Multiple Vulnerabilities in Cisco Firewall Services Module

Advisory ID: cisco-sa-20121010-fwsm

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121010-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 2012 October 10 16:00 UTC (GMT)

内容

要約

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 Firewall Services Module（FWSM）には、次の脆弱性が存在します。

- DCERPC インスペクション バッファ オーバーフローの脆弱性
- DCERPC インスペクションの DoS 脆弱性

これらの脆弱性は相互依存していないため、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。

これらの脆弱性が悪用されると、認証されていないリモートの攻撃者によって該当デバイスの再起動が引き起こ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。

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。これら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-20121010-fwsm

注： Cisco Catalyst 6500 シリーズ ASA サービス モジュール、および Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスもこれらの脆弱性の影響を受ける可能性があります。

Cisco Catalyst 6500 シリーズ ASA サービス モジュールおよび Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに影響する脆弱性に関しては、別途 Cisco Security Advisory が公開されています。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-20121010-asa

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 には、複数の脆弱性が存在します。影響を受ける Cisco FWSM のバージョンは、脆弱性によって異なります。

脆弱性が存在する製品

影響を受けるバージョンの詳細については、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。

DCERPC インスペクション バッファ オーバーフローの脆弱性

Cisco FWSM は、DCERPC インスペクションが有効化されているときに脆弱性が存在します。デフォルトでは DCERPC インスペクションは有効になっていません。

DCERPC インスペクションの DoS 脆弱性

Cisco FWSM は、DCERPC インスペクションが有効化されているときに脆弱性が存在します。デフォルトでは DCERPC インスペクションは有効になっていません。

DCERPC インスペクションの有効/無効の確認

ご利用の FWSM 構成がこれらの脆弱性の影響を受けるかどうか確認するには、 **show service-policy | include dcerpc** コマンドを実行します。

次の例は、DCERPC インスペクションが有効になっている Cisco FWSM を示しています。

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

実行中のソフトウェア バージョンを知る方法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、管理者が **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ます。

脆弱性が存在しない製品

シスコ適応型セキュリティ アプライアンスおよび Cisco ASA サービス モジュールを除き、現在、他のシスコ製品においてこれらの脆弱性の影響を受けるものは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 は次のセクションで説明する複数の脆弱性の影響を受けます。**DCERPC インスペクション バッファ オーバーフローの脆弱性**

DCERPC は、Microsoft 社の分散クライアント/サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

DCERPC インスペクション エンジンのコードには、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再起動が引き起こされる、またはスタックがオーバーフローさせられ任意のコマンドが実行される可能性のある脆弱性が存在します。この脆弱性は、有効な DCERPC セッション内における DCERPC パケットに対する検証が不適切であることに起因します。攻撃者は、該当システムによってインスペクションが行われる巧妙に細工された DCERPC パケットを送信することで、この脆弱性を不正利用する可能性があります。

注：この脆弱性は、通過トラフィックによってのみ不正利用が可能で、 シングルおよびマルチコンテキスト モードの両方における、ルーテッドおよび透過的ファイアウォール モードの両方に影響します。また、IPv4 および IPv6 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。

この脆弱性は、Cisco Bug ID CSCtr27522（ 登録ユーザのみ ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-4661 が割り当てられています。

DCERPC インスペクションの DoS 脆弱性

DCERPC インスペクション エンジンには、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再起動が引き起こされる可能性のある 2 つの脆弱性が存在します。これらの脆弱性は、有効な DCERPC セッション内における DCERPC パケットに対する検証が不適切であることに起因します。攻撃者は、該当システムによってインスペクションが行われる巧妙に細工された DCERPC パケットを送信することで、この脆弱性を不正利用する可能性があります。

注：これらの脆弱性は、通過トラフィックによってのみ不正利用が可能で、 シングルおよびマルチコンテキスト モードの両方における、ルーテッドおよび透過的ファイアウォール モードの両方に影響します。また、IPv4 および IPv6 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。
これらの脆弱性は Cisco Bug ID CSCtr27524（登録ユーザのみ）および CSCtr27521（登録ユーザのみ）として文書化され、Common Vulnerability and Exposure（CVE）ID として CVE-2012-4662 および CVE-2012-4663 がそれぞれ割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ 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導き出すことができます。

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、シスコは個々の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/

CSCtr27522 - DCERPC Inspection Buffer Overflow Vulnerability Calculate the environmental score of					
CVSS Base Score - **9.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	Partial	Complete
CVSS Temporal Score - **7.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtr27524 - DCERPC Inspection 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	

CSCtr27521 - DCERPC Inspection 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

これらの脆弱性のいずれかが悪用されると、該当するデバイスが再起動する可能性があります。繰り返し悪用されると DoS 状態となる可能性があります。DCERPC インスペクション バッファ オーバーフローの脆弱性が悪用されると、 スタック オーバーフローが引き起こされ、任意のコマンドの実行が可能になることがあります。

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 and Responses アーカイブや、本アドバイザリ以降に公開のアドバイザリを参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

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、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。情報が不明確な場合は、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。

DCERPC インスペクション バッファ オーバーフローの脆弱性

Vulnerability	Major Release	First Fixed Release
DCERPC Inspection Buffer Overflow Vulnerability - CSCtr27522	3.1	Not Vulnerable
	3.2	Not Vulnerable
	4.0	Not Vulnerable
	4.1	4.1(9)

DCERPC インスペクションの DoS 脆弱性

Vulnerability	Major Release	First Fixed Release
DCERPC Inspection Denial Of Service Vulnerabilities - CSCtr27524 and CSCtr27521	3.1	Not Vulnerable

	3.2	Not Vulnerable
	4.0	Not Vulnerable
	4.1	4.1(7)

推奨リリース

次の表に、すべての推奨リリースを記載します。これらの推奨リリースには、このアドバイザリに記載のあるすべての脆弱性の修正が含まれています。シスコは「Recommended Releases」列のリリース、またはそれ以降のリリースにアップグレードすることを推奨します。

Major Release	Recommended Release
3.1	Not Vulnerable
3.2	Not Vulnerable
4.0	Not Vulnerable
4.1	4.1(9)

ソフトウェアのダウンロード

Cisco FWSM ソフトウェアは Cisco.com 内の Software Center からダウンロードできます。
http://www.cisco.com/cisco/software/navigator.html

Cisco Catalyst 6500 シリーズ ASA サービス モジュールについては、**[Products] > [Cisco Interfaces and Modules] > [Cisco Services Modules] >[Cisco Catalyst 6500 Series Firewall Services Module] > [ASA Services Module (FWSM) Software]** に移動してください。これらバージョンの一部は暫定バージョンのため、ダウンロード ページの *[Interim]* タブを開くことで見つけることができます。

回避策

管理者は、不要であれば DCERPC インスペクションを無効にすることでこれらの脆弱性を回避できます。

これらの脆弱性を軽減する他の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に特有の問題に関してご確認ください。

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、適切な処置について支援を受けてください。

回避策の効果は、使用製品、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のお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とする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か、お客様のサービス プロバイダーやサポート会社にご相談ください。

サービス契約をご利用でないお客様

シスコから直接購入したが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、サードパーティ ベンダーから購入したが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を入手してください。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの 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 を通して無償アップグレードをお求めください。

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を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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。

本セキュリティ アドバイザリで説明した脆弱性は、シスコ内部でのテストによって発見されました。

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。またシスコシステムズ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-20121010-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電子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

このアドバイザリに関する今後の更新があれば、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。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2012-October-10	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支援、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について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。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。