Como eu me certifico de que meu ESA aceita somente conexões de SSH dos clientes que usam SSH v2?

Índice

Introdução

Este documento descreve como rever e para configurar versões da autenticação SSH em Cisco envie por correio eletrónico a ferramenta de segurança (ESA).

Como eu me certifico de que meu ESA aceita somente conexões de SSH dos clientes que usam SSH v2?

O ESA pode ser configurado para permitir conexões do Shell Seguro (ssh). As conexões de SSH cifram o tráfego entre o host de conexão e o ESA. Isto protege a informação da autenticação como o nome de usuário e senha. Há duas versões principal do protocolo SSH: versão 1 (SSH v1) e versão 2 (SSH v2). O SSH v2, sendo mais recente, é mais seguro do que SSH v1, e assim muitos administradores ESA preferem permitir somente conexões dos clientes que usam SSH v2.

Em versões de AsyncOS com 7.6.3, as conexões de desabilitação SSH v1 podem ser feitas do CLI com o **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
```

Em versões de AsyncOS 8.x e mais novo, a opção de desabilitar SSH v1 não existe com **sshconfig**. Se o SSH v1 foi permitido antes da elevação de 8.x, o SSH v1 permanecerá permitido e acessível no ESA, mesmo depois que a elevação está completa mesmo que todo o apoio para

SSH v1 esteja removido. Esta pode ser uma edição para os administradores que executam auditorias e testes de penetração regulares de Segurança.

Porque todo o apoio para SSH v1 foi removido, um pedido do apoio deve ser aberto para ter SSHv1 desabilitado.

Execute o comando seguinte de um host externo de Linux/Unix, ou a outra conexão aplicável CLI da escolha, confirmar se o SSH v1 é permitido ou desabilitado ao ESA na pergunta:

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

O rendimento esperado é do “versões principal protocolo difere: 1 contra 2", que sinalizaria que o SSH v1 está desabilitado. Se não, e o SSH v1 é permitido ainda, você 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 saída sinalizaria que o SSH v1 é ainda dentro uso e pode causar a insegurança com o ESA após ter promovido o a 8.x ou mais novo. Isto pode ser trazido à atenção com um teste de penetração ou uma auditoria de Segurança, e identifica uma diferença significativa. A fim corrigir, você precisará de abrir um caso de suporte e um pedido para ter este corrigido. Você precisará de poder fornecer um túnel do apoio do ESA para o Suporte técnico de Cisco.

Informações Relacionadas

- CSCuo46017: As sobras SSHv1 permitidas após a elevação e não podem ser desabilitadas
- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems