

Linux内核被发现存重大缺陷 可令电脑被黑

<http://www.sina.com.cn> 2003年12月03日 08:55 [新浪科技](#)

新浪科技讯 安全专家们近日声称发现Linux内核的一个新缺陷，这一缺陷将会使攻击者能够获得接入一台易受攻击的电脑的根使用权继而控制整台电脑。一个不知名的黑客最近利用上述缺陷侵入了数台Debian Project组织的服务器，这才使新的缺陷被人发现。

这一发现使整个Linux家族都受到波及。因为缺陷出现在Linux内核，这实际上已影响了操作系统的各个部分，一些厂商已证实他们的产品非常容易受到攻击。缺陷主要存在于已发布的2.4.0到2.5.69版本的内核中，还好2.4.23-pre7和2.6.0-test6版本已经得到升级。

据赛门铁克公司的分析显示，缺陷本身是因brk()系统调用中的一个整数溢出而产生，而brk()系统调入主要是负责存储管理功能的。当它在调入do_brk()功能时，使用了用户地址和长度变量，但在增加变量时却并不检查整数溢出。

赛门铁克认为，这一缺陷将允许外壳级的本地用户有权使用系统来提高他的权限，直至最高。这样，攻击者就可以随意操纵此台电脑。赛门铁克警告说，新的缺陷能和许多远程漏洞相连接，可使远程攻击者获得根访问权。

红帽(RedHat Inc.)公司和Debian Project对此都发出公告，并提供了解决方案。其他厂商的产品也存在易受攻击的弱点，包括MandrakeSoft、SuSE Linux和Caldera International公司的产品等。

据赛门铁克分析，虽然上述缺陷导致黑客对Debian服务器的攻击收效不大，但这种缺陷攻击的方法显然已在黑客行业当中传播开了。(陈立荣)

[【评论】](#) [【推荐】](#) [【大中小】](#) [【打印】](#) [【关闭】](#)