思科就WLAN软件安全问题提出警告 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/181/2021_2022__E6_80_9D_E7_A7_91_E5_B0_B1W_c101_181606.htm 根据思科公司新近发布的一份 安全 警告，该公司的无线局域网 管理 软件存在“多个缺陷”，其中一个缺陷可以让远程用户以系统管理员的默认密码登录。 警告列出了6个缺陷，而且还表示应急方案只能解决部分缺陷。这些问题属于思科无线控制系统（WCS）中的问题，该软件负责思科基于控制器的WLAN（无线局域网）的 网络 与射频管理、位置追踪、入侵检测和预防。 这些缺陷在 Linux 和Windows版本的WCS中都有发现，主要是3.2及以前版本，不过在版本4.0中也发现了一个缺陷。完整资料在思科网站上都有，还提供了一个PDF版本。 最严重的问题可能要数未知用户名和固定密码问题，利用这一点，远程用户能够获取WCS 数据库的访问权限，而数据库中存储了WCS服务器管理的所有接入点的配置信息，其中包括密钥。有了那些密钥，攻击者便能够对加密后的网络数据进行解密。 攻击者还有可能利用默认系统管理员用户名“ root ”和默认密码“ public ”获得WCS安装的完全控制权。用户在安装或首次登录时不要求更改此密码。思科已提供了该缺陷的一个应急方案。 在一些WCS文件中，用户名和密码是以明文形式出现的。 利用其它缺陷，攻击者能够在运行WCS的文件系统中读写任何位置的数据，在用户的Web 浏览器中执行脚本代码，甚至还能获取WCS的用户名和安装目录的路径。 