FWSMバージョン：2.3(1)

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。

詳細

Cisco ファイアウォール サービス モジュールは、Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の高速な統合型ファイアウォール モジュールです。このモジュールでは、ステートフル パケット フィルタリングとディープ パケット インスペクションを使用したファイアウォール サービスが提供されています。

特定のバージョンの FWSM ソフトウェアに複数の脆弱性が存在するため、デバイスで予期しないリロードが発生したり、適用中のセキュリティ ポリシーに反したトラフィックの許可や拒否が行われたりする可能性があります。

1.不正なHTTPトラフィックの拡張検査によりリロードが発生する可能性

この脆弱性により、FWSM が HTTP 要求の*拡張*検査を実行する際、および不正形式の HTTP 要求が FWSM で検査される際に、FWSM のリロードが発生する場合があります。FWSM で HTTP トラフィックの拡張検査が行われるのは、**inspect http <appfw>** コマンドが設定に含まれている場合だけです（*appfw* は特定の HTTP マップの名前です）。 このコマンドは、デフォルトで無効になっています。

注：HTTPトラフィックの拡張検査は、設定に影響を与えます。HTTP トラフィックの通常検査（HTTP マップを指定しない **inspect http** コマンドを使用）の設定では、この脆弱性には該当しません。

HTTP トラフィックの拡張検査の内容および設定方法についての詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/products_module_configuration_guide_chapter09186a0080577c72.html#wp1390330

この脆弱性は、Cisco Bug ID CSCsd75794(登録ユーザ専用)に記載されています。

2.不正なSIPメッセージの検査によりリロードが発生する場合がある

この脆弱性により、TCP 上の SIP の場合には **fixup protocol sip <ポート番号>** コマンド、UDP 上の SIP の場合には **fixup protocol sip udp <ポート番号>** コマンド（FWSM ソフトウェア 2.3.x 以前の場合）か *inspect sip* ***コマンド（FWSM ソフトウェア 3.x 以降の場合）で、SIP メッセージのディープ パケット インスペクションが有効になっていると、不正形式の SIP メッセージを（TCP か UDP 上で）受信した際に FWSM がリロードする場合があります。*** SIP fixup（2.x 以前の場合）および SIP inspection（3.x 以降の場合）は、デフォルトで有効になっています。

この脆弱性は、Cisco Bug ID CSCsg80915(登録ユーザ専用)に記載されています。

3. FWSM宛てのパケットの処理によりリロードが発生する場合がある

この脆弱性により、syslog メッセージ 710006 を生成しようとする際に、FWSM がリロードします。この問題が発生するのは、次の 2 つの条件が満たされた場合だけです。

- デバイスのいずれかの IP アドレス宛てのパケットが FWSM で受信されたが、メッセージが TCP、UDP、ICMP、OSPF、フェールオーバー、PIM、IGMP、ESP のいずれのプロトコルでもない。パケットの送信元にはかかわりません。
- syslogメッセージ710006を生成するのに十分なレベルでロギングを有効にする必要があります。デフォルトでは、デバッグレベル (レベル7) です。デフォルトでは、ロギングが無効になっていることに注意してください。デバッグとトラブルシューティングで必要な場合にだけ、デバッグ レベルでロギングすることを推奨いたします。
  注：Cisco Security Monitoring, Analysis and Response System(CS-MARS)のドキュメントでは、より多くのイベントをファイアウォールで報告できるように、デバッグレベルでのロギングを推奨しています。

syslog メッセージ 710006 についての詳細は、次のドキュメントを参照してください。

- Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータのファイアウォール サービス モジュール ロギング設定とシステム ログ メッセージ、3.1
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_system_message_guide_chapter09186a00804d74bd.html#wp1285757

この脆弱性は、Cisco Bug ID CSCse85707(登録ユーザ専用)に記載されています。

4.不正なHTTPS要求の処理によりリロードが発生する場合がある

この脆弱性により、ネットワーク アクセスをユーザに許可する前にユーザ認証を行うように、ネットワーク管理者がデバイスを設定している場合は、ユーザが Web サイトにアクセスしようとする際に、FWSM のリロードが発生する場合があります。この機能は、「ネットワーク アクセスの認証」つまり *auth-proxy* と呼ばれており、**aaa authentication match** コマンドや **aaa authentication include** コマンドで有効にされます。

