Cisco Security Advisory: Multiple Vulnerabilities in Cisco Firewall Services Module

Advisory ID: cisco-sa-20111005-fwsm

http://www.cisco.com/warp/public/707/cisco-sa-20111005-fwsm.shtml

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 2011 October 05 1600 UTC (GMT)

目次

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。

- Syslog メッセージ メモリ破壊に関する DoS 脆弱性
- 認証プロキシに関する DoS 脆弱性
- TACACS+ 認証バイパスに関する脆弱性
- Sun Remote Procedure Call（SunRPC）インスペクションに関する DoS 脆弱性
- Internet Locator Server（ILS）インスペクションに関する 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。

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。

このアドバイザリは次のリンクに掲載されます。 http://www.cisco.com/warp/public/707/cisco-sa-20111005-fwsm.shtml

注：Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスおよび Cisco Catalyst 6500 シリーズ ASA サービス モジュールは、このアドバイザリに記載されている一部の脆弱性の影響を受けます。Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスおよび Cisco Catalyst 6500 シリーズ ASA サービス モジュールに影響を与えるこれらおよびその他の脆弱性については、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ています。 http://www.cisco.com/warp/public/707/cisco-sa-20111005-asa.shtml

該当製品

脆弱性が存在する製品

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 ソフトウェアのバージョンは、脆弱性によって異なります。脆弱性のあるバージョンに関する具体的な情報については、「ソフトウェア バージョンと修正」セクションを参照してください。

Syslog メッセージ メモリ破壊に関する DoS 脆弱性

脆弱性のあるバージョンの Cisco FWSM ソフトウェアを実行しているデバイスは、次の条件が満たされると、この脆弱性の影響を受けます。

- デバイスに IPv6 アドレスに対するインターフェイスがある
- システム ロギングが有効になっている（コマンド **logging enable**）
- デバイスが任意の方法でシステム ログ メッセージ 302015 を生成するように構成されている（次の例を参照）

システム ログ メッセージ 302015 はデフォルトの重大度レベルが 6（informational）になっているため、システム管理者がこのデフォルトの重大度レベルを変更していないと仮定した場合、デバイスが**任意の**宛先にレベル 6 またはレベル 7（デバッグ）でロギングすると、この脆弱性が引き起こされます。一例として、次に脆弱な構成を示します。

```
logging enable
!
logging console informational
logging buffered informational
[...]
```

重大度別で、またはこのメッセージ ID を明示的に含めることによる、システム ログ メッセージ 302015 を含むカスタム メッセージ リストの使用（**logging list** コマンド経由）も脆弱な構成です。例えば、次の構成も脆弱性が存在します。

```
logging enable
!
```

```
logging list MYLIST level informational
<and/or>
logging list MYLIST message 302015
!
logging trap MYLIST
```

注：システム ログ メッセージのデフォルトの重大度レベルは変更可能です。システム ログ メッセージ 302015 のデフォルトの重大度レベルが変更されており、変更後の重大度レベルで任意の宛先にログを行うようにデバイスが構成されている場合も、デバイスはやはり脆弱性が存在します。

認証プロキシに関する DoS 脆弱性

脆弱性のあるバージョンの Cisco FWSM ソフトウェアを実行しているデバイスは、ネットワーク アクセスにカットスルー プロキシまたは認証プロキシとしても知られる、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を使用するように構成されている場合、この脆弱性の影響を受けます。該当するデバイスの構成に **aaa authentication match** コマンドまたは **aaa authentication include** コマンドが存在する場合、ネットワーク アクセス認証機能が有効になっています。

TACACS+ 認証バイパスに関する脆弱性

脆弱性のあるバージョンの Cisco FWSM ソフトウェアを実行しているデバイスは、AAA に Terminal Access Controller Access-Control System Plus（TACACS+）を使用するように構成されている場合、この脆弱性の影響を受けます。AAA サーバ グループが次に類似した方法で定義されている場合、デバイスは TACACS+ 向けに構成されています。

```
aaa-server my-tacacs-server protocol tacacs+
aaa-server my-tacacs-server (inside) host 192.168.1.1
  [...]
```

