Vermeiden Sie die Schwachstellen POODLE und POODLE BITES, wenn Sie ASA und AnyConnect verwenden.

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Schwachstelle Padding Oracle On Downgraded Legacy Encryption (POODLE) vermeiden müssen, wenn Sie Adaptive Security Appliances (ASAs)- und AnyConnect for Secure Sockets Layer (SSL)-Verbindungen verwenden.

Hintergrundinformationen

Die POODLE-Schwachstelle wirkt sich auf bestimmte Implementierungen des Transport Layer Security Version 1 (TLSv1)-Protokolls aus und könnte es einem nicht authentifizierten Remote-Angreifer ermöglichen, auf vertrauliche Informationen zuzugreifen.

Die Schwachstelle ist auf eine unsachgemäße Blockchiffrierung zurückzuführen, die in TLSv1 implementiert wurde, wenn Sie den Cipher Block Chaining (CBC)-Modus verwenden. Ein Angreifer könnte diese Schwachstelle ausnutzen, um einen "orakle padding"-Side-Channel-Angriff auf die kryptografische Nachricht durchzuführen. Ein erfolgreicher Exploit könnte es dem Angreifer ermöglichen, auf vertrauliche Informationen zuzugreifen.

Problem

Die ASA ermöglicht eingehende SSL-Verbindungen in zwei Formen:

1. Clientless-WebVPN
2. AnyConnect-Client

Keine der TLS-Implementierungen auf der ASA oder dem AnyConnect-Client ist jedoch von POODLE betroffen. Stattdessen ist die SSLv3-Implementierung betroffen, sodass alle Clients (Browser oder AnyConnect), die SSLv3 aushandeln, für diese Schwachstelle anfällig sind.

> **Vorsicht**: POODLE-BITES wirken sich jedoch auf TLSv1 auf der ASA aus. Weitere Informationen zu betroffenen Produkten und Bugfixes finden Sie in CVE-2014-8730.

Lösung

Cisco hat diese Lösungen für dieses Problem implementiert:

1. Alle Versionen von AnyConnect, die zuvor SSLv3 unterstützt (ausgehandelt) haben, wurden veraltet, und die zum Download verfügbaren Versionen (sowohl v3.1x als auch v4.0) handeln SSLv3 nicht aus, sodass sie nicht für das Problem anfällig sind.

2. Die Standardprotokolleinstellung der ASA wurde von SSLv3 in TLSv1.0 geändert, sodass, solange die eingehende Verbindung von einem Client stammt, der TLS unterstützt, das ausgehandelt wird.

3. Die ASA kann manuell so konfiguriert werden, dass sie nur bestimmte SSL-Protokolle mit folgendem Befehl akzeptiert:

   `ssl server-version`

   Wie in Lösung 1 erwähnt, handelt keiner der derzeit unterstützten AnyConnect-Clients mehr über SSLv3 aus, sodass der Client keine Verbindung zu einer ASA herstellen kann, die mit einem der folgenden Befehle konfiguriert wurde:

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

   Bei Bereitstellungen jedoch, bei denen die veralteten AnyConnect-Versionen v3.0.x und v3.1.x verwendet werden (bei denen es sich um alle AnyConnect-Buildversionen PRE 3.1.05182 handelt) und in denen SSLv3-Aushandlung speziell verwendet wird, besteht die einzige Lösung darin, die Verwendung von SSLv3 zu beenden oder ein Client-Upgrade in Erwägung zu ziehen.

4. Die tatsächliche Behebung für POODLE BITES (Cisco Bug ID CSCus08101) wird nur in die neuesten Zwischenversionen integriert. Sie können ein Upgrade auf eine ASA-Version durchführen, die das Problem behebt. Die erste verfügbare Version auf Cisco Connection Online (CCO) ist Version 9.3(2.2).

   Die ersten behobenen ASA-Softwareversionen für diese Schwachstelle sind:
   8.2 Zug: 8.2.5.558.4 Zug: 8.4.7.269.0 Zug: 9.0.4.299.1 Zug: 9.1.69.2 Zug: 9.2.3.39.3 Zug: 9.3.2.2

TLSv1.2

- Die ASA unterstützt TLSv1.2 ab Softwareversion 9.3(2).
- Alle AnyConnect-Clients der Version 4.x unterstützen TLSv1.2.

Das bedeutet:

- Wenn Sie Clientless WebVPN verwenden, kann jede ASA, die diese Version der Software oder höher ausführt, TLSv1.2 aushandeln.

- Wenn Sie den AnyConnect-Client verwenden, müssen Sie ein Upgrade auf Version 4.x-Clients durchführen, um TLSv1.2 verwenden zu können.

Zugehörige Informationen

  - VE 2014-8730
  - Cisco Bug-ID CSCug51375
  - Cisco Bug-ID CSCur42776
- Technischer Support und Dokumentation - Cisco Systems