Évitez la vulnérabilité de CANICHE et de MORSURES de CANICHE quand vous utilisez l'ASA et l'AnyConnect

Contenu

Introduction

Ce document décrit ce que vous devez faire pour éviter Oracle complétant sur la vulnérabilité existante de cryptage Downgraded (CANICHE) quand vous utilisez les appliances de sécurité adaptable (ASA) et l'AnyConnect pour la Connectivité de Secure Sockets Layer (SSL).

Informations générales

Réalisations d'affects de vulnérabilité de CANICHE les certaines du protocole de la version 1 de Transport Layer Security (TLSv1) et pourraient permettre à un attaquant unauthenticated et distant pour accéder aux informations confidentielles.

La vulnérabilité est due à la remplissage inexacte de chiffre par bloc mise en application dans TLSv1 quand vous utilisez le bloc de chiffrement enchaînant le mode (CBC). Un attaquant a pu exploiter la vulnérabilité afin d'exécuter une attaque de côté-canal « de remplissage d'oracle » sur le message cryptographique. Une exploit réussie a pu permettre à l'attaquant pour accéder aux informations confidentielles.

Problème

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

1. Webvpn sans client
2. Client d'AnyConnect

Cependant, aucune des réalisations de TLS sur l'ASA ou le client d'AnyConnect n'est affectée par le CANICHE. Au lieu de cela, l'implémentation SSLv3 est affectée de sorte que tous les clients (navigateur ou AnyConnect) qui négocient SSLv3 sont susceptibles de cette vulnérabilité.

> **Attention** : Les MORSURES de CANICHE cependant affecte le TLSv1 sur l'ASA. Pour plus d'informations sur les Produits et les difficultés affectés, référez-vous à CVE-2014-8730.

Solution

Cisco a mis en application ces solutions au problème :

1. Toutes les versions d'AnyConnect qui ont précédemment pris en charge SSLv3 (négocié) ont été désapprouvées et les versions disponibles pour le téléchargement (v3.1x et v4.0) ne négocieront pas SSLv3 ainsi de elles ne sont pas susceptibles de la question.

2. La configuration de protocole du par défaut de l'ASA a été changée de SSLv3 à TLSv1.0 de sorte que tant que la connexion entrante est d'un client qui prend en charge le TLS, ce soit ce qui sera négocié.

3. L'ASA peut être manuellement configurée pour recevoir seulement des protocoles spécifiques SSL avec cette commande :

   ssl server-version

   En tant qu'en solution 1 mentionné, aucun des clients actuellement pris en charge d'AnyConnect ne négocie désormais SSLv3, ainsi le client ne se connectera pas à n'importe quelle ASA configurée à l'un 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 qui ont été désapprouvées (qui sont toutes les versions PRÉ 3.1.05182 de construction d'AnyConnect), et dans le quel négociation SSLv3 est spécifiquement utilisée, la seule solution est d'éliminer l'utilisation de SSLv3 ou de considérer une mise à jour de client.

4. La difficulté réelle pour des MORSURES de CANICHE (ID de bogue Cisco CSCus08101) sera intégrée dans les dernières versions de version intermédiaire seulement. Vous pouvez améliorer à une version ASA qui a la difficulté pour résoudre le problème. La première version disponible sur le Cisco Connection Online (CCO) est version 9.3(2.2).

   Les premières versions logicielles fixes ASA pour cette vulnérabilité sont comme suit : **8.2 Série : 8.2.5.558.4 Série : 8.4.7.269.0 Série : 9.0.4.299.1 Série : 9.1.69.2 Série : 9.2.3.39.3 Série : 9.3.2.2**

TLSv1.2

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

Ceci signifie :

- Si vous utilisez le webvpn sans client, alors n'importe quelle ASA qui exécute cette version de logiciel ou plus élevé peut négocier TLSv1.2.

- Si vous utilisez le client d'AnyConnect, afin d'utiliser TLSv1.2, vous devrez améliorer aux

clients de version 4.x.

Informations connexes

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