Cisco Firewall Services Module Cut-Through Proxy Denial of Service Vulnerability

Advisory ID: cisco-sa-20140219-fwsm

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140219-fwsm

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。

Revision 1.0

For Public Release 2014 February 19 16:00 UTC (GMT)

目次

要約
該当製品
詳細
脆弱性スコア詳細
影響
ソフトウェア バージョンおよび修正
回避策
修正済みソフトウェアの入手
不正利用事例と公式発表
この通知のステータス：FINAL
情報配信
更新履歴
シスコ セキュリティ手順

要約

Cisco Firewall Services Module（FWSM）ソフトウェアには脆弱性があり、認証されていないリモートの攻撃者によって該当システムのリロードが引き起こされる可能性があります。

この脆弱性は、カットスルー プロキシによって割り当てられたメモリを解放する際に競合状態が発生することに起因します。攻撃者は、カットスルー プロキシ認証をトリガーする条件に一致するようにトラフィックを送信することで、この脆弱性を不正利用する可能性があります。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。この脆弱性を軽減する回避策はありません。このアドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140219-fwsm

該当製品

Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の Cisco FWSM ソフトウェアは、この脆弱性の影響を受けます。影響を受けるリリースの詳細については、このア

ドバイザリの「ソフトウェア バージョンおよび修正」セクションを参照してください。

Cisco FWSM ソフトウェアは、ソフトウェア メンテナンス終了となっています。代替製品に関しては、シスコの担当者までお問い合わせください。

脆弱性が認められる製品

Cisco FWSM は、カットスルー プロキシ機能が有効になっている場合に、この脆弱性の影響を受けます。この機能は、 **match** コマンドまたは **include** コマンドを使用して、認証、許可、アカウンティングに対して有効にすることができます。この機能が使用中かどうかを判別するには、**show running-config aaa authentication| include match|include** コマンドを使用して、出力が返されるかどうかを確認します。外部 AAA サーバ、または AAA 用 Cisco FWSM ローカル ユーザ データベースを使用する設定に脆弱性が存在します。

次の例は、 *AuthOutbound* という名称の外部 AAA サーバを介してアクセス リスト *SERVER_AUTH* に一致しているトラフィックを認証するように構成されている Cisco FWSM を示しています。この例の設定は、 **match** コマンドで実装されます。

```
FWSM/admin# show running-config aaa authentication| include match|include
aaa authentication match SERVER_AUTH inside AuthOutbound
```

次の例は、**include** コマンドで実装される同様の設定を示しています。

```
FWSM/admin# show running-config aaa authentication| include match|include
aaa authentication include SERVER_AUTH inside AuthOutbound
```

Cisco FWSM ソフトウェアでは、カットスルー プロキシ機能はデフォルトでは有効になっていません。

実行中のソフトウェア バージョンの確認

デバイスで実行中の Cisco FWSM ソフトウェアのバージョンを確認するには、次の例に示すように **show version** コマンドを実行します。

```
FWSM> show version

FWSM Firewall Version 4.0(16)
[...]
```

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 Cisco 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 4.0(16)
[...]
```

バージョン情報は Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータから取得することもできます。デバイスで実行中の Cisco FWSM ソフトウェアのバージョンを確認するには、Cisco IOS ソフトウェアまたは Cisco Catalyst OS ソフトウェアから **show module** コマ

ンドを実行して、システム上にインストールされているモジュールおよびサブモジュールを表示します。

次の例は、スロット 2 に Cisco FWSM（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   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)       8.7(0.22)BUB Ok
  2  0018.ba41.5092 to 0018.ba41.5099   4.0   7.2(1)       4.0(16)      Ok
  3  0014.a90c.9956 to 0014.a90c.995d   5.0   7.2(1)       7.0(4)E4     Ok
  4  0014.a90c.66e6 to 0014.a90c.66ed   1.7   Unknown      Unknown
PwrDown
  5  0013.c42e.7fe0 to 0013.c42e.7fe3   4.4   8.1(3)       12.2(33)SXH8 Ok

[...]
```

正しいスロットの場所を確認した後、 **show module <** *slot number* **>** コマンドを実行して、実行中のソフトウェア バージョンを識別します。

```
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)       4.0(16)      Ok

[...]
```

上の例では、Cisco FWSM がバージョン 4.0(16) を実行していることが、Sw 列に示されています。

Virtual Switching System（VSS）は、2 台の物理的な Cisco Catalyst 6500 シリーズ スイッチを 1 台の論理的な仮想スイッチとして動作させるときに使用します。 **show module switch all** コマンドでスイッチ 1 およびスイッチ 2 に所属するすべての Cisco FWSM のソフトウェア バージョン

を表示できます。このコマンドの結果は **show module** *<slot number>* の結果に類似していますが、VSS の各スイッチ内のモジュールに関するモジュール情報が含まれています。

脆弱性が認められない製品

Cisco ASA ソフトウェアは、この脆弱性の影響を受けません。

この脆弱性の影響を受ける他のシスコ製品は、現在確認されていません。

詳細

Cisco FWSM 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。FWSM 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。

Cisco FWSM ソフトウェアは、AAA ネットワーク アクセス サービスのカットスルー プロキシ機能をサポートしています。

Cisco Firewall Services Module（FWSM）ソフトウェアのカットスルー プロキシ機能の脆弱性により、認証されていないリモートの攻撃者によって該当システムのリロードが引き起こされる可能性があります。

この脆弱性は、カットスルー プロキシによって割り当てられたメモリを解放する際に競合状態が発生することに起因します。攻撃者は、カットスルー プロキシ認証をトリガーする条件に一致するようにトラフィックを送信することで、この脆弱性を不正利用する可能性があります。この脆弱性を不正利用することにより、攻撃者は該当システムのリロードを引き起こすことができる場合があります。 不正利用が繰り返されることにより、Denial of Service（DoS）状態が発生します。

注：シングルおよびマルチ コンテキスト モードの両方で、ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードの両方に影響します。この脆弱性は、IP バージョン 4（IPv4）トラフィックによってのみ引き起こされます。通過トラフィックと FWSM デバイス宛てのトラフィックによって、引き起こされる可能性があります。外部 AAA サーバ、または AAA 用 Cisco FWSM ローカル ユーザ データベースを使用する設定に脆弱性が存在します。

この脆弱性は、Cisco Bug ID CSCuj16824（ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2014-0710 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCuj16824 - Cisco FWSM Cut-Through Proxy Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.1**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete
CVSS Temporal Score - **5.9**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性が不正利用されると、該当するデバイスがリロードされる可能性があります。不正利用が繰り返されることにより、Denial of Service（DoS）状態が発生します。

ソフトウェア バージョンおよび修正

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt/ の Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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デバイスに十分なメモリがあること、現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

次の表には、各メジャー リリース バージョンに関し、この脆弱性への修正が含まれたリリースの情報を記載します。

	3.1	3.2	4.0	
CSCuj16824 - Cisco FWSM Cut-Through Proxy Denial of Service Vulnerability[1]	Migrate to 3.2.x or later	3.2(28)	Migrate to 4.1 or later	4

[1] この脆弱性は、3.1(21)、3.2(21)、4.0(16)、4.1(6) よりも前の Cisco FWSM ソフトウェア リリースには影響しません。

注： Cisco FWSM ソフトウェアは、ソフトウェア メンテナンス終了となっています。代替製品に関しては、シスコの担当者までお問い合わせください。

回避策

カットスルー プロキシ機能を無効にする以外には、この脆弱性を軽減する回避策はありません。

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレードを入手することができます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（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とその公表は確認しておりません。

この脆弱性は、サポート ケースの解決中に発見されたものです。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140219-fwsm

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2014-February-19	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。