注：上の例では、「my-tacacs-server」が AAA サーバ グループの名前です。

SunRPC インスペクションに関する DoS 脆弱性

脆弱性のあるバージョンの Cisco FWSM ソフトウェアを実行しているデバイスは、SunRPC インスペクションが有効にされていると、これらの脆弱性の影響を受けます。SunRPC インスペクションはデフォルトで有効にされています。

SunRPC インスペクションが有効にされているかを確認するには、 **show service-policy | include sunrpc** コマンドを使用して結果が返るかどうかを確認します。結果の例を次に示します。

```
FWSM# show service-policy | include sunrpc
      Inspect: sunrpc, packet 324, drop 5, reset-drop 0
```

または、SunRPC インスペクションが有効になっているデバイスは、次に類似した構成を有します（**inspect sunrpc** コマンドは実際に SunRPC インスペクションを有効にするコマンドです。ただし Cisco FWSM で実際にトラフィックを検査するにはほかのコマンドが必要です）。

```
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
```

```
  ...
  inspect sunrpc
!
service-policy global_policy global
```

注：サービス ポリシーは特定のインターフェイスに適用されることもあります。(上の例ではグローバル適用が示されています。)

ILS インスペクションに関する DoS 脆弱性

脆弱性のあるバージョンの Cisco FWSM ソフトウェアを実行しているデバイスは、ILS プロトコルのインスペクションが有効にされていると、これらの脆弱性の影響を受けます。デフォルトでは ILS インスペクションは有効になっていません。

ILS インスペクションが有効にされているかを確認する方法は、「SunRPC インスペクションに関する DoS 脆弱性」を参照してください。構成キーワード「sunrpc」の代わりに「ils」を使用します。

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、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。

注意：Cisco IOS ソフトウェアの最近のバージョンでは、**show module** コマンドから各モジュールのソフトウェア バージョンを確認できます。 よって、**show module <slot number>** コマンドを実行する必要はありません。

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。

または次の例のように、**show version** コマンドを使用して Cisco FWSM からバージョン情報を直接取得することもできます。

```
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)
[...]
```

脆弱性が存在しない製品

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアン・Xおよび Cisco Catalyst 6500 シリーズ 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。

Syslog メッセージ メモリ破壊に関する DoS 脆弱性

Cisco FWSM は、通常運用のモニタリングおよびネットワークまたはデバイスの問題のトラブルシューティングに関する情報を提供するシステム ログ（syslog）機能を備えています。システム ログ メッセージには異なる重大度（デバッグ、情報、エラー、重大など）が割り当てられており、異なるロギング先に送信することができます。

DoS 脆弱性が特定のシステム ログ メッセージ（メッセージ ID 302015、「Built outbound UDP connection session-id for src-intf:IP/Port to dst-intf:IP/Port ARP-Incomplete」）の実装に存在し、デバイスを通過する IPv6 トラフィックについてそのシステム ログ メッセージが生成される必要がある場合、メモリ破壊を引き起こして、Cisco FWSM のロックアップまたはクラッシュにつながることがあります。Cisco FWSM が自動で回復できず、手動による再起動が必要な場合があります。

システム ログ メッセージ 302015 はデフォルトの重大度レベルが 6（informational）です。このシステム メッセージのデフォルトの重大度レベルを変更しても、システムが変更後の重大度レベルで任意の宛先にロギングする場合、この問題を回避することはできません。Cisco FWSM に IPv6 アドレスに対するインターフェイスがないと、この問題は発生しません。

この脆弱性は Cisco Bug ID CSCti83875（登録ユーザのみ）として文書化され、CVE ID CVE-2011-3296 が割り当てられています。

認証プロキシに関する DoS 脆弱性

Cisco FWSM 認証プロキシ機能は、ネットワーク リソースへのアクセス制御に AAA の使用を許可します。特に、Cisco FWSM カットスルー プロキシは最初にアプリケーション レイヤでユーザに情報を入力させ、AAA サーバに対して認証を行います。Cisco FWSM がユーザを認証すると、セッション フローが変わり、すべてのトラフィックはユーザの コンピュータとアクセスされるネットワーク リソース間で直接送受信されます。

