Comment puis-je m'assurer que mon ESA accepte uniquement les connexions SSH des clients utilisant SSH v2 ?

Contenu

Introduction

Ce document décrit comment examiner et configurer les versions d'authentification SSH sur l'appliance de sécurité de la messagerie Cisco (ESA).

Comment puis-je m'assurer que mon ESA accepte uniquement les connexions SSH des clients utilisant SSH v2 ?

Le ESA peut être configuré pour autoriser les connexions SSH (Secure Shell). Les connexions SSH chiffrent le trafic entre l'hôte de connexion et l'ESA. Cela protège les informations d'authentification comme le nom d'utilisateur et les mots de passe. Il existe deux versions principales du protocole SSH : version 1 (SSH v1) et version 2 (SSH v2). SSH v2, plus récent, est plus sécurisé que SSH v1, et de nombreux administrateurs ESA préfèrent donc autoriser uniquement les connexions des clients utilisant SSH v2.

Sur les versions d'AsyncOS à 7.6.3, la désactivation des connexions SSH v1 peut être effectuée à partir de l'interface de ligne de commande avec **sshconfig** :

```
mail3.example.com> sshconfig
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
- SETUP - Configure general settings.
[]> setup
SSH v1 is currently ENABLED.
Choose the operation you want to perform:
- DISABLE - Disable SSH v1
[]> DISABLE
```

Sur les versions d'AsyncOS 8.x et ultérieures, l'option de désactivation de SSH v1 n'existe pas avec **sshconfig**. Si SSH v1 a été activé avant la mise à niveau de 8.x, SSH v1 restera activé et

accessible sur l'ESA, même après la mise à niveau, même si toutes les fonctionnalités de SSH v1 ont été supprimées. Cela peut poser problème aux administrateurs qui effectuent régulièrement des audits de sécurité et des tests de pénétration.

Comme toute la prise en charge de SSH v1 a été supprimée, une demande de support doit être ouverte pour que SSHv1 soit désactivé.

Exécutez la commande suivante à partir d'un hôte Linux/Unix externe ou d'une autre connexion CLI de votre choix pour confirmer si SSH v1 est activé ou désactivé sur l'ESA en question :

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Protocol major versions differ: 1 vs. 2
```

Le résultat attendu est « Les versions principales du protocole diffèrent : 1 contre 2 », ce qui indique que SSH v1 est désactivé. Si ce n'est pas le cas, et que SSH v1 est toujours activé, vous verrez :

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Password:
Response:
Last login: Thu Oct 30 14:53:40 2014 from 192.168.0.3
Copyright (c) 2001-2013, Cisco Systems, Inc.

AsyncOS 8.0.1 for Cisco IronPort C360 build 023

Welcome to the Cisco IronPort C360 Messaging Gateway(tm) Appliance
myesa.local>
```

Ce résultat indique que SSH v1 est toujours en cours d'utilisation et peut provoquer une insécurité avec l'ESA après la mise à niveau vers 8.x ou une version plus récente. Il est possible d'attirer l'attention sur ce point au moyen d'un test de pénétration ou d'un audit de sécurité, et d'identifier une lacune significative. Pour corriger cette erreur, vous devez ouvrir un dossier d'assistance et demander à ce que ce dossier soit corrigé. Vous devez être en mesure de fournir un tunnel d'assistance à partir de l'ESA pour l'assistance technique Cisco.

Informations connexes

- CSCuo46017 : SSHv1 reste activé après la mise à niveau et ne peut pas être désactivé
- Cisco Email Security Appliance - Guides de l'utilisateur final
- Support et documentation techniques - Cisco Systems