実際には、無効な特定の HTTPS 要求により、このリロードが発生します。そのため、通常の Web ブラウザで発生する可能性は低いと考えられます。

この脆弱性は、Cisco Bug ID CSCsg50228(登録ユーザ専用)に記載されています。

5.長いHTTP要求の処理によりリロードが発生する場合がある

この脆弱性により、**aaa authentication match** コマンドや **aaa authentication include** コマンドでネットワーク アクセスの認証 (「auth-proxy」) をネットワーク管理者が有効にしている場合にも、FWSM のリロードが発生する可能性があります。ただし、この場合、要求される URL が非

常に長いという意味では通常の要求ではありませんが、リロードの原因となる HTTP 要求は有効です。Web ブラウザにより、通常の参照中にそのような要求が生成される可能性は潜在的にあります。

この脆弱性は、Cisco Bug ID CSCsd91268(登録ユーザ専用)に記載されています。

6. HTTPSトラフィックの処理によりリロードが発生する場合がある

この脆弱性により、FWSM 自身を宛先とする特定のタイプの HTTPS トラフィックが FWSM で受信された場合に、FWSM がリロードする場合があります。この問題が懸念されるのは、FWSM 上の HTTPS サーバが **http server enable** コマンドで有効になっている場合だけです。このコマンドは、デフォルトで無効になっています。

Cisco では、リロードを引き起こす HTTPS トラフィックを生成する可能性がある商用の脆弱性スキャナを確認しています。通常の Web ブラウザのトラフィックがこの不具合を引き起こす事例は報告されていません。

この脆弱性は、Cisco Bug ID CSCsf29974(登録ユーザ専用)に記載されています。

7.不正なSNMP要求の処理によりリロードが発生する可能性

この脆弱性により、信頼できるデバイスから不正形式の SNMP メッセージを受信すると FWSM がリロードする場合があります。この信頼できるデバイスは、**snmp-server host <インターフェイス名> <信頼できるデバイスの IP>** コマンドで明示的な SNMP ポーリング アクセスを許可されている必要があります。

この脆弱性は、Cisco Bug ID CSCse52679(登録ユーザ専用)に記載されています。

8. ACL の操作により ACL が破損する場合がある

この脆弱性により、ACL 内の Access Control Entry（ACE; アクセス コントロール エントリ）が、異常と評価されたり、評価が行われなかったりする可能性があります。トラフィックに明らかな影響が出る以外に、**show access-list** コマンドの出力と **show running-config** コマンドで対応する ACL を表示したときの内容が一致しない場合も、ACL が破損していることを示しています。デバイスを手動でリロードする以外に、この状態を修復する方法はありません。

オブジェクト グループを使用する ACL を操作すると ACL の破損が発生します。

この脆弱性は、Cisco Bug ID CSCse60868（登録ユーザ専用）、CSCse99740(登録ユーザ専用)、およびCSCsd50667(登録ユーザ専用)に記載されています。

回避策

Cisco 機器に適用可能な追加の軽減策については以下の "Cisco Applied Intelligence companion document" より入手可能です。

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070214-firewall

1.不正なHTTPトラフィックの拡張検査によりリロードが発生する可能性

HTTP トラフィックの拡張検査を無効にすれば、この脆弱性を緩和できます。HTTP の拡張検査を無効にすると、HTTP トラフィックに関連する可能性がある特定の攻撃や他の脅威を FWSM で防御できなくなることに注意してください。HTTP トラフィックの拡張検査は、**inspect http <appfw>** コマンドを設定から削除すれば無効になります。*appfw* は HTTP マップの名前です。

inspect http <appfw> コマンドおよびこのコマンドで HTTP トラフィックに対して行われる検査タイプについての詳細は、次の URL にあるこのコマンドのドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a008048e279.html#wp1570030

HTTP マップを指定しない **inspect http** コマンドは設定に残すことができます。残しても、この脆弱性の影響をデバイスが受けることはありません。

2.不正なSIPメッセージの検査によりリロードが発生する場合がある

SIP メッセージのディープ パケット インスペクション (3.x より前のソフトウェア バージョンの場合は「fixup」、3.x 以降の場合は「inspect」) を無効にすれば、この脆弱性を緩和できます。FWSMソフトウェア2.x以前では、TCPおよびUDPトランスポートを介したSIPメッセージのディープパケットインスペクションを停止するには、**no fixup protocol sip**と**no fixup protocol sip udp**の両方を使用する必要があります(FWSM 3.x以降では、**no inspect sip**はTCPとUDPの両方を介したSIPメッセージのディープパケットインスペクションを停止します)。 ただし、このようにすると、SIP トラフィックに対してステートフル アプリケーション インスペクションが実施されなくなるため、SIP セッションを終端するデバイスに悪影響が及ぶ可能性があり、このプロトコルのセッションを終端するデバイスに、デバイスのクラッシュや不正侵入を発生させる可能性があるパケットが到達する可能性があります。

