¿Cómo me aseguro de que mi ESA sólo acepta conexiones SSH de clientes que utilizan SSH v2?

Contenido

Introducción

Este documento describe cómo revisar y configurar las versiones de autenticación SSH en Cisco Email Security Appliance (ESA).

¿Cómo me aseguro de que mi ESA sólo acepta conexiones SSH de clientes que utilizan SSH v2?

El ESA se puede configurar para permitir conexiones 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 las contraseñas. Hay dos versiones principales del protocolo SSH: versión 1 (SSH v1) y versión 2 (SSH v2). Por ser más reciente, SSH v2 es más seguro que SSH v1 y, por lo tanto, muchos administradores ESA prefieren permitir únicamente conexiones de clientes que utilizan SSH v2.

En las versiones de AsyncOS a 7.6.3, la inhabilitación de las conexiones SSH v1 se puede realizar desde la CLI con **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 posteriores, la opción de inhabilitar SSH v1 no existe con **sshconfig**. Si SSH v1 estaba habilitado antes de la actualización de 8.x, SSH v1 permanecerá habilitado y accesible en el ESA, incluso después de que la actualización se complete, aunque se

haya eliminado todo el soporte para SSH v1. Esto puede suponer un problema para los administradores que realizan auditorías de seguridad periódicas y pruebas de penetración.

Dado que se ha eliminado toda la compatibilidad con SSH v1, se debe abrir una solicitud de soporte para que SSHv1 esté desactivado.

Ejecute el siguiente comando desde un host Linux/Unix externo, u otra conexión CLI aplicable, para confirmar si SSH v1 está habilitado o inhabilitado para el ESA en cuestión:

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

El resultado esperado es "Las versiones principales del protocolo difieren: 1 frente a 2", lo que indicaría que SSH v1 está inhabilitado. Si no, y SSH v1 sigue habilitado, 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>
```

Este resultado indicaría que SSH v1 sigue en uso y puede causar inseguridad con el ESA después de actualizarlo a 8.x o más. Esto puede señalarse a la atención mediante una prueba de penetración o una auditoría de seguridad, e identificar una brecha significativa. Para corregirlo, deberá abrir un caso de soporte y solicitar que se corrija. Deberá poder proporcionar un túnel de soporte desde el ESA para el soporte técnico de Cisco.

Información Relacionada

- CSCuo46017: SSHv1 permanece habilitado después de la actualización y no se puede inhabilitar
- Dispositivo de seguridad Cisco Email Security Appliance - Guías de usuario final
- Soporte Técnico y Documentación - Cisco Systems