Éviter la vulnérabilité POODLE et POODLE BITES lorsque vous utilisez ASA et AnyConnect

Contenu

Introduction

Ce document décrit ce que vous devez faire pour éviter la vulnérabilité Padding Oracle On Downgradated Legacy Encryption (POODLE) lorsque vous utilisez des appliances de sécurité adaptatives (ASA) et la connectivité AnyConnect for Secure Sockets Layer (SSL).

Informations générales

La vulnérabilité POODLE affecte certaines implémentations du protocole TLSv1 (Transport Layer Security version 1) et peut permettre à un attaquant distant non authentifié d'accéder à des informations sensibles.

La vulnérabilité est due à un remplissage de chiffrement de bloc incorrect implémenté dans TLSv1 lorsque vous utilisez le mode Chaînage de bloc de chiffrement (CBC). Un attaquant pourrait exploiter la vulnérabilité afin d'exécuter une attaque de canal latéral « oracle padding » sur le message cryptographique. Une exploitation réussie pourrait permettre à l'attaquant d'accéder à des informations sensibles.

Problème

L'ASA autorise les connexions SSL entrantes sous deux formes :

1. WebVPN sans client
2. Client AnyConnect

Cependant, aucune des implémentations TLS sur l'ASA ou le client AnyConnect n'est affectée par POODLE. Au lieu de cela, la mise en oeuvre de SSLv3 est affectée de sorte que tous les clients (navigateur ou AnyConnect) qui négocient SSLv3 soient susceptibles de cette vulnérabilité.

> **Attention** : POODLE BITES affecte cependant le TLSv1 sur l'ASA. Pour plus d'informations sur les produits et correctifs concernés, reportez-vous à CVE-2014-8730.

Solution

Cisco a mis en oeuvre les solutions suivantes à ce problème :

1. Toutes les versions d'AnyConnect qui supportaient précédemment SSLv3 (négocié) ont été déconseillées et les versions disponibles pour téléchargement (v3.1x et v4.0) ne négocieront pas SSLv3, de sorte qu'elles ne sont pas sensibles au problème.

2. Le paramètre de protocole par défaut de l'ASA a été modifié de SSLv3 à TLSv1.0 de sorte que tant que la connexion entrante provient d'un client qui prend en charge TLS, c'est ce qui sera négocié.

3. L'ASA peut être configuré manuellement pour accepter uniquement des protocoles SSL spécifiques avec cette commande :

   `ssl server-version`

   Comme mentionné dans la solution 1, aucun des clients AnyConnect actuellement pris en charge ne négocie plus SSLv3, de sorte que le client ne pourra pas se connecter à un ASA configuré avec l'une ou l'autre de ces commandes :

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

   Cependant, pour les déploiements qui utilisent les versions v3.0.x et v3.1.x AnyConnect déconseillées (qui sont toutes des versions de build AnyConnect PRE 3.1.05182) et dans lesquelles la négociation SSLv3 est spécifiquement utilisée, la seule solution est d'éliminer l'utilisation de SSLv3 ou d'envisager une mise à niveau client.

4. Le correctif réel pour POODLE BITES (ID de bogue Cisco CSCus08101) sera intégré dans les dernières versions provisoires uniquement. Vous pouvez effectuer une mise à niveau vers une version ASA qui a la solution pour résoudre le problème. La première version disponible sur Cisco Connection Online (CCO) est la version 9.3(2.2).

   Les premières versions fixes du logiciel ASA pour cette vulnérabilité sont les suivantes : **8.2 Train : 8.2.5.558.4 Train : 8.4.7.269.0 Train : 9.0.4.299.1 Train : 9.1.69.2 Train : 9.2.3.39.3 Train : 9.3.2.2**

TLSv1.2

- L'ASA prend en charge TLSv1.2 depuis la version 9.3(2) du logiciel.
- Les clients AnyConnect version 4.x prennent tous en charge TLSv1.2.

Cela signifie :

- Si vous utilisez WebVPN sans client, tout ASA qui exécute cette version du logiciel ou une version supérieure peut négocier TLSv1.2.

- Si vous utilisez le client AnyConnect, afin d'utiliser TLSv1.2, vous devrez effectuer une mise à niveau vers les clients Version 4.x.

Informations connexes

- CVE-2014-8730
- ID bogue Cisco CSCug51375
- ID bogue Cisco CSCur42776
- Support et documentation techniques - Cisco Systems