Linux内核SCTP漏洞无大碍不打补丁也可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_ti2020/581/2021_2022_Linux_E5_86_85_E6_A0_c103_581822.htm udev才过，SCTP接踵而来。看看milw0rm上溢出程序的名字就有点恐怖“ Linux Kernel 2.6.x SCTP FWD Memory COrruption Remote Exploit ”，稍加留意会看到exp上有这么一行“ NOTE: you need at least one sctp application bound on the target box “ 。看到这一行，心里放心了不少。因为我们知道SCTP不是一个常用的协议，但在电信网络骨干里会经常见到它。并且绝大多数linux发行版默认也不启用SCTP支持。 所以理论上说要利用这个漏洞就必须满足两个条件： 1、系统默认支持SCTP或者加载sctp LKM。 2、系统有一个sctp用户空间程序监听某个sctp端口。（一般的端口扫描程序无法发现sctp端口。） 但理论归理论，实践才会出真知，对于一个至少是remote dos的漏洞，掺不得一点马虎。我找了个opensuse11.1回来，做了下试验，发现是可以被DOS，但是前提的确是需要满足我上面说的两个条件。 先看看监听sctp协议的sctp_darn程序开放的端口。 在这之后，opensuse就挂起了，但是如果我不运行这个sctp_darn程序， 这个exp是无法导致系统挂起的。如果还不放心，可以执行下面的命令，把sctp.ko删除，放心，你几乎永远都用不上它。rm -f `modprobe -l | grep -w sctp.ko`，最后你可以用lksctp-tools里的checksctp检查下你的系统是否支持sctp。 更多优质资料尽在百考试题论坛 百考试题在线题库 linux认证更多详细资料 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