Dépannage de la vulnérabilité de chiffrement CBC dans NCCM 3.8+ et CSPC 2.9+

Table des matières

Introduction

Ce document décrit comment dépanner la vulnérabilité de chiffrement CBC dans NCCM 3.8+ et CSPC 2.9+.

Problème

Dans les versions récentes de CSPC/NCCM, nous avons une vulnérabilité faible de chiffrement CBC. Dans la plupart des cas, vous pouvez le réparer en mettant à jour les fichiers de configuration ssh souhaités. Cependant, cet article a été soulevé pour refuser explicitement leur accès via des politiques de chiffrement. Utilisez ceci si tout le reste échoue. Cela ne peut pas affecter les stratégies de chiffrement par défaut, mais plutôt ajouter une couche supplémentaire au-dessus de la stratégie par défaut.

Approche traditionnelle

Assurez-vous que tous les chiffrements CVC ont été supprimés de sshd_config. Si le problème persiste, vous pouvez fournir une entrée vide au paramètre sous /etc/sysconfig/sshd.

```
CRYPTO_POLICY=
```

Assurez-vous de prendre une sauvegarde avant d'effectuer toute modification.

Pour vérifier si cela a fonctionné, exécutez cette commande sur votre ordinateur distant :

```
ssh -vv -oCiphers=aes128-cbc,aes256-cbc 127.0.0.1
```

Si vous êtes invité à saisir un mot de passe ou à ajouter des clés RSA, le problème persiste.

Solution

Si la procédure précédente échoue, vous pouvez ajouter une couche supplémentaire de stratégie de chiffrement en refusant explicitement tout accès aux chiffrements CBC. Nous ne recommandons pas de modifier la configuration par défaut d'une stratégie de chiffrement. Cette approche est donc conseillée.

Avant de continuer, assurez-vous qu'aucune couche supplémentaire n'est appliquée au-dessus de la stratégie de chiffrement DEFAULT. S'il existe d'autres couches, vous pouvez les examiner avant d'apporter des modifications. Pour vérifier ceci, exécutez cette commande :

```
update-crypto-policies --show
```

La réponse est DEFAULT. Si c'est le cas, vous pouvez passer aux étapes suivantes sans procéder à une vérification supplémentaire.

Créez un nouveau fichier sous le chemin absolu :

```
/etc/crypto-policies/policies/modules/DISABLE-CBC.pmod
```

Vous pouvez nommer ce fichier de n'importe quelle manière, mais l'extension se termine par .pmod.

Puisque nous supprimons cette vulnérabilité pour restreindre l'accès ssh à l'aide de ces chiffrements, entrez cette ligne comme la seule entrée dans ce nouveau fichier :

```
ssh_cipher = -AES-128-CBC -AES-256-CBC
```

Remarque : Ceci est uniquement à titre de référence. Vous pouvez ajouter tous les chiffrements que vous essayez explicitement de refuser, mais il est conseillé de créer un nouveau fichier pour tout autre chiffrage que CBC afin d'éviter toute confusion.

Après avoir enregistré le fichier, définissez la valeur de crypto-policies de DEFAULT à cette couche supplémentaire en exécutant cette commande :

```
update-crypto-policies --set DEFAULT:DISABLE-CBC
```

Là encore, la valeur DISABLE-CBC peut différer en fonction du nom fourni lors de la création du fichier.

Vous pouvez maintenant revérifier en exécutant :

```
update-crypto-policies --show
```

Cette fois, il affiche DEFAULT:DISABLE-CBC, confirmant qu'une couche supplémentaire a été ajoutée sans modifier le fichier par défaut.

À ce stade, si vous revérifiez l'accès, il est refusé :

```
ssh -vv -oCiphers=aes128-cbc,aes256-cbc 127.0.0.1
```

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.