Linux不可读文件被跟踪漏洞Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022_Linux_E4_B8_8D_E5_8F_c103_645365.htm 受影响系统： Linux kernel 2.2.17 Linux kernel 2.2.16 Linux kernel 2.2.15 Linux kernel 2.2.14 Linux kernel 2.2.13 Linux kernel 2.2.12 Linux kernel 2.2.10 不受影响系统： Linux kernel 2.4 描述： ptrace是一个Unix系统调用，通常在断点调试中用于分析运行中的进程，gdb、strace等调试工具都使用了这个系统调用。Linux 2.2.x内核(甚至更早版本的内核)的ptrace实现存在一个漏洞，允许攻击者获取本来无权获取的的敏感信息。 出于安全考虑，普通用户不能使用ptrace()系统调用跟踪分析setuid程序，不能使用上述调试工具关联其他用户启动的运行中的进程。如果二进制文件bar对于用户foo来说不可读(r权限去掉了)，foo用户无权使用ptrace()系统调用跟踪bar程序的执行。 所有这些限制都在ptrace(PT_ATTACH, ...)实现中得到检查。但是，当ptrace()用于跟踪子进程时，未能正确检查安全限制，bar程序对于foo用户可执行，即使不可读，也可按子进程方式跟踪bar程序的执行过程，此时可以观察bar程序的内存映像。恶意用户可能利用这种技术获取敏感信息，本来这些敏感信息通过chmod go-r后防止诸如strings bar一类的窥探。可以利用该漏洞为进一步损害系统安全性做准备。 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