Cisco FWSM ソフトウェアの一部バージョンには DoS 脆弱性が存在し、カットスルーまたは認証プロキシとしても知られる、ネットワークへのアクセスをユーザに付与する認証を使用するように構成されているデバイスに影響を与えます。**aaa authentication match** または **aaa authentication include** コマンドを含む構成が脆弱な構成です。多数のネットワーク アクセス認証要求がある際に、この脆弱性が引き起こされることがあります。

この脆弱性は Cisco Bug ID CSCtn15697（登録ユーザのみ）として文書化され、CVE ID CVE-2011-3297 が割り当てられています。

TACACS+ 認証バイパスに関する脆弱性

AAA は、ユーザが誰であるか（認証）、ユーザが何をできるか（認可）、そしてユーザが何をしたか（アカウンティング）を Cisco FWSM が確認することを可能にします。Cisco FWSM は VPN ユーザ、ファイアウォール セッション、デバイスへの管理者権限でのアクセスに対する TACACS+ 認証をサポートします。

Cisco FWSM には TACACS+ 実装における認証バイパスの脆弱性が存在します。不正利用に成功した場合、リモートの攻撃者は VPN ユーザ（Cisco FWSM は管理に VPN セッションのみを許可する）、ファイアウォール セッション、またはデバイスへの管理者権限でのアクセスの TACACS+ 認証をバイパスすることができます。

この脆弱性は Cisco Bug ID CSCto74274（登録ユーザのみ）として文書化され、CVE ID CVE-2011-3298 が割り当てられています。

SunRPC インスペクションに関する DoS 脆弱性

SunRPC インスペクション エンジンは SunRPC プロトコルに対するアプリケーション インスペクションを有効または無効にします。SunRPC は Network File System（NFS）および Network Information Service（NIS）によって使用されます。SunRPC サービスは任意のポートで実行可能です。サーバの SunRPC サービスにクライアントがアクセスを試みるとき、サービスが実行されているポートを知る必要があります。クライアントは well-known ポート 111 でポート マッパー プロセス（通常 rpcbind）をクエリーすることにより、これを実行します。

Cisco FWSM は、SunRPC インスペクションが有効化されている場合、巧妙に細工された異なる SunRPC メッセージを処理しているときにデバイスの再起動を引き起こす 4 つの脆弱性があります。これらの脆弱性は通過トラフィックによってのみ引き起こされます。デバイス宛てのトラフィックはこれらの脆弱性を引き起こしません。

これらの脆弱性は Cisco Bug ID CSCtq09972（登録ユーザのみ）、CSCtq09978（登録ユーザのみ）、CSCtq09986（登録ユーザのみ）、CSCtq09989（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-2011-3299、CVE-2011-3300、CVE-2011-3301 および CVE-2011-3302 がそれぞれ割り当てられています。

ILS インスペクションに関する DoS 脆弱性

ILS インスペクション エンジンは、Microsoft NetMeeting、SiteServer、および Lightweight Directory Access Protocol（LDAP）を使用して ILS サーバとディレクトリ情報を交換する Active Directory 製品に Network Address Translation（NAT）サポートを提供します。

Cisco FWSM は、ILS インスペクションが有効化されている場合、不正な ILS メッセージを処理しているときにデバイスの再起動を引き起こす可能性がある脆弱性の影響を受けます。この脆弱性は通過トラフィックによってのみ引き起こされます。デバイス宛てのトラフィックはこの脆弱性を引き起こしません。

この脆弱性は Cisco Bug ID CSCtq57802（登録ユーザのみ）として文書化され、CVE ID CVE-2011-3303 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、個々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 URL にて CVSS に関する FAQ 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 URL にて提供しています。

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

-- Syslog message 302015 may lead to memory corruption and CP lockup **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	

-- FWSM crash in thread name uauth **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	

-- Crafted TACACS+ reply considered as successful auth by FWSM **Calculate the environmental score of**					
CVSS Base Score - **7.9**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Adjacent Network	Medium	None	Complete	Complete	Complete
CVSS Temporal Score - **6.5**					
Exploitability		Remediation Level		Report	

		Confidence
Functional	Official-Fix	Confirmed

SunRPC Inspection Denial of Service Vulnerabilities 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	

-- ILS inspection crash on malformed ILS traffic 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

