¿Cómo me aseeguro que mi ESA valida solamente las conexiones SSH de los clientes que usan el v2 de SSH?

Contenido

Introducción

Este documento describe cómo revisar y configurar las versiones de la autenticación SSH en Cisco envíe por correo electrónico el dispositivo de seguridad (ESA).

¿Cómo me aseeguro que mi ESA valida solamente las conexiones SSH de los clientes que usan el v2 de SSH?

El ESA se puede configurar para permitir las conexiones del Secure Shell (SSH). Las conexiones SSH cifran el tráfico entre el host de conexión y el ESA. Esto protege la información de autenticación como el nombre de usuario y contraseña. Hay dos versiones importantes del protocolo SSH: versión 1 (v1 de SSH) y versión 2 (v2 de SSH). El v2 de SSH, siendo más reciente, es más seguro que el v1 de SSH, y muchos administradores ESA prefieren así permitir solamente las conexiones de los clientes que usan el v2 de SSH.

En las versiones de AsyncOS con 7.6.3, inhabilitar las conexiones del v1 de SSH se puede hacer del CLI con el **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
```

En las versiones de AsyncOS 8.x y más nuevo, la opción de inhabilitar el v1 de SSH no existe con el **sshconfig**. Si el v1 de SSH fue habilitado antes de la actualización de 8.x, el v1 de SSH seguirá

siendo habilitado y accesible en el ESA, incluso después la actualización es completa aunque todo el soporte para el v1 de SSH se ha quitado. Esto puede ser un problema para los administradores que realizan las auditorías de Seguridad regulares y la prueba de penetración.

Pues todo el soporte para el v1 de SSH se ha quitado, una petición del soporte se debe abrir para hacer SSHv1 inhabilitar.

Ejecute el siguiente comando de Linux externo/host UNIX, o la otra conexión aplicable CLI de la opción, de confirmar si el v1 de SSH se habilita o se inhabilita al ESA en la pregunta:

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

El resultado esperado es “versiones importantes del protocolo diferencia: 1 contra el 2", que señalaría que el v1 de SSH está inhabilitado. Si no, y el v1 de SSH todavía se habilita, usted verá:

```
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>
```

Esta salida señalaría que el v1 de SSH es todavía funcionando y puede causar la inseguridad con el ESA después de actualizarlo a 8.x o más nuevo. Esto se puede traer a la atención con una prueba de penetración o una auditoría de Seguridad, e identifica un intervalo significativo. Para corregir, usted necesitará abrir un caso de soporte y una petición para hacer esto corregir. Usted necesitará poder proporcionar un túnel del soporte del ESA para el Soporte técnico de Cisco.

Información Relacionada

- CSCuo46017: SSHv1 sigue siendo habilitado después de la actualización y no puede ser inhabilitado
- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems