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-20100217-asa
初公開日 : 2010-02-17 16:00
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : Yes
Cisco バグ ID :

CVE-2010-0151
CVE-2010-0150
CVE-2010-0568
CVE-2010-0569
CVE-2010-0566
CVE-2010-0149
CVE-2010-0567
CVE-2010-0565

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:

- TCP 接続枯渇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
- Skinny Client Control Protocol（SCCP）インスペクション サービス拒否の脆弱性
- WebVPN データグラム の 転送 層 セキュリティ（DTLS）サービス拒否の脆弱性

- 巧妙に細工された TCP セグメント 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
- NT LAN Manager バージョン 1（NTLMv1）認証 バイパス 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。

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-20100217-asa で掲示されます。

該当製品

修正済みソフトウェア

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 脆弱点から影響を受けます。 Cisco ASA ソフトウェアの影響を受けたバージョンは特定の脆弱性によって変わります。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。

TCP 接続枯渇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 アプライアンスは TCP 接続の終了フェーズの間に特定の TCP セグメントの受け取りを通して引き起こすことができる TCP 接続枯渇状態を経験するかもしれません（新しい TCP 接続は許可されません）。 次の機能の何れかのために設定されるときバージョン 7.1.x を実行しているアプライアンス、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:

- SSL VPN
- Cisco Adaptive Security Device Manager（ASDM）管理アクセス
- Telnet 経由のアクセス
- SSH アクセス
- 仮想 Telnet
- バーチャルHTTP
- 暗号化された音声 インスペクション用の Transport Layer Security（TLS）プロキシ

SIP インスペクション サービス拒否の脆弱性

2 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 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、7.1.x、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。 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 **| ーロコマンドを含み、**出力が戻ることを確認して下さい。 出力例は次の例で表示する:

```
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:

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

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。 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。 SCCP インスペクションはデフォルトで有効に なります。

SCCP 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 **| スキニー** コマンドを**含み、**出力が戻ることを確認して下さい。 出力例は次の例で表示する:

```
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アプライアンスに次と同じような設定があります:

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

WebVPN DTLS 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 アプライアンスは存在 します サービス拒否の脆弱性から WebVPN および DTLS が有効に なるとき影響を受けま。 影響を受けたバージョンは 7.1.x、7.2.x、8.0.x、8.1.x および 8.2.x が含まれています。 管理者は「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 WebVPN を有効に することができます。 DTLS は「グループ ポリシー webvpn」コンフィギュレーションモードの **SVC dtls enable コマンドの**発行によって有効に することができます。 次のコンフィギュレーション の 断片は DTLS を有効に する WebVPN 設定の例を提供します:

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

WebVPN がデフォルトでディセーブルにされるが、DTLS は最近のソフトウェアリリースでデフォルトで有効に なります。

巧妙に細工された TCP セグメント 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 アプライアンスは不正 な TCP セグメントによって引き起こすことができるサービス拒否の脆弱性から影響を受けますアプライアンスを通過する。 この脆弱性はコンフィギュレーションだけに影響を与えます**静的な**文の終わりで*ネイルドされた*オプションを使用する。 さらに、トラフィックはまたインライン モードの Cisco AIP-SSM （**静的な**文と一致する侵入防御システム（IPS） モジュール）によって検査する必要があります。 IPS インライン オペレーションモードは**インラインに IPS の**使用によって有効に なります**{故障する終わり |**「クラス」コンフィギュレーションモードの故障する**開いた}**コマンド。 Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス ソフトウェア バージョン 7.0.x を実行している、7.1.x、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。

巧妙に細工された IKE メッセージ サービス拒否の脆弱性

Cisco ASA 5500 シリーズの終端により適応型セキュリティ アプライアンス（ASA）ソフトウェア 中断 されるべき同じデバイスで終えるすべての IPSecトンネルを引き起こす可能性があること IPSecトンネルを通して送信 される 巧妙に細工された IKE メッセージ。 バージョン 7.0.x、7.1.x、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。 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。

NTLMv1 認証 バイパス の 脆弱性

認証 バイパス の 脆弱性は NTLMv1 認証が設定されるとき 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。 バージョン 7.0.x、7.1.x、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。 管理者は **aaa-server <AAA** *サーバグループ タグ* **> プロトコル nt** コマンドおよび認証がその AAA サーバ グループを使用するように要求するサービスを設定することと NTLMv1 プロトコルを使用する認証、許可、アカウンティング（AAA） サーバグループの定義によって NTLMv1 認証を設定できます。 NTLMv1 認証が有効に され、アクティブであることを確認するために、**提示 aaa-server プロトコル nt** コマンドを発行して下さい。 出力例は次の例で表示する:

```
ciscoasa#show aaa-server protocol nt
Server Group:    test
Server Protocol: nt
Server Address:  192.168.10.11
Server port:     139
Server status:   ACTIVE, Last transaction (success) at 11:10:08 UTC  Fri Jan 29
<output truncated>
```

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 アプライアンスは次の脆弱性から影響を受けます:

- TCP 接続枯渇サービス拒否の脆弱性
- SIP インスペクション サービス拒否の脆弱性

- SCCP 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 IKE メッセージ サービス拒否の脆弱性
- NTLMv1 認証 バイパス の 脆弱性

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** Command Line Interface （ CLI ） コマンドを発行できます。 ソフトウェア バージョン 8.0(4) 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
Cisco Adaptive Security Appliance Software Version 8.0(4)
Device Manager Version 6.0(1)
<output truncated>
```

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 Firewall サービス モジュール (FWSM) はいくつかのこのアドバイザリの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 217-fwsm で利用できます。

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 1.1	2010-February-17	応用軽減情報への追加されたリンク。
リビジョン 1.0	2010-February-17	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。