任意の DoS 脆弱性が悪用されると、該当するデバイスが再起動する可能性があります。繰り返し不正利用されると、サービス拒否（DoS）状態が続く可能性があります。

TACACS+ 認証バイパスの脆弱性が悪用されると、攻撃者が VPN、ファイアウォール、および（または）管理者権限でのセッションの認証をバイパスできる可能性があります。

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際には、 http://www.cisco.com/go/psirt/ および本アドバイザリ以降に公開のアドバイザリも参照して、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。

次の Cisco FWSM ソフトウェア テーブルの各行には、主要な Cisco FWSM ソフトウェア トレインが示されており、そのトレインの修正を含む最初のリリース（「First Fixed Release」）とその提供予定日（現時点で未提供の場合）が「First Fixed Release」列に示されています。特定の列のリリースより古い（「First Fixed Release」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。脆弱なリリースは少なくとも示されたリリース以降のバージョン（「First Fixed Release」以降）へアップグレードすることが推奨されます。

Major Release	First Fixed Release
3.1	3.1(21)
3.2	3.2(22)
4.0	4.0(16)
4.1	4.1(7)

修正済みの Cisco FWSM ソフトウェアは、Cisco.com 内の Software Center（ http://www.cisco.com/cisco/software/navigator.html ）にアクセスして、[Products] > [Security] > [Firewall] > [Firewall Integrated Switch/Router Services] > [Cisco Catalyst 6500 Series Firewall Services Module] > [Firewall Services Module (FWSM) Software] に移動することでダウンロードできます。

回避策

このシスコ セキュリティ アドバイザリでは、相互に独立した複数の脆弱性が説明されています。これらの脆弱性およびそれぞれ対応策は互いから独立しています。

Syslog メッセージ メモリ破壊に関する DoS 脆弱性

この脆弱性に対しては、コマンド **no logging message 302015** で syslog 302015 を完全に無効にすることが有効な回避策です。

認証プロキシに関する DoS 脆弱性

この脆弱性に対する回避策はありません。

TACACS+ 認証バイパスに関する脆弱性

RADIUS や LDAP など別の認証プロトコルを使用する以外、この脆弱性に対する回避策はありま

せん。

SunRPC インスペクションに関する DoS 脆弱性

管理者は、不要であれば SunRPC 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。管理者はポリシーマップ設定内において、クラス設定サブモードで **no inspect sunrpc** コマンドを発行することによって SunRPC インスペクションを無効にすることができます。SunRPC インスペクションを無効にすると、SunRPC トラフィックがセキュリティ アプライアンスで止められる可能性があります。

ILS インスペクションに関する DoS 脆弱性

管理者は、不要であれば ILS インスペクションを無効にすることで脆弱性を回避できます。管理者はポリシーマップ設定内において、クラス設定サブモードで **no inspect ils** コマンドを発行することによって ILS インスペクションを無効にすることができます。ILS インスペクションを無効にすると、ILS トラフィックがセキュリティ アプライアンスで止められる可能性があります。

修正済みソフトウェアの入手

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。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 ライセンスの条項または、Cisco.com Downloads の http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他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、シスコのワールドワイド Web サイト上の 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、本脆弱性に関する適切な処置について指示と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。TAC の連絡先は次のとおりです。

- +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、このお知らせの 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に対する無償アップグレードは、TAC 経由でご要求いただく必要があります。

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、 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 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。

Syslog メッセージ メモリ破壊に関する DoS 脆弱性、認証プロキシに関する DoS 脆弱性、TACACS+ 認証バイパスに関する脆弱性はお客様のサービス リクエストのトラブルシューティング中に発見されました。

SunRPC インスペクションに関する DoS 脆弱性および ILS インスペクションに関する DoS 脆弱性は、シスコの社内テストで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

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。

http://www.cisco.com/warp/public/707/cisco-sa-20111005-fwsm.shtml

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- 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
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。 しかしながら、前述のメーリング リストもしくはニュースグループに対し 積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報を ご確認いただくことをお勧めいたします。

更新履歴

Revision 1.0	2011-October-05	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、シスコ ワールドワイド Web サイトの
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスして

ください。このページには、シスコのセキュリティ通知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。