ASA と AnyConnect を使用する場合に、POODLE および POODLE BITES の脆弱性を回避する

Document ID: 118780

Updated: 2015 年 5 月 6 日

Contributed by Atri Basu, Cisco TAC Engineer.

PDF のダウンロード
印刷
フィードバック

関連製品

- Cisco AnyConnect VPN Client
- Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア
- Secure Socket Layer (SSL)
- Cisco AnyConnect セキュア モビリティ クライアント
- Cisco ASA 5500-X シリーズ次世代ファイアウォール

目次

概要

Secure Sockets Layer （ SSL ） 接続のために (ASA) および AnyConnect 適応型セキュリティ アプライアンス (ASA) 使用するとき Downgraded レガシー 暗号化 (プードル) 脆弱性のパッディング Oracle を避けるために必要があるものをこの資料に記述されていますする。

背景説明

Transport Layer Security バージョン 1 （ TLSv1 ）プロトコルのプードル脆弱性影響ある特定の実装はリモート攻撃者非認証が機密情報にアクセスするようにし。

脆弱性は Cipher Block Chaining （ CBC ）モードを使用するとき TLSv1 で設定される不適当なブロック 暗号パッディングが原因です。 攻撃者は暗号メッセージの「神託埋め込み」側チャネル攻撃を行うために脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が機密情報にアクセスすることを可能にする可能性があります。

問題

ASA は 2 フォームの着信 SSL 接続を可能にします:

1. Clientless WebVPN
2. AnyConnect Client

ただし、ASA または AnyConnect クライアントの TLS 実装のどれもプードルから影響を受けません。 その代り、SSLv3 実装はどのクライアントでも (ブラウザか AnyConnect ） SSLv3 をネゴシエートするこの脆弱性に敏感ですように影響を受けています。

> **注意**： しかしプードルかみ傷は ASA の TLSv1 に影響を与えます。 該当製品および修正に関する詳細については、CVE-2014-8730 を参照して下さい。

解決策

Cisco はこの問題にこれらのソリューションを設定しました:

1. 以前 (ネゴシエートされた ） SSLv3 を非難されたダウンロードのために利用可能 な バージョンが (v3.1x および v4.0 両方 ） SSLv3 をサポートし、従ってそれらは問題に敏感ネゴシエートしないではないです AnyConnect のすべてのバージョン。

2. ASA の既定のプロトコル設定は SSLv3 から TLSv1.0 に着信接続が TLS をサポートするクライアントからある限り、それがネゴシエートされるものがであるように変更されました。

3. ASA はこのコマンドで特定の SSL プロトコルだけ受け入れるために手動で設定することができます:

   `ssl server-version`
   ソリューション 1 に言及されているように、AnyConnect 現在サポートされたクライアントのどれも SSLv3 をもうネゴシエートしません、従ってクライアントはこれらのコマンドのどちらかで設定されたあらゆる ASA に接続し損います:`ssl server-version sslv3`
   `ssl server-version sslv3-only`
   ただし、どので SSLv3 ネゴシエーションが特に使用されるか非難された v3.1.x AnyConnect バージョンおよび v3.0.x を使用する配備のために (ある 3.1.05182 ） AnyConnect すべてのビルド バージョン PRE は、および、唯一のソリューション SSLv3 の使用を除去するか、

またはクライアントをアップグレードと考慮することです。

4. プードルかみ傷（Cisco バグ ID CSCus08101）のための実際の修正は暫定リリース バージョンだけに統合されています。 問題を解決する修正がある ASA バージョンにアップグレードできます。 最初の利用可能 なバージョン on Cisco 接続オンライン（CCO）はバージョン 9.3(2.2) です。

   この脆弱性のための最初の固定 ASA ソフトウェア リリースは次の通りです:
   8.2 トレイン: 8.2.5.558.4 トレイン: 8.4.7.269.0 トレイン: 9.0.4.299.1 トレイン: 9.1.69.2 トレイン: 9.2.3.39.3 トレイン: 9.3.2.2

TLSv1.2

- ASA はソフトウェア バージョン 9.3(2) の時点で TLSv1.2 をサポートします。
- AnyConnect バージョン 4.x クライアントはすべて TLSv1.2 をサポートします。

この場合、次を意味します。

- Clientless WebVPN を使用する場合、このソフトウェアのバージョンを実行したりまたはより高く TLSv1.2 をネゴシエートできますどの ASA でも。

- AnyConnect クライアントを使用する場合、TLSv1.2 を使用するために、バージョン 4.x クライアントにアップグレードする必要があります。

関連情報

- CVE-2014-8730
- Cisco バグ ID CSCug51375
- Cisco バグ ID CSCur42776
- テクニカルサポートとドキュメント - Cisco Systems

Cisco サポート コミュニティ - 特集対話

Cisco サポート コミュニティでは、フォーラムに参加して情報交換することができます。

Updated: 2015 年 5 月 6 日
Document ID: 118780