如何确保我的ESA仅接受来自使用SSH v2的客户端的SSH连接？

目录

简介

本文档介绍如何在思科邮件安全设备(ESA)上查看和配置SSH身份验证版本。

如何确保我的ESA仅接受来自使用SSH v2的客户端的SSH连接？

ESA可配置为允许安全外壳(SSH)连接。 SSH连接会加密连接的主机和ESA之间的流量。这可保护用户名和密码等身份验证信息。SSH协议有两个主要版本：版本1(SSH v1)和版本2(SSH v2)。SSH v2较新，比SSH v1更安全，因此许多ESA管理员倾向于仅允许来自使用SSH v2的客户端的连接。

在AsyncOS版本到7.6.3上，可通过CLI使用sshconfig禁用SSH v1**连接**:

```
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
```

在AsyncOS 8.x及更高版本上，禁用SSH v1的选项与sshconfig不**存在**。 如果在8.x升级之前启用了SSH v1，则SSH v1在ESA上将保持启用和可访问，即使升级完成后SSH v1的所有支持都已删除。对于定期执行安全审计和渗透测试的管理员而言，这可能是一个问题。

由于SSH v1的所有支持都已删除，因此必须打开支持请求才能禁用SSHv1。

从外部Linux/Unix主机或其他适用的CLI连接（可选）运行以下命令，以确认是否对相关ESA启用或禁用SSH v1:

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

预期输出为“协议主要版本不同：1 vs. 2”，这表示SSH v1已禁用。 否则，SSH v1仍处于启用状态，您将看到：

```
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>
```

此输出将表明SSH v1仍在使用中，并且在将其升级到8.x或更高版本后，可能会导致ESA不安全。 这可以通过渗透测试或安全审计引起注意，并确定一个重大差距。 为了进行更正，您需要提交支持案例并请求更正。 您需要能够从ESA为思科技术支持提供支持隧道。

相关信息

- CSCuo46017:SSHv1在升级后保持启用状态，无法禁用
- 思科邮件安全设备 — 最终用户指南
- 技术支持和文档 - Cisco Systems