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

内容

概要

このドキュメントでは、適応型セキュリティ アプライアンス（ASA）と AnyConnect をセキュアソケット レイヤ（SSL）接続に使用するときに Padding Oracle On Downgraded Legacy Encryption（POODLE）脆弱性の発生を回避するために実行する必要がある作業について説明します。

背景説明

POODLEの脆弱性は、Transport Layer Security Version 1(TLSv1)プロトコルの特定の実装に影響を与え、認証されていないリモートの攻撃者が機密情報にアクセスする可能性があります。

この脆弱性は、Cipher Block Chaining(CBC)モードを使用するときにTLSv1で実装される不適切なブロック暗号パディングに起因します。攻撃者は、この脆弱性を不正利用して、暗号化メッセージに対して「oracle padding」サイドチャネル攻撃を実行する可能性があります。エクスプロイトに成功すると、攻撃者は機密情報にアクセスできる可能性があります。

問題

ASAは、次の2つの形式で着信SSL接続を許可します。

1. Clientless WebVPN
2. AnyConnect Client

ただし、ASAまたはAnyConnectクライアントでのTLS実装はいずれもPOODLEの影響を受けません。代わりに、SSLv3の実装が影響を受けるため、SSLv3をネゴシエートするすべてのクライアント（ブラウザまたはAnyConnect）がこの脆弱性の影響を受ける可能性があります。

> **注意**：ただし、POODLE BITESはASAのTLSv1に影響を与えます。影響を受ける製品および修正の詳細については、CVE-2014-8730を参照してください。

解決方法

シスコは、この問題に対して次のソリューションを実装しました。

1. 以前にサポートされていた（ネゴシエートされた）SSLv3のすべてのバージョンは廃止され、ダウンロード可能なバージョン（v3.1xとv4.0の両方）はSSLv3をネゴシエートしないため、この問題は発生しません。

2. ASAのデフォルトのプロトコル設定はSSLv3からTLSv1.0に変更され、着信接続がTLSをサポートするクライアントからのものであれば、ネゴシエートされます。

3. ASAは、次のコマンドを使用して、特定のSSLプロトコルのみを受け入れるように手動で設定できます。

   ssl server-version

   ソリューション1で説明したように、現在サポートされているAnyConnectクライアントはSSLv3をネゴシエートしなくなるため、クライアントは次のコマンドのいずれかを使用して設定されたASAへの接続に失敗します。

   ```
   ssl server-version sslv3
   ssl server-version sslv3-only
   ```

   ただし、廃止されたv3.0.xおよびv3.1.x AnyConnectバージョン(すべてのAnyConnectビルドバージョンPRE 3.1.05182)を使用し、SSLv3ネゴシエーションが特に使用される展開では、SSLv3の使用を排除するか、クライアントのアップグレードを検討します。

4. POODLE BITES(Cisco Bug ID CSCus08101)の実際の修正は、最新の暫定リリースバージョンにのみ統合されます。この問題を解決する修正を含むASAバージョンにアップグレードできます。Cisco Connection Online(CCO)で最初に利用可能なバージョンは、バージョン9.3(2.2)です。

   この脆弱性に対する最初の修正済みASAソフトウェアリリースは次のとおりです。
   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以降でTLSv1.2をサポートしています。
- 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。

- クライアントレスWebVPNを使用する場合、このバージョン以上のソフトウェアを実行するASAはTLSv1.2をネゴシエートできます。

- AnyConnectクライアントを使用する場合、TLSv1.2を使用するには、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 Bug ID CSCug51375
- Cisco Bug ID CSCur42776
- テクニカル サポートとドキュメント – Cisco Systems