Désactiver les chiffrements de mode CBC du serveur SSH sur l’ASA

Table des matières

Introduction

Ce document décrit comment désactiver le serveur SSH CBC mode Chiffres sur ASA. Sur la vulnérabilité d'analyse CVE-2008-5161, il est documenté que l'utilisation d'un algorithme de chiffrement par bloc en mode Chaînage de blocs de chiffrement (CBC), rend plus facile pour les attaquants distants de récupérer certaines données en texte clair à partir d'un bloc arbitraire de texte chiffré dans une session SSH via des vecteurs inconnus.

Le chiffrement par blocs (CBC) est un mode de fonctionnement du chiffrement par blocs. Cet algorithme utilise un chiffrement par blocs pour fournir un service d'information tel que la confidentialité ou l'authenticité.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurité adaptatif Architecture de plate-forme ASA
- Chaînage de blocs de chiffrement (CBC)

Composants utilisés

Les informations de ce document sont basées sur un Cisco ASA 5506 avec OS 9.6.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Par défaut, le mode CBC ASA est activé sur l'ASA, ce qui peut constituer une vulnérabilité pour les informations du client.

Solution

Après l'amélioration de CSCum6371, la possibilité de modifier les chiffrements ssh ASA a été introduite sur la version 9.1(7), mais la version qui a officiellement les commandes ssh cipher encryption et l'intégrité du chiffrement ssh est 9.6.1.

Afin de désactiver le mode CBC Chiphers sur SSH suivez cette procédure :

Exécutez « sh run all ssh » sur l'ASA :

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption medium
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

Si vous voyez la commande ssh cipher encryption medium cela signifie que l'ASA utilise des chiffrements de moyenne et haute puissance qui est configuré par défaut sur l'ASA.

Afin de voir les algorithmes de chiffrement ssh disponibles dans l'ASA, exécutez la commande show ssh ciphers :

```
ASA(config)# show ssh ciphers
Available SSH Encryption and Integrity Algorithms Encryption Algorithms:
        all:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        low:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        medium:  3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        fips:    aes128-cbc   aes256-cbc
        high:    aes256-cbc   aes256-ctr
Integrity Algorithms:
        all:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
        low:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
        medium:  hmac-sha1    hmac-sha1-96
        fips:    hmac-sha1
        high:    hmac-sha1
```

Le résultat montre tous les algorithmes de chiffrement disponibles : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr.

Afin de désactiver le mode CBC afin qu'il puisse être utilisé sur la configuration ssh, personnalisez les algorithmes de chiffrement à utiliser, avec la commande suivante :

```
ssh cipher encryption custom aes128-ctr:aes192-ctr:aes256-ctr
```

Une fois que ceci est fait, exécutez la commande show run all ssh, maintenant dans la configuration de cryptage de chiffrement ssh tous les algorithmes utilisent seulement le mode CTR :

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption custom "aes128-ctr:aes192-ctr:aes256-ctr"
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

De même, les algorithmes d'intégrité SSH peuvent être modifiés avec la commande ssh cipher integration.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.