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のDoS脆弱性

アドバイザリーID : cisco-sa-20120620-asaipv6
初公開日 : 2012-06-20 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCua27134

CVE-2012-3058

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。

概要

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)およびCisco Catalyst 6500シリーズASAサービスモジュール(Cisco ASASM)には脆弱性があり、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リロードが引き起こされる可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。こ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、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-asaipv6

該当製品

Cisco ASAおよびCisco ASASMはこの脆弱性の影響を受けます。Cisco ASAソフトウェアのすべての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。影響を受け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。

脆弱性のある製品

具体的なバージョン情報については、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およびCisco ASASMには脆弱性があり、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リロードが引き起こされる可能性があります。

Cisco ASAソフトウェアは、次の条件がすべて満たされると、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実行されている
- Cisco ASAまたはCisco ASASMでIPv6が有効になっている
- Cisco ASAまたはCisco ASASMでシステムロギングが有効になっており、システムがメッセージID 110003を記録するように設定されている

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実行されていることを確認するには、show firewallコマンドを発行します。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。

<#root>

```
ciscoasa# show firewall
Firewall mode:

Transparent
```

IPv6 は、デフォルトでは有効化されていません。 トランスペアレントファイアウォールモードに設定されたCisco ASAまたはCisco ASASMでIPv6を少なくとも有効にするには、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 アドレスを設定すると、リンクローカル アドレスは各インターフェイスで自動的に設定されます。

Cisco ASAまたはCisco ASASMでIPv6が有効になっていることを確認するには、show ipv6 interfaceコマンドを発行して、出力が返されることを確認します。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、IPv6が有効になっている2つのインターフェイス (内部と外部) で設定されたCisco ASAを示しています。

<#root>

```
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場合に生成されます。このsyslogメッセージの詳細については、http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.htmlにある『Cisco ASA System Log Messages』ガイドを参照してください。Cisco ASAではデフォルトでロギングは有効になっていませんが、ロギングが有効にされると、syslogメッセージ110003が自動的に有効になります。

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）のロギングが設定されているCisco ASAソフトウェアには脆弱性が存在する可能性があります。
ロギングが有効になっているかどうかを確認するには、show loggingコマンドを発行します。次の例は、ロギングが有効で、バッファロギングがレベル6（情報）で有効になっているCisco ASAを示しています。

<#root>

```
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を含むカスタムメッセージリスト(logging listコマンドを使用して作成)を、重大度ごとまたはメッセージIDを明示的に含めることも、脆弱な設定です。

syslogメッセージのデフォルトの重大度レベルは変更できます。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、新しい重大度レベルで任意の宛先にログを記録するようにデバイスが設定されている場合、そのデバイスには脆弱性が存在します。

実行ソフトウェア バージョンの判別

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。

<#root>

```
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またはCisco ASDMウィンドウの左上隅に表示される表でソフトウェアバージョンを確認できます。

Cisco PIXセキュリティアプライアンスについての情報

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を受けません。Cisco PIXはメンテナンスサポートが終了しています。Cisco PIXをご使用のお客様には、Cisco ASAへの移行をお勧めします。

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリ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)およびCisco Catalyst 6500シリーズASAサービスモジュール(Cisco ASASM)には脆弱性があり、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リロードが引き起こされる可能性があります。

注： この脆弱性は、IPv6中継トラフィックによってのみトリガーされ、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）に設定されている場合はCisco ASAとCisco ASASMの両方に影響します。

この脆弱性は、Cisco Bug ID CSCua27134(登録ユーザ専用)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。

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ていないことを確認するには、show running-configuration loggingコマンドを発行します。次の例は、メッセージ110003のロギングが無効になっているときのコマンドの出力を示しています。

```
<#root>

ciscoasa#

show run logging


[...]
no logging message 110003
[...]
```

修正済みソフトウェア

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 アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性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。](http://www.cisco.com/go/psirt)

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規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、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。

脆弱性	メジャー リリース	First Fixed Release（修正された最初のリリース）
Cisco ASA IPv6パケットに関するDoS脆弱性	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
	8.41	8.4（4.1）
	8.5	8.5(1.11)（2012年7月に提供開始）
	8.6	8.6(1.3)（2012年7月提供開

		始)

[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

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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やその公表を確認していません。

この脆弱性は、サービスリクエストの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-asaipv6

改訂履歴

リビジョン 1.0	2012年6月20日	初版リリース

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。