Cisco Security Advisory: Multiple Vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances and Cisco Catalyst 6500 Series ASA Services Module

Advisory ID: cisco-sa-20111005-asa

http://www.cisco.com/warp/public/707/cisco-sa-20111005-asa.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 1.1

Last Updated 2011 October 05 2145 UTC (GMT)

For Public Release 2011 October 05 1600 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 ASA 5500 シリーズ適応型セキュリティ アプライアンスと Cisco Catalyst 6500 シリーズ ASA サービス モジュールには次のような複数の脆弱性があります。

- MSN インスタント メッセンジャー（IM）インスペクションに関する DoS 脆弱性
- TACACS+ 認証バイパスに関する脆弱性

- SunRPC インスペクションに関する DoS 脆弱性 4 件
- Internet Locator Service（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。

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、http://www.cisco.com/warp/public/707/cisco-sa-20111005-asa.shtml で公開されています。

注：Cisco Firewall Services Module（FWSM; ファイアウォール サービス モジュール）は TACACS+ 認証バイパスの脆弱性、SunRPC インスペクションに関する DoS 脆弱性、ILS インスペクションに関する DoS 脆弱性の影響を受けます。FWSM に影響するこの脆弱性に関して別途 Cisco Security Advisory が公開されています。このアドバイザリは、http://www.cisco.com/warp/public/707/cisco-sa-20110831-fwsm.shtml で公開されています。

該当製品

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスと Cisco Catalyst 6500 シリーズ ASA サービス モジュールには複数の脆弱性があります。影響を受ける Cisco ASA 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。

MSN IM インスペクションに関する DoS 脆弱性

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの MSM IM インスペクション機能は、DoS 脆弱性の影響を受けます。

デフォルトでは MSN IM インスペクションは有効になっていません。

管理者は MSN IM インスペクションを有効にすることで、メッセージがパラメータに違反したときのアクションを指定し、IM インスペクション ポリシー マップを作成することができます。その後、次の例に示すとおり、IM インスペクションを有効にするとインスペクション ポリシー マップを適用できます。

```
policy-map type inspect im MY-MSN-INSPECT
 parameters
 match protocol msn-im
  log
!
policy-map global_policy
  class inspection_default
    inspect im MY-MSN-INSPECT
```

TACACS+ 認証バイパスに関する脆弱性

認証バイパスの脆弱性は、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの TACACS+ の実装に影響を与えます。

TACACS+ を有効にして認証、認可、またはアカウンティング（AAA）を実施するには、まず AAA プロトコルごとに AAA サーバ グループを少なくとも 1 つ作成してから、**aaa-server** コマンドで 1 台以上のサーバを各グループに追加する必要があります。AAA サーバ グループは名前で識別します。次の例に AAA サーバ グループで TACACS+ 認証を設定する方法について示します。

```
aaa-server my-tacacs-sever protocol tacacs+
aaa-server my-tacacs-server (inside) host 203.0.113.11
```

SunRPC インスペクションに関する DoS 脆弱性

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの SunRPC インスペクション機能には、4 件の DoS 脆弱性があります。

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かどうかを確認するには、**show service-policy | include sunrpc** コマンドを発行して出力結果を確認します。次の例のような結果が返されます。

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

Cisco ASA で SunRPC インスペクションを有効にするために次の設定コマンドが使用されています。

```
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  ...
  inspect sunrpc
  ...
!
service-policy global_policy global
```

ILS インスペクションに関する DoS 脆弱性

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの ILS インスペクション機能には、DoS 脆弱性があります。

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かどうかを確認するには、**show service-policy | include ils** コマンドを発行して出力結果を確認します。次の例のような結果が返されます。

```
ciscoasa# show service-policy | include ils
      Inspect: ils, packet 0, drop 0, reset-drop 0
```

Cisco ASA で ILS インスペクションを有効にするために次の設定コマンドが使用されています。

```
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  ...
  inspect ils
  ...
!
service-policy global_policy global
```

実行中のソフトウェア バージョンを知る方法

脆弱性のあるバージョンの Cisco ASA ソフトウェアがアプライアンスで実行されているかどうかを知るには、**show version** コマンドを発行します。次の例は、ソフトウェア バージョン 8.4(1) を実行している Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスを示しています。

```
ASA#show version | include Version
Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)
```

Cisco 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。

脆弱性が存在しない製品

Cisco FWSM を除いて、これらの脆弱性の影響を受けるシスコ製品は現在確認されていません。

詳細

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスと Cisco Catalyst 6500 シリーズ ASA サービス モジュールには次に示す脆弱性があります。

MSN IM インスペクションに関する DoS 脆弱性

IM インスペクション エンジンは IM アプリケーションにきめ細かい制御を適用し、ネットワークの使用を制御して機密データの漏えいやワームの拡散、企業ネットワークにおけるその他の脅威を防止します。

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの MSN IM インスペクション機能には、DoS 脆弱性があります。悪用が成功すると、認証されていない攻撃者によって該当するデバイスが再起動される可能性があります。その結果、長時間にわたって DoS 状態が続く可能性があります。

注：この脆弱性は通過トラフィックによってのみ引き起こされます。アプライアン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。デフォルトでは MSN IM インスペクションは有効になっていません。

この脆弱性は Cisco Bug ID CSCtl67486（ 登録ユーザのみ ）として文書化され、CVE ID CVE-2011-3304 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 を有効にすると、ASA はユーザが誰か（認証）、ユーザは何ができるか（認可）、ユーザが何をしたか（アカウンティング）を特定できるようになります。Cisco ASA では、VPN ユーザ、ファイアウォール セッション、デバイスへの管理アクセスに対する TACACS+ 認証をサポートします。

