PIX および ASA アプライアンスでの LDAP および VPN の脆弱性

High

アドバイザリーID : cisco-sa-20070502-asa
初公開日 : 2007-05-02 16:00
バージョン 1.1 : Final
CVSSスコア : 8.0
回避策 : Yes
Cisco バグ ID :

CVE-2007-2462
CVE-2007-2463
CVE-2007-2464

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 Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）および PIX セキュリティ アプライアンスには、複数の脆弱性が存在します。 これらの脆弱性の中には、Lightweight Directory Access Protocol（LDAP）認証のバイパスに関する 2 つの脆弱性と、Denial of service（DoS; サービス拒否）に関する 2 つの脆弱性が含まれます。

LDAP 認証バイパスの脆弱性は、LDAP 認証サーバを使用するように設定されているデバイスが実行する特定の処理手順によって発生します。 これらの脆弱性により、認証を受けていないユーザが内部ネットワークまたはデバイス自体にアクセスできる可能性があります。

DoS に関する 2 つの脆弱性は、デバイスが Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を終了するときに発生する可能性があります。 これらの DoS 脆弱性が攻撃者に悪用されると、VPN ユーザの接続が切断されたり、新しい接続が妨げられたり、デバイスがトラフィックを送信できなくなったりする可能性があります。

これらの脆弱性は、認証、IPSec VPN、および SSL VPN のコードに分散しています。 このアドバイザリでは、次の不具合に分類して説明を行います。

- LDAP 認証バイパス
- パスワード期限が設定された VPN でのサービス拒否
- SSL VPN でのサービス拒否

Cisco では、該当するお客様用に、これらの脆弱性に対応する無償ソフトウェアを提供しております。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070502-asa で掲示されます。

該当製品

修正済みソフトウェア

ソフトウェア バージョン 7.1 および 7.2 が稼働している Cisco ASA および PIX セキュリティ アプライアンスは、脆弱である可能性があります。 特定の脆弱性に該当するバージョンであるかどうかを確認するには、次の表を参照してください。

脆弱性	該当するソフトウェア バージョン
LDAP 認証バイパス	7.2(2)8 より前の 7.2 バージョン
パスワード期限が設定された VPN でのサービス拒否	7.1(2)49 より前の 7.1 バージョン 7.2(2)17 より前の 7.2 バージョン
SSL VPN でのサービス拒否	7.1(2)49 より前の 7.1 バージョン 7.2(2)19 より前の 7.2 バージョン

デバイスで実行されている Cisco ASA または PIX システム ソフトウェアのバージョンを確認するには、デバイスの Command Line Interface (CLI; コマンドライン インターフェイス) にログインして、**show version** コマンドを発行します。 ソフトウェア リリース 7.2(2)10 が稼働している ASA の例を次に示します。

```
ciscoasa#show version

Cisco Adaptive Security Appliance Software Version 7.2(2)10
```

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、アプリケーションにログインすると、ログイン ウィンドウの表または ASDM ウィンドウの左上隅に、次のようなラベルでバージョンが表示されます。

PIX Version 7.2(2)10

該当するソフトウェア バージョンが稼働している Cisco ASA および PIX セキュリティ アプライアンスは、次のいずれかの設定を実行している場合にのみ脆弱です。

LDAP 認証バイパスの脆弱性

Cisco PIX または ASA デバイスが脆弱になるケースとしては、次の 2 つの設定シナリオが存在します。

- Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）
  LDAP 認証サーバを使用し、PAP 以外の認証プロトコルを使用するように設定されているデバイスは、脆弱である可能性があります。 設定における LDAP サーバーの指定は、CLI コマンド **aaa-server ldap server host <ip address>** を使用して行います。 認証プロトコルの指定は、設定の **tunnel-group <tunnel-group> ppp-attributes** セクション内で **authentication <protocol>** コマンドを使用して行います。
  脆弱なデバイスにおいて、この脆弱性に関連する設定セグメントを次に示します。 次の設定例では、認証サーバは LDAP と指定され、認証プロトコルは ms-chap-v2 と指定されています。
  ```
  ciscoasa#show version

  Cisco Adaptive Security Appliance Software Version 7.2(2)10
  ```
- リモート管理アクセス
  リモート管理アクセス（telnet、SSH、HTTP）を許可し、クレデンシャルの検証に LDAP Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）サーバを使用するように設定されているデバイスは、脆弱である可能性があります。
  LDAP サーバは、設定ファイル内の **aaa-server <server_group> protocol ldap** コマンドの server_group として定義されています。 遠隔管理 アクセスのための LDAP認証 サーバはコマンドによって、**AAA認証{telnet** 定義されます **| SSH | http | シリアル}コンソール server_group**。
  脆弱なデバイスにおいて、この脆弱性に関連する設定セグメントを次に示します。 認証サーバが LDAP として指定され、SSH に対するリモート管理アクセスが許可されていて、定義済みの LDAP AAA サーバによってクレデンシャルが検査されるようになっています。
  ```
  ciscoasa#show version

  Cisco Adaptive Security Appliance Software Version 7.2(2)10
  ```

パスワード期限が設定された VPN でのサービス拒否

次の例に示すように、**password-management** コマンドが tunnel-group セクションにある場合、そのデバイスはこの脆弱性の対象になる可能性があります。

```
ciscoasa#show version

Cisco Adaptive Security Appliance Software Version 7.2(2)10ciscoasa#show version

Cisco Adaptive Security Appliance Software Version 7.2(2)10
```

SSL VPN でのサービス拒否

インターフェイスでクラスレス SSL VPN が有効になっているデバイスは、この脆弱性に該当します。

クライアントレス SSL VPN が有効なデバイスの実行コンフィギュレーションには **webvpn** セクションが含まれます。 このエントリは次のようなものです。

```
ciscoasa#show version
```

脆弱性を含んでいないことが確認された製品

Firewall Services Module（FWSM）は、このアドバイザリで説明されているどの脆弱性の影響も受けません。

Cisco ASA および PIX セキュリティ アプライアンスは、次の条件が満たされている場合、これらの脆弱性には該当しません。

L2TP セッションの LDAP 認証バイパス

次の条件が満たされている ASA および PIX セキュリティ アプライアンスは、この脆弱性には該当しません。

- L2TP over IPSec を使用するように設定され、LDAP 以外の認証サーバを使用するように設定されているデバイス
- L2TP over IPSec を使用するように設定され、PAP を実行する LDAP 認証サーバを使用するように設定されているデバイス
- リモート管理セッションの認証に LDAP 以外の AAA サーバまたはローカル データベースを使用するデバイス

パスワード期限が設定された VPN でのサービス拒否

パスワード期限のあるリモート アクセス トンネル グループが設定されていないデバイスは、この脆弱性に該当する可能性はありません。

SSL VPN でのサービス拒否

クライアントレス SSL VPN 接続をサポートするように設定されていないデバイスは、この脆弱性に該当する可能性はありません。 PIX セキュリティ アプライアンスはクライアントレス SSL VPN 接続をサポートしないので、脆弱ではありません。

改訂履歴

リビジョン 1.1	2008-April-24	CSCsh81111 および CSCsi16248 のために記録する CVSS への更新済リンク。
リビジョン 1.0	2007 年 5 月 2 日	初版リリース

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。