FWSM ソフトウェア リリース 3.x が稼働している場合は、信頼できるホストだけからのトラフィックを許可するという代替策を利用できます。この方法を実施する場合の設定は次のとおりです。

```
access-list sip-acl extended permit udp 10.1.1.0 255.255.255.0 host 192.168.5.4 eq sip
access-list sip-acl extended permit udp host 192.168.5.4 10.1.1.0 255.255.255.0 eq sip

class-map sip-traffic
 match access-list sip-acl
```

```
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
 class sip-traffic
  inspect sip
!
service-policy global_policy global
```

この例では、10.1.1.0 ネットワーク内の任意のホスト（信頼できるネットワークの Inside）と IP アドレス 192.168.5.4 のホスト（信頼できるネットワークの Outside）が SIP エンドポイントになります。これらの IP アドレスは、実際のネットワークで使用されている IP アドレスに置き換える必要があります。

SIP は UDP ベースのプロトコルなので、SIP メッセージはスプーフィングされる可能性があることに注意してください。

3. FWSM宛てのパケットの処理によりリロードが発生する場合がある

この脆弱性が問題になるのは、syslog メッセージ 710006 が生成されるときだけなので、syslog メッセージ 710006 の生成をすべて無効にするか、このメッセージが生成される syslog レベルよりも低い syslog レベルでロギングすれば、問題を回避できます。

デフォルトでは、syslog メッセージ 710006 が生成されるのは syslog レベル 7（「デバッグ」）なので、レベル 6 以下でロギングすれば問題を回避できます。この方法は、**logging <宛先> 6** コマンドを使用すれば実行できます。syslog メッセージ 710006 が別のロギング レベルに変更されている場合は、必要に応じて使用するロギング レベルを変更して、メッセージが生成されないようにする必要があります。

「デバッグ」レベルでロギングする必要がある場合は、**no logging message 710006** コマンドを使用して、この syslog メッセージだけを無効にしてこの脆弱性を排除することもできます。

4.不正なHTTPS要求の処理によりリロードが発生する場合がある

この脆弱性に対する回避策はありません。

5.長いHTTP要求の処理によりリロードが発生する場合がある

この脆弱性に対する回避策はありません。

6. HTTPSトラフィックを処理するとリロードが発生する場合がある

この脆弱性は、特定のタイプの HTTPS トラフィックを正しく処理できない FWSM 上の HTTPS サーバで発生するので、この機能が不要な場合は、**no http server enable** コマンドで HTTPS サーバを無効にすれば問題を回避できます。この機能は ASDM で使用されているので、FWSM の設定が ASDM だけを使用して行われている場合、HTTPS サーバを無効するこの回避策を使用できない可能性があることに注意してください。

さらに、信頼できる IP アドレスやネットワークだけからの HTTPS 接続を許可して、問題が発生する可能性を下げることもできます。この方法は **http** コマンドを使用して実行できます。たとえば、次のコマンドを実行します。

```
FWSM(config)# http 192.168.1.10 255.255.255.255 inside
```

このようにすれば、IP アドレス 192.168.1.10 からの HTTPS 接続だけが許可されます。

7.不正なSNMP要求の処理によりリロードが発生する可能性

この不具合が発生するのは、FWSM 上で SNMP アクセスを許可されているデバイスから不正形式の SNMP メッセージを受信した場合だけです。SNMP が不要な場合は、**no snmp-server host <インターフェイス名> <信頼できるデバイスの IP アドレス>** コマンドを使用してこの機能を削除できます。そうすれば、この脆弱性を排除できます。

8. ACL の操作により ACL が破損する場合がある

この脆弱性に対する回避策はありません。ただし、デバイスの通常の動作時には ACL は破壊されず、特定のタイプのトラフィックを契機としてこの問題が発生する可能性もないことに注意してください。この問題が発生する可能性があるのは、管理者が設定を変更した場合（さらに具体的にいえば、管理者が ACL を操作した場合）だけです。 そのため、ACL の変更がメンテナンスの時間帯だけに行われており、変更後に FWSM がリロードされている場合には、この脆弱性を懸念する必要はありません。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance

Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

次の FWSM ソフトウェアの表の各行には、このドキュメントで説明されている脆弱性のいずれかが説明されています。修正を含む最初のリリース（「第 1 修正済みリリース」）とその提供予定日が「第 1 修正済みリリース」の列に、脆弱性ごとに示されています。特定の列のリリースより古い（「第 1 修正済みリリースより古い）リリースが稼働中のデバイスは、脆弱であることが確認されています。このようなリリースは、少なくとも、示されているリリース以上（最初の修正リリース ラベル以上）にアップグレードしてする必要があります。

脆弱性	**First Fixed Release（修正された最初のリリース）**
1.不正なHTTPトラフィックの拡張検査によりリロードが発生する可能性(CSCsd75794)	3.1(3.24)（2.3.x シリーズは該当せず）
2.不正なSIPメッセージの検査によりリロードが発生する場合がある(CSCsg80915)	2.3.x シリーズの場合は 2.3(4.12)、3.x シリーズの場合は 3.1(3.24)
3. FWSM宛てのパケット処理によりリロードが発生する場合がある(CSCse85707)	3.1(3.3)（2.3.x シリーズは該当せず）
4.不正なHTTPS要求の処理によりリロードが発生する場合がある(CSCsg50228)	3.1(3.18)（2.3.x シリーズは該当せず）
5.長いHTTP要求の処理によりリロードが発生する場合がある(CSCsd91268)	3.1(1.9)（2.3.x シリーズは該当せず）
6. HTTPSトラフィックの処理によりリロードが発生する場合がある(CSCsf29974)	3.1(3.11)（2.3.x シリーズは該当せず）
7.不正なSNMP要求の処理によりリロードが発生する場合がある(CSCse52679)	3.1(3.1)（2.3.x シリーズは該当せず）
8. ACLの操作によりACLが破損する(CSCse60868)、(CSCse99740)および(CSCsd50667)	2.3.x シリーズの場合は 2.3(4.7)、3.x シリーズの場合は 3.1(3.1)

2.3.x シリーズの場合、FWSM ソフトウェア バージョン 2.3(4.12) に、このドキュメントで説明したすべての脆弱性の修正が取り込まれています。

3.x シリーズの場合、FWSM ソフトウェア バージョン 3.1(4) に、このドキュメントで説明したすべての脆弱性の修正が取り込まれています。

FWSM ソフトウェアは、Cisco.com の次の場所からダウンロードできます。

http://www.cisco.com/pcgi-bin/tablebuild.pl/cat6000-fwsm?psrtdcat20e2

FWSM リリース 2.3(4.12) の場合は、次のリンクを使用してください。

http://www.cisco.com/pcgi-bin/tablebuild.pl/FWSMPSIRT?psrtdcat20e2

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

これらの脆弱性の一部に関しては、お客様の機器の通常運用中にこれらの問題が発生したことが Cisco に報告されています。それ以外の脆弱性は、社内テスト中に発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070214-fwsm

改訂履歴

リビジョン 1.4	2007 年 6 月 20 日	FWSM のリリース ノートとの整合性を保つために CSCsd50667（CSCse99740 の重複）に関する情報を追加。
リビジョン 1.3	2007 年 2 月 23 日	「不正形式 SIP メッセージの検査によりリロードが発生する場合がある」の脆弱性が TCP と UDP の両方で転送される SIP トラフィックに影響すること、使用するコマンドによっては設定が両方に影響する可能性があることに関する記述を明確化。SIP を無効にするという回避策で、両方のコマンドの削除が必要になる場合もあります。
リビジョン 1.2	2007 年 2	このドキュメントの以前のバージョンでは、FWSM 3.x ソフトウェアでは、SIP 検査がデフォルトで無効になっているという誤記がありました。アドバイザリを改定して、「不正形式 SIP メッセージの検査によりリロードが発生する場合がある」という脆弱性に 2.x と 3.x のソフトウェアの

	月21日	デフォルト設定が該当することを明記しました。
リビジョン1.1	2007年2月14日	CSCsd91268 の CVSS スコアを見直しました（リモート コード実行の可能性を反映するため）。CSCse60868 と CSCse99740 の CVSS スコアを見直しました（認証が必要であることを反映するため）。
リビジョン1.0	2007年2月14日	初回公開リリース

利用規約

本アドバイザリ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。 本アドバイザリ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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。