Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの多重 脆弱点

High

アドバイザリーID : cisco-sa-20100804-asa

初公開日 : 2010-08-04 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : Yes

Cisco バグ ID :

CVE-2010-1581
CVE-2010-2817
CVE-2010-1580
CVE-2010-2816
CVE-2010-2815
CVE-2010-2814
CVE-2010-1578
CVE-2010-1579

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 アプライアンスは多重 脆弱点から次の通り影響を受けます:

- 3 SunRPC インスペクション サービス拒否の脆弱性
- 3 Transport Layer Security（TLS）サービス拒否の脆弱性
- セッション開始プロトコル（SIP）インスペクション サービス拒否の脆弱性

- 巧妙に細工された インターネット キー エクスチェンジ（IKE） メッセージ サービス拒否の脆弱性

これらの脆弱性は相互依存ではないです; リリースは他から 1 脆弱性から影響を受ける必ずしも影響を受けしません。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100804-asa で掲示されます。

注: Cisco Firewall サービス モジュール（FWSM）は SunRPC DoS 脆弱性から影響を受けます。別途の Cisco Security Advisory は FWSM に影響を与える脆弱性を表わすために公開されました。 このアドバイザリは 804-fwsm で利用できます。

該当製品

修正済みソフトウェア

特定のバージョン情報に関しては、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下さい。

SunRPC インスペクション サービス拒否の脆弱性

3 サービス拒否 （DoS）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 SunRPC インスペクション 機能に影響を与えます。 不正侵入の成功は支えられた DoS 状態という結果に終るかもしれません。

バージョン 7.2.x、8.0.x、8.1.x および 8.2.x は影響を受けています。 SunRPC インスペクションはデフォルトで有効に なります。

SunRPC インスペクションが有効に なるかどうか確認するために、**show service ポリシーを**発行して下さい | 表示するものがのような次の例で **sunrpc** コマンドを**含み、**出力される、戻されることを確認して下さい。

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

次の設定コマンドが Cisco ASA の SunRPC インスペクションを有効に するのに使用されています。

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

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

Transport Layer Security（TLS）サービス拒否の脆弱性

3 DoS 脆弱性は一連の巧妙に細工された TLS パケットによって引き起こすことができる Cisco ASA セキュリティ アプライアンス モデルにあります。 不正侵入の成功は支えられた DoS 状態という結果に終るかもしれません。 バージョン 7.2.x、8.0.x、8.1.x、8.2.x および 8.3.x はこれらの脆弱性の何れか一つ以上から影響を受けます。 次の機能の何れかのために設定される Cisco ASA デバイスは影響を受けています:

- セキュア ソケット レイヤ（SSL）仮想 な プライベート ネットワーク（SSL VPN）
- Cisco Adaptive Security Device Manager（ASDM）接続を許可するために影響を受けたデバイスが設定される時
- 暗号化された音声検査の TLS プロキシ
- HTTPS を使用する場合のネットワーク アクセスのためのカットスルー プロキシ

SSL VPN（か WebVPN）は **webvpn** コンフィギュレーションモードの**イネーブル <interface** *名前* **>** コマンドで有効に なります。 SSL VPN はデフォルトでディセーブルにされます。 次のコンフィギュレーション の 断片は SSL VPN 設定の例を提供します。

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

ASDM アクセスはこれらの脆弱性の 3 から影響を受けます。 ASDM を使用するために、HTTPS サーバは Cisco ASA への HTTPS 接続を許可するために有効に する必要があります。 サーバは **HTTPサーバ イネーブル[ポート]**コマンドを使用して有効に することができます。 デフォルト ポートは 443 です。 セキュリティ アプライアンス モデルに内部 HTTPサーバにアクセスできるホストを規定 するためにグローバル コンフィギュレーション モードで **http** コマンドを使用して下さい。

暗号化された音声 インスペクション 機能のための TLS プロキシはこれらの脆弱性から影響を受けます。 この機能は Cisco ASA バージョン 8.0(2)で導入され、デフォルトでディセーブルにされます。

暗号化された音声 インスペクション 機能のための TLS プロキシがデバイスで有効に なったかどうか確認するために、次の例に示すように**提示 TLS プロキシ** コマンドを、使用して下さい:

```
ciscoasa# show tls-proxy
Maximum number of sessions: 1200

TLS-Proxy 'sip_proxy': ref_cnt 1, seq# 3
Server proxy:
```

```
Trust-point: local_ccm
Client proxy:
Local dynamic certificate issuer: LOCAL-CA-SERVER
Local dynamic certificate key-pair: phone_common
Cipher suite:  aes128-sha1 aes256-sha1
Run-time proxies:
    Proxy 0xcbae1538: Class-map: sip_ssl, Inspect: sip
Active sess 1, most sess 3, byte 3456043
...
<output truncated>
```

TLS プロキシ サポート SIP およびスキニー プロトコル。 スキニー インスペクション用の TLS プロキシは次の例に示すように **Inspect スキニー <skinny_map > TLS プロキシ <proxy_name** を使用して **>**、有効に することができます:

```
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# inspect skinny my-inspect tls-proxy my-tls-proxy
asa(config)# service-policy global_policy global
```

注: セキュア SCCP は TCPポート 2443 を使用します; ただし、それは異なるポートに設定することができます。

SIP インスペクション用の TLS プロキシは次の例に示すように **Inspect 一ロ <map > TLS プロキシ <proxy_name** を使用して **>**、有効に することができます:

```
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# inspect sip my-inspect tls-proxy my-tls-proxy
asa(config)# service-policy global_policy global
```

ネットワーク アクセス 機能のためのカットスルー プロキシが HTTPS と使用されるとき Cisco ASA はまた脆弱です。 この機能は **https が**命じる **AAA認証リスナー**との HTTPS を使用して直接認証のために次の例に示すように、有効に なります:

```
ASA(config)# aaa authentication listener https inside port 443
```

セッション開始プロトコル（SIP）インスペクション サービス拒否の脆弱性

DoS 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 SIP インスペクション 機能に影響を与えます。 バージョン 7.0.x は、7.1.x、7.2.x 影響を受けていません。 バージョン 8.0.x、8.1.x および 8.2.x は影響を受けています。 SIP インスペクションはデフォルトで有効に なります。

SIP インスペクションが有効に なるかどうか確認するために、**show service ポリシーを**発行して下さい **|** 表示するものがのような次の例で**一ロ**コマンドを**含み**、出力される、戻されることを確認して下さい。

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

また、有効に なる SIP インスペクションがあるアプライアンスに次と同じような設定があります:

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

```
 class inspection_default
  ...
  inspect sip
  ...
!
service-policy global_policy global
```

注: サービス ポリシーはまた前例で示されているグローバルコンフィギュレーションの代りに特定のインターフェイスに適用できます。

巧妙に細工された インターネット キー エクスチェンジ（IKE） メッセージ サービス拒否の脆弱性

Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス（ASA）ソフトウェア バージョン 7.0.x、7.1.x、7.2.x、8.0.x、8.1.x、8.2.x および 8.3.x は影響を受けています。 IKE はデフォルトで有効に なりません。 IKE が有効に なる場合、**isakmp enable <interface** *名前* **>** コマンドは設定に現われます。

Cisco PIX 500 シリーズ セキュリティ アプライアンス モデル脆弱性ステータス

Cisco PIX 500 シリーズ セキュリティ アプライアンスは SunRPC、TLS および IKE メッセージ DoS 脆弱性から影響を受けます。

Cisco PIX 500 シリーズ セキュリティ アプライアンスがソフトウェアメンテナンスリリースの端に 2009 年 7月 28 日達したので、それ以上のソフトウェア リリースは Cisco PIX 500 シリーズ セキュリティ アプライアンスに利用できません。 Cisco PIX 500 シリーズ セキュリティ アプライアンス 顧客は Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに移行するか、またはこのアドバイザリの回避策 セクションにリストされている適当な回避策を設定するように勧められます。 修正済みソフトウェアは Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに利用できます。 詳細については、 http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5709/ps2030/end_of_life_notice_cisco_pix_525_sec_app.html でライフ発表の終わりを参照して下さい。

実行ソフトウェア バージョンの判別方法

Cisco ASA ソフトウェアの脆弱なバージョンがアプライアンスで動作しているかどうか判別するために、管理者は **show version コマンドを**発行できます。 ソフトウェア バージョン 8.3(1) を実行している次の例は Cisco ASA 5500 シリーズを適応型セキュリティ アプライアンス（ASA）ソフトウェア示したものです:

```
ASA#show version | include Version
Cisco Adaptive Security Appliance Software Version 8.3(1)
Device Manager Version 6.3(1)
```

Cisco ASDM をデバイスを管理するのに使用する顧客は Cisco ASDM ウィンドウの Login ウィンドウか左上のコーナーで表示する 表でソフトウェア バージョンを見つけることができます。

脆弱性を含んでいないことが確認された製品

Cisco FWSM を除いて、その他のCisco製品は現在これらの脆弱性から影響を受けるために知られていません。

改訂履歴

リビジョン 1.0	2010-August-04	初回公開リリース

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。