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-20110223-asa **初公開日 :** 2011-02-23 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-2011-0394 CVE-2011-0395 CVE-2011-0393 CVE-2011-0396

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 アプライアンスは次の脆弱性から影響を受けます:

- 透過ファイアウォール パケット バッファ枯渇脆弱性
- Skinny Client Control Protocol （ SCCP ） インスペクション サービス拒否の脆弱性
- ルーティング情報プロトコル (RIP ） サービス拒否の脆弱性
- 不正 な ファイル システム アクセスの脆弱性

これらの脆弱性は独立 して います; 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。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110223-asa で掲示されます。

注: Cisco Firewall サービス モジュール (FWSM) はこれらの脆弱性の 1 から影響を受けます。別途の Cisco Security Advisory は Cisco 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。 そのアドバイザリは 223-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。

透過ファイアウォール パケット バッファ枯渇脆弱性

パケット バッファ枯渇脆弱性はセキュリティ アプライアンス モデルが透過ファイアウォール モードで動作するために設定されるとき Cisco ASA ソフトウェアの複数のバージョンに影響を与えます。 透過ファイアウォール モードはアプライアンスでコマンド **ファイアウォール 透過的なが**設定にある場合有効に なります。 デフォルト ファイアウォール モードは、透過的**ルーティングされます。 提示ファイアウォール** コマンドもファイアウォール オペレーションモードを判別するのに使用することができます:

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

SCCP インスペクション サービス拒否の脆弱性

サービス拒否の脆弱性は Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの SCCP インスペクション 機能に影響を与えます。

管理者は SCCP インスペクションが **show service ポリシーのことを**発行によって有効に なったかどうか確認できます **| スキニー** コマンドを**含めば**表示するもののがのような次の例でその出力を確認することは、戻ります。

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

また、有効に なる SCCP インスペクションがあるデバイ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 skinny ... ! service-policy
global_policy global
```

注: サービス ポリシーはまたグローバルにの代りに前例で表示する特定のインターフェイスに適用できます。

SCCP インスペクションはデフォルトで有効に なります。

RIP サービス拒否の脆弱性

サービス拒否の脆弱性は RIP および Cisco Phone プロキシ 機能が両方同じデバイスで有効になるとき Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの RIP 実装に影響を与えます。 次の例は影響を受けた設定 (Cisco ASA ソフトウェア バージョン 8.0 をおよび 8.1) 表示したものです:

```
router rip
 ...
! phone-proxy <instance name> media-termination address <IP address> ... <Rest of phone proxy
feature configuration>
```

または（Cisco ASA ソフトウェア バージョン 8.2 およびそれ以降）:

```
router rip
 ...
! media-termination <instance name> address <IP address> ! <Rest of phone proxy feature
configuration>
```

セキュリティ アプライアンス モデルは RIP メッセージ（**router rip**）を処理する場合脆弱ですおよびグローバル な メディアの停止 アドレスが Cisco Phone プロキシ 機能のために（設定されれば前例を参照して下さい）。 Cisco ASA ソフトウェア バージョン 8.0 および 8.1 がグローバル な メディアの停止 アドレスしか可能にしないことに注目して下さい。 ただし、Cisco ASA ソフトウェア バージョン 8.2 およびそれ以降で、インターフェイスにメディアの停止 アドレスを接続することは可能性のあるです。 この設定はメディアの停止 コンフィギュレーションモードの**指令アドレス < IP アドレス > インターフェイス <interface name> の**発行によって達成される影響を受けていません。

RIP も Cisco Phone プロキシ 機能もデフォルトで有効に なりません。

不正 な ファイル システム アクセスの脆弱性

不正 な ファイル システム アクセスの脆弱性はセキュリティ アプライアンス モデルがローカル認証局（CA）で設定されるとき Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに影響を与えます。 影響を受けた設定は次の最小コマンドで構成されています:

```
crypto ca trustpoint <trustpoint name>
 keypair <keypair name>
 crl configure
crypto ca server
crypto ca certificate chain <trustpoint name>
 certificate ca 01
  ...
 ! http server enable
```

ローカル CA サーバはデフォルトで有効に なりません。

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 アプライアンスは透過ファイアウォール パケット バッファ枯渇脆弱性および SCCP インスペクション サービス拒否の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マイルストーンの端に 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 モデル 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 アプライアンスだけに利

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。

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 Adaptive Security Device Manager（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 PIX 500 シリーズ セキュリティ アプライアンスおよび Cisco Firewall サービス モジュールを除いて、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	2011-February-23	初回公開リリース

利用規約