目录

目标

本文是帮助排除故障/在代码升级以后解决对连结9000的SSH问题。

简介

在我们深潜到SSH问题的原因里，它是必要知道关于以下漏洞(前SSH服务器CBC模式加密启用的已启用& SSH弱MAC算法)影响连结9000平台。

CVE ID ：CVE- 2008-5161 (SSH服务器CBC模式加密启用的已启用& SSH弱MAC算法)

问题说明：SSH服务器CBC模式密码器已启用漏洞(SSH服务器CBC启用的模式密码器)

SSH服务器配置支持密码链块(CBC)加密。这可能允许攻击者从密文恢复明文消息。注意此插件只检查SSH服务器的选项，并且不检查易受攻击软件版本。

推荐的解决方案已知:
禁用CBC模式密码器加密和enable (event) CTR或GCM密码器模式
加密。

参考
008-5161

问题

在升级对7.0(3)I2(1)我们的代码以后无法对SSH连结9000和获得根据错误

解决方案

在无法后的原因对在编码以后7.0(3)I2(1)的升级的SSH连结9000及以后，是弱Cihpers通过CSCuv39937修正禁用。

此问题的长期解决方案将使用安排旧有弱密码器禁用的更新/最新的SSH客户端。

临时解决方案在连结9000可以是跟随弱密码器的添加返回。

注意通过添加旧有密码器返回您使用弱密码器并且安全风险。