如何确保，我的ESA只接受从使用SSH v2的客户端的SSH连接？

目录

简介

本文描述如何查看，并且配置SSH在思科的验证版本给安全工具(ESA)发电子邮件。

如何确保，我的ESA只接受从使用SSH v2的客户端的SSH连接？

ESA可以配置允许安全壳SSH连接。 SSH连接加密连接的主机和ESA之间的流量。这保护认证信息类似用户名和密码。有SSH协议的两个主要版本：版本1 (SSH v1)和版本2 (SSH v2)。SSH v2，是更加最近的，比SSH v1是安全的更多和许多ESA管理员prefer只因而允许从使用SSH v2的客户端的连接。

在AsyncOS版本通过7.6.3，禁用的SSH v1连接可以从与**sshconfig**的CLI完成：

```
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版本和更新，禁用的SSH v1的选项不存在与**sshconfig**。 如果SSH v1在升级8.x之前启用， SSH v1将保持已启用和可访问在ESA，在升级完成以后，即使SSH的v1所有支持删除。这可能是执行正常安全跟踪和侵彻试验的管理员的一个问题。

因为SSH的v1所有支持删除，必须打开支持请求安排SSHv1禁用。

从一台外部Linux/UNIX主机运行以下命令，或者选择的其他可适用的CLI连接，确认SSH v1是否是启用或禁用的对有问题的ESA ：

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
```

```
Protocol major versions differ: 1 vs. 2
```

预期的输出是“协议主要版本有所不同：1与2"，表明SSH v1禁用。 否则，并且SSH v1仍然启用，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>
```

此输出表明SSH v1是在使用中的，并且能在升级它以后导致与ESA的不可靠8.x或新。 这可能带给与侵彻试验或安全跟踪的关注，并且识别一个重大的差距。 为了更正，您将需要打开支持案件和请求安排此被更正。 您将需要能为技术支持提供从ESA的支持通道。

相关信息

- CSCuo46017 ：SSHv1保持已启用在升级以后，并且不可能禁用
- 思科电子邮件安全工具-最终用户指南
- 技术支持和文档 - Cisco Systems