无线控制器是否涉及CVE-2008-5161漏洞

wlan安全 **陈铮** 2017-10-10 发表

早期版本涉及该问题，参考开源修改漏洞使用CTR的加密模式代替CBC模式（不需要额外配置命令）

· 问题现象：CVE-2008-5161。
· 问题产生条件：某些SSH服务器/客户端的SSH协议处理错误，包括OpenSSH 4.7p1和可能的其他版本，当使用CBC算法时使远程攻击者更容易恢复一定的明文传输数据。