Cisco ASA の TACACS+ 実装には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、攻撃者はリモートから VPN ユーザ、ファイアウォール セッション、またはデバイスへの管理アクセスに対する TACACS+ 認証をバイパスできる可能性があります。攻撃者がこの攻撃を不正利用するには、ASA と TACACS+ サーバ間のネットワークにアクセスできる必要があります。

この脆弱性は Cisco Bug ID CSCto40365（ 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

Sun RPC インスペクション エンジンは Sun RPC 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実行します。Sun RPC は Network File System（NFS）および Network Information Service（NIS）によって使用されます。Sun RPC サービスは任意のポートで実行可能です。サーバの Sun RPC 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 ASA 5500 シリーズ適応型セキュリティ アプライアンスの SunRPC インスペクション機能には 4 件の DoS 脆弱性があり、認証されていない攻撃者によって該当するデバイスが再起動され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引き起こされます。アプライアン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。これらの脆弱性は TCP パケットではなく、UDP パケットを使用して引き起こされることがあります。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。

これらの脆弱性は Cisco Bug ID CSCto92380（ 登録ユーザのみ ）、CSCtq06065（ 登録ユーザのみ ）、CSCtq06062（ 登録ユーザのみ ）、CSCto92398（ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2011-3299、CVE-2011-3300、CVE-2011-3301、CVE-2010-3302 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 LDAP を使用する Microsoft NetMeeting、SiteServer、Active Directory 製品で NAT サポートを提供します。これにより、これら製品は ILS サーバとディレクトリ情報を交換することができます。

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの ILS インスペクション機能には、DoS 脆弱性があります。悪用が成功すると、認証されていない攻撃者によって該当するデバイスが再起動される可能性があります。その結果、長時間にわたって DoS 状態が続く可能性があります。

注：この脆弱性は通過トラフィックによってのみ引き起こされます。アプライアン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。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。

この脆弱性は Cisco Bug ID CSCtq57697（ 登録ユーザのみ ）として文書化され、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 計算ツールを以下の URL にて提供しています。

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

CSCtl67486 - MSN IM Inspection Denial of Service Vulnerability **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	
CSCto40365 - TACACS+ Authentication Bypass Vulnerability **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	

CSCto92380, CSCtq06065, CSCtq06062, CSCto92398 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	

CSCtq57697 - 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

これらすべての 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。この脆弱性が繰り返し悪用されると、継続的な DoS 状態となる可能性があります。

TACACS+ 認証バイパスに関する脆弱性の不正利用が成功した場合、攻撃者は VPN、ファイアウォール、および管理セッション、またはいずれか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

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。

Vulnerability	Major Release	First Fixed Release
MSN Instant Messeger (IM) Inspection Denial of Service Vulnerability (CSCtl67486)	7.0	Not vulnerable
	7.1	Not vulnerable
	7.2	7.2(5.3)
	8.0	8.0(5.25)
	8.1	8.1(2.50)
	8.2	8.2(5.11)
	8.3	8.3(2.23)
	8.4	8.4(2)
	8.5	8.5(1.1)
TACACS+ Authentication Bypass Vulnerability (CSCto40365)	7.0	7.0(8.13)
	7.1	Vulnerable; migrate to 7.2(5.4) or later
	7.2	7.2(5.3)
	8.0	8.0(5.24)
	8.1	8.1(2.50)
	8.2	8.2(5)
	8.3	8.3(2.18)
	8.4	8.4(1.10)
	8.5	8.5(1.1)
SunRPC Inspection Denial of	7.0	7.0(8.13)

Service Vulnerabilities (CSCto92380, CSCtq06065, CSCtq06062, CSCto92398)	7.1	Vulnerable; migrate to 7.2(5.4) or later
	7.2	7.2(5.4)
	8.0	8.0(5.25)
	8.1	Vulnerable; migrate to 8.2 or later
	8.2	8.2(5.11)
	8.3	8.3(2.23)
	8.4	8.4(2.6)
	8.5	8.5(1.1)
ILS Inspection Denial of Service Vulnerability (CSCtq57697.)	7.0	7.0(8.13)
	7.1	Vulnerable; migrate to 7.2(5.4) or later
	7.2	7.2(5.4)
	8.0	8.0(5.25)
	8.1	8.1(2.50)
	8.2	8.2(5.6)
	8.3	8.3(2.23)
	8.4	8.4(2.7)
	8.5	8.5(1.1)

推奨リリース

推奨リリースについては、以下のテーブルをご参照下さい。これらの推奨リリースには、このアドバイザリで説明されている脆弱性に対する修正を含んでいます。シスコはこれらの推奨リリース、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
7.0	7.0(8.13)
7.1	Vulnerable; migrate to 7.2(5.4) or later
7.2	7.2(5.4)
8.0	8.0(5.25)
8.1	Vulnerable; migrate to 8.2 or later
8.2	8.2(5.13)
8.3	8.3(2.25)
8.4	8.4(2.8)
8.5	8.5(1.1)

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。

MSN インスタント メッセンジャー（IM）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 MSN IM 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 im** コマンドを発行することによって MSN IM インスペクションを無効にすることができます。MSN IM インスペクションを無効にすると、MSN IM 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。

TACACS+ 認証バイパスに関する脆弱性

RADIUS、Active Directory など別の認証プロトコルを使用する以外に、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。お客様はソフトウェア 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利用することにより、
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 に記載されている Cisco のソフトウェ

ア ライセンス条件に同意したものと見なされます。

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。大半のお客様は、http://www.cisco.com にある Cisco の Web サイトの Software Center からアップグレードを入手できます。

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。

すべての DoS 脆弱性は、社内テストで発見されたものです。

TACACS+ 認証の脆弱性は、お客様のサービス リクエストへの対応中に発見されました。

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

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-asa.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 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 1.1	2011-October-05	Updated recommended release table.
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。