Cisco Security Advisory: Cisco Firewall Services Module Crafted Protocol Independent Multicast Message Denial of Service Vulnerability

Advisory ID: cisco-sa-20120314-fwsm

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-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 1.1

Last Updated 2012 March 19 16:05 UTC (GMT)

For Public Release 2012 March 14 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 Catalyst 6500 シリーズ Firewall Services Module（FWSM）には、Protocol Independent Multicast（PIM）の DoS 脆弱性があります。
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が存在する場合があります。このアドバイザリの「回避策」セクションを参照して下さい。。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-20120314-fwsm注：Cisco 適応型セキュリティ アプライアンス（ASA）と Cisco Catalyst 6500 ASA サービス モジュール（ASASM）も上記の脆弱性の影響を受けます。
ASA および ASASM に影響するこの脆弱性に関しては、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に掲載されます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asa

該当製品

Cisco Catalyst 6500 シリーズ Firewall Services Module（FWSM）は、次の脆弱性の影響を受けます。リリースされているすべてのバージョンの FWSM ソフトウェアが影響を受けるわけではありません。 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。

脆弱性が存在する製品

該当する具体的なバージョンについては、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。**PIM の DoS 脆弱性**Cisco FWSM ソフトウェアは、マルチキャスト ルーティングが有効化されている場合、PIM メッセージの処理中に該当するデバイスの再起動が引き起こされる可能性のある脆弱性があります。マルチキャスト ルーティングはデフォルトでは無効にされていますが、Cisco FWSM でマルチキャスト ルーティングを有効にした場合、自動的に PIM が有効となります。マルチキャスト ルーティングを有効にするには、次のコマンドを使用します。

```
fwsm(config)# multicast-routing
```

インターフェイスで PIM が有効にされているかを確認するには、 **show pim interface** コマンドを使用します。次の例は PIM が「inside」インターフェイスで有効にされている状態を示しています。

```
fwsm# sh pim interface

Address         Interface          PIM   Nbr    Hello   DR          DR
                                         Count  Intvl   Prior

172.16.1.66       inside             on    0      30      1           this
system
```

脆弱性が存在しない製品

Cisco ASA および Cisco Catalyst 6500 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

このセクションではこの脆弱性について詳細に説明します。

PIM の DoS 脆弱性マルチキャスト ルーティングは、単一の情報ストリームを同時に複数の受信者に送信することでトラフィックを減少させる帯域幅節約技術です。PIM は、どの IP ルーティング プロトコルからも独立した、マルチキャスト ルーティング プロトコルです。PIM はユニキャスト ルーティング テーブルを作成するために、Exterior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Border Gateway Protocol（BGP）、または静的なルートなど、どのユニキャスト ルーティング プロトコルを使用することもできます。PIM はこのユニキャスト ルーティング情報を使用してマルチキャスト転送機能を実行し、IP プロトコルには依存しません。PIM はマルチキャスト ルーティング プロトコルと呼ばれますが、実際は完全な非依存型のマルチキャスト ルーティング テーブルを構築するのではなく、ユニキャスト ルーティング テーブルを使用してリバース パス フォワーディング（RPF）チェック機能を

実行します。他のルーティング プロトコルではルータ間のマルチキャスト ルーティング更新の送受信を行いますが、PIM では行いません。脆弱性は PIM が実行される方法に存在し、マルチキャスト ルーティングが有効にされている場合、PIM メッセージの処理において該当するデバイスが再起動する可能性があります。この脆弱性は、PIM メッセージの不適切な処理に起因します。攻撃者は巧妙に細工された PIM メッセージを該当システムに送信することで、この脆弱性を不正利用できる可能性があります。
この脆弱性は、Cisco Bug ID CSCtu97367（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-2012-0356 が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

CSCtu97367 Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

PIM の DoS 脆弱性

この脆弱性の不正利用に成功した場合、リモートの認証されていない攻撃者によって該当するシステムの再起動が引き起こされることがあります。

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 アーカイブと、後続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。

PIM の DoS 脆弱性

Vulnerability	Major Release	First Fixed Release
Protocol Independent Multicast Denial of Service Vulnerability	2.2	Not Affected
	2.3	Not Affected
	3.1	Vulnerable: Migrate to 3.2
	3.2	3.2(23) Available late March 2012
	4.0	Vulnerable: Migrate to 4.1
	4.1	4.1(8)

回避策

PIM の DoS 脆弱性PIM を有効にすることが必要な場合は、この脆弱性を軽減する回避策はありません。しかし、マルチキャスト ルーティングは必要であっても、PIM をインターフェースで使用しない場合には、**no pim** インターフェース レベル コマンドを実行することで Cisco FWSM のインターフェースで PIM を無効にすることができます。

次の例は Cisco FWSM デバイス上で *outside* として定義された Vlan20 インターフェースで、PIM が無効になっている例です。

```
interface Vlan20
 nameif outside
 security-level 0
 ip address 192.168.1.1 255.255.255.0
 no pim
```

全てのインターフェースで PIM が無効になっていることを確認するには、**show pim interface** コマンドを実行し、全てのインターフェースで PIM スレートが *off* になっていることを確認します。次の例では Cisco FWSM の全てのインターフェースで PIM が無効になっています。

```
fwsm# show pim interface

Address         Interface          PIM   Nbr    Hello   DR
DR
                                         Count  Intvl   Prior

192.168.1.1     outside            off   0      30      1
not elected
172.16.1.66     inside             off   0      30      1
not elected
```

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。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 または http://www.cisco.com/public/sw-center/sw-usingswc.shtml 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。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

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 Center 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

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。

このセキュリティ アドバイザリで説明した脆弱性は、カスタマー 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-20120314-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 1.1	2012-March-19	"Workarounds" section: Added a workaround for when PIM is not in use
Revision 1.0	2012-March-14	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。