利用极点五笔6.0漏洞轻松破解Vista PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/454/2021_2022__E5_88_A9_E7_94_A8_E6_9E_81_E7_c100_454498.htm Windows Vista的一大卖点就是其可靠的安全性，UAC、内置防火墙等功能把Vista打造得如同铜墙铁壁。难道真的不可被攻破吗？其实利用输入法漏洞，无需输入密码，就可以直接以系统管理员的权限登录系统，执行任意操作。如此低级但严重的漏洞到底是如何在Vista上重演的呢？ 出现这样低级的漏洞其实也不能完全怪Vista，存在漏洞的《极点五笔输入法》才是罪魁祸首。问题出在其6.0版本（2007.2.26.0.98）中，当Vista系统安装上该版本的《极点五笔输入法》后，就像两种独立的化学物质，本身不会有反应，但当两者融合在一起的时候，就会产生剧烈的化学反应，低级的漏洞由此诞生。 漏洞触发条件 这个漏洞的危害性很大，但是要触发这个漏洞，也是需要有一定条件的： 条件1：6.0版本（2007.2.26.0.98）的《极点五笔输入法》输入法。这是必要前提，只有该版本的输入法存在此漏洞，最新的版本已经填补了漏洞。此外，Google输入法最初的1.0版本也存在此漏洞。 条件2：系统处于锁定状态。当Vista启动到登录界面时，是不会触发漏洞的，只有当系统处于锁定状态时，漏洞才会被激活。 满足这两点后，我们就可以轻松绕过Vista的密码验证，直接进入系统了。下面我们来对这个漏洞进行测试。 绕过系统验证登录 Step1：假设当前登录界面处于锁定状态下，点击界面左下角键盘状的输入法选择按钮，在出现的菜单中选择《极点五笔输入法》。 Step2：点击一下登录界面的空白处，这时会出现《极点五笔输入

法》的输入法状态条，在上面点右键，在出现的菜单中依次选择“ 输入法设置→设置另存为 ”。 Step3：在登录界面会弹出一个文件保存对话框，在这个对话框中我们可以浏览硬盘中的任意文件，包括创建和删除文件。 Step4：在对话框中操作文件很不方便，况且并不能算是真正的入侵，因此我们可以利用漏洞创建一个具有管理员权限的账户，用这个账户进入系统。 在对话框的地址栏中输入“ c:\windows\system32\net.exe user hacker 123456 /add ”，输入完毕后点击一下旁边的“ 前进 ”按钮，这时会有一个“ 命令提示符 ”窗口一闪而过。虽然登录界面看起来没有什么变化，但我们已经在系统中创建了一个名为hacker，密码为123456的普通账户 Step5：接下来我们将它提升为系统的管理员，再次在地址栏中输入“ net localgroup administrators hacker /add ”并回车，仍旧是一个“ 命令提示符 ”窗口一闪而过。ok，现在我们已经是系统的管理员了，关闭当前的对话框窗口，点击登录界面上的“ 切换用户 ”按钮。接下去请相信你的眼睛，hacker账户已经俨然出现在了登录界面上。下面就不用多说了，用hacker账户登录，在Vista系统中尽情的爽吧。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com