Cisco ASA 5500 Series Adaptive Security Appliances and Cisco Catalyst 6500 Series ASA Services Module Denial of Service Vulnerability

Advisory ID: cisco-sa-20120620-asaipv6

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-asaipv6

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 April 20 16:00 UTC (GMT)

目次

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（Cisco ASA）と Cisco Catalyst 6500 シリーズ ASA サービス モジュール（Cisco ASASM）には、リモートの認証されていない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のある脆弱性が存在します。

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。これらの脆弱性に対しては回避策があります。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-20120620-asaipv6

該当製品

Cisco ASA および Cisco ASASM がこの脆弱性の影響を受けます。ただし、Cisco ASA ソフトウェアの全バージョンがこの脆弱性の影響を受けるわけではありません。該当するバージョンの詳細については、このセキュリティ 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。

Cisco ASA と Cisco ASASM には、リモートの認証されていない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のある脆弱性が存在します。

Cisco ASA ソフトウェアは、次のすべての条件が存在する場合、この脆弱性の影響を受ける可能性があります。

- Cisco ASA または Cisco ASASM がトランスペアレント ファイアウォール モードで動作している
- Cisco ASA または Cisco ASASM で IPv6 が有効である
- Cisco ASA または Cisco ASASM でシステム ロギングが有効にされており、かつシステムがメッセージ ID 110003 のログを行うように構成されている

Cisco ASA または Cisco ASASM がトランスペアレント ファイアウォール モードで動作しているかを確認するには、**show firewall** コマンドを実行します。次の例は、トランスペアレント ファイアウォール モードで動作している Cisco ASA を示しています。

```
ciscoasa# show firewall
Firewall mode: Transparent
```

IPv6 はデフォルトで有効にされていません。トランスペアレント ファイアウォール モードで構成されている Cisco ASA または Cisco ASASM で IPv6 を有効にするには、少なくとも IPv6 が正しく動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスが設定されている場合、リンクローカル アドレスは自動的に各インターフェイスで設定されます。

Cisco ASA または Cisco ASASM で IPv6 が有効にされているかを確認するには、 **show ipv6 interface** コマンドを実行し、コマンドが出力結果を返すか確認します。次の例は、トランスペアレント ファイアウォール モードで動作しており、IPv6 が有効である、2 つのインターフェイス（inside および outside）で構成された Cisco ASA を示しています。

```
ciscoasa# show ipv6 interface
outside is up, line protocol is up
 IPv6 is enabled, link-local address is fe80::219:2fff:fe83:4f42
 No global unicast address is configured
 Joined group address(es):
   ff02::1
   ff02::1:ff83:4f42
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds
 ND advertised retransmit interval is 1000 milliseconds
 Hosts use stateless autoconfig for addresses.
inside is up, line protocol is up
 IPv6 is enabled, link-local address is fe80::219:2fff:fe83:4f43
 No global unicast address is configured
 Joined group address(es):
   ff02::1
   ff02::1:ff83:4f43
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ND DAD is enabled, number of DAD attempts: 1
```

```
      ND reachable time is 30000 milliseconds
      ND advertised retransmit interval is 1000 milliseconds
      Hosts use stateless autoconfig for addresses.
```

Syslog メッセージ ID 110003 は、Cisco ASA がインターフェイス ルーティング テーブルでネクストホップを見つけられないときに生成されます。この Syslog メッセージの詳細については、『Cisco ASA システム ログ メッセージ』ガイドを参照してください。
http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html
Cisco ASA ではロギングはデフォルトでは有効になっていません。ただし、ロギングが有効にされると自動的に Syslog メッセージ 110003 が有効になります。

Syslog メッセージ 110003 のデフォルトの重大度レベルは 6（informational）です。レベル 6 以上（レベル 6 ～ 7）でロギングが設定されている Cisco ASA ソフトウェアは脆弱性が存在する可能性があります。
ロギングが有効にされているか確認するには、**show logging** コマンドを使用します。次の例は、ロギングが有効であり、バッファ ロギングがレベル 6（informational）で有効にされている Cisco ASA を示しています。

```
    ciscoasa#
```

show logging

```
Syslog logging: enabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Debug-trace logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 2 messages logged
Trap logging: disabled
Permit-hostdown logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

Syslog メッセージ 110003 を含む（重大度別、またはこのメッセージ ID を明示的に含めることのいずれかによる）カスタム メッセージ リスト（**logging list** コマンド経由で作成）の使用も脆弱な構成です。

Syslog 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。Syslog メッセージ 110003 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口グを行うようにデバイスが構成されている場合も、デバイスにはやはり脆弱性が存在します。

実行中のソフトウェア バージョンの確認

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。

```
    ciscoasa#

show version | include Version
```

```
Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)
```

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 ウィンドウの表内、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。

Cisco PIX セキュリティ アプライアンスに関する情報

Cisco PIX は、このセキュリティ アドバイザリに記載されている脆弱性の影響は受けません。 Cisco PIX セキュリティ アプライアンスはメンテナンス終了となっています。Cisco PIX をご利用のお客様は、Cisco ASA に移行することを推奨します。

脆弱性が存在しない製品

他のシスコ製品において、この脆弱性の影響を受けるもの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 (Cisco ASA) と Cisco Catalyst 6500 シリーズ ASA サービス モジュール (Cisco ASASM) には、リモートの認証されていない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のある脆弱性が存在します。

注：この脆弱性は IPv6 通過トラフィックによってのみ引き起こされる可能性があり、トランスペアレント ファイアウォール モード (シングルまたはマルチコンテキスト モードに関わらず) で構成された Cisco ASA および Cisco ASASM の両方に影響します。

この脆弱性は、Cisco Bug ID CSCua27134（ 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-2012-3058 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/

CSCua27134 - Cisco ASA IPv6 Packets 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	

影響

この脆弱性の不正利用に成功した場合、影響を受けたデバイスでは再起動が発生することがあります。繰り返し悪用されると DoS 状態が継続す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。

Vulnerability	Major Release	First Fixed Release
Cisco ASA IPv6 Packets Denial Of Service Vulnerability	7.0	Not Affected
	7.1	Not Affected
	7.2	Not Affected
	8.0	Not Affected
	8.1	Not Affected
	8.2	Not Affected
	8.3	Not Affected
	8.4[1]	8.4(4.1)
	8.5	8.5(1.11); Available July 2012
	8.6	8.6 (1.3); Available July 2012

[1]この脆弱性は 8.4(2) で発生しました。8.4(2) より前のバージョンはこの脆弱性の影響を受けません。

回避策

有効な回避策は、Cisco ASA が Syslog メッセージ 110003 を生成しないようにすることです。Syslog メッセージ 110003 を無効にするには、**no logging message 110003** コマンドを使用します。

メッセージが生成されないことを確認するには、**show running-configuration logging** コマンドします。メッセージ 110003 の口ギングが無効にされた場合のコマンドの出力例を次に示します。

```
ciscoasa# show run logging
[...]
no logging message 110003
[...]
```

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。

この脆弱性は、サービス リクエスト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-20120620-asaipv6

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-June-20	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。