Contenu

Introduction

Ce document décrit comment passer en revue et configurer des versions d'authentification de SSH sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Comment est-ce que je m'assure que mon ESA reçoit seulement des connexions SSH des clients utilisant le SSH v2 ?

L'ESA peut être configuré pour permettre des connexions de Protocole Secure Shell (SSH). Les connexions SSH chiffrent le trafic entre l'hôte se connectant et l'ESA. Ceci protège les informations d'authentification comme le nom d'utilisateur et mot de passe. Il y a deux versions majeures du protocole de SSH : version 1 (SSH v1) et version 2 (SSH v2). Le SSH v2, étant plus récent, est plus sécurisé que le SSH v1, et beaucoup d'administrateurs ESA préfèrent ainsi permettre seulement des connexions des clients utilisant le SSH v2.

Sur des versions d'AsyncOS par 7.6.3, désactiver des connexions du SSH v1 peut être fait du CLI avec le **sshconfig** :

Sur des versions d'AsyncOS 8.x et plus nouveau, l'option de désactiver le SSH v1 n'existe pas avec le **sshconfig**. Si le SSH v1 était activé avant la mise à jour de 8.x, le SSH v1 restera activé et accessible sur l'ESA, même après que la mise à jour est complète quoique tout le soutien du SSH v1 ait été enlevé. Ceci peut être une question pour les administrateurs qui réalisent des audits de sécurité réguliers et l'essai de traversée.

Car tout le soutien du SSH v1 a été enlevé, une demande de support doit être ouverte pour faire désactiver SSHv1.

Exécutez la commande suivante d'un hôte externe de Linux/Unix, ou toute autre connexion applicable CLI de choix, de confirmer si le SSH v1 est activé ou désactivé à l'ESA en question :

La sortie prévue est des « versions majeures de Protocol diffèrent : 1 contre 2", qui signalerait que le SSH v1 est désactivé. Sinon, et le SSH v1 est encore activé, vous verrez :

Cette sortie signalerait que le SSH v1 est encore en service et peut entraîner l'insécurité avec l'ESA après évolution de lui à 8.x ou plus nouveau. Ceci peut être porté à la connaissance avec un test ou un audit de sécurité de traversée, et identifie un écart significatif. Afin de corriger, vous devrez ouvrir une valise et une demande de support pour faire corriger ceci. Vous devrez pouvoir fournir un tunnel de support de l'ESA pour le support technique de Cisco.

Informations connexes

- CSCuo46017 : Les restes SSHv1 activés après mise à jour et ne peuvent pas être désactivés
- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems