Linux安全神话破灭：遭遇信任危机出路何在

http://www.sina.com.cn 2003年12月11日 07:56 eNet硅谷动力

【eNews专稿】破碎的安全神话？

2003年12月初，以企鹅为形象代表的Linux世界起了轩然大波。12月1日，开源软件推广机构“Debian计划”警告说，存在于Linux核心中的一个瑕疵帮助攻击者侵入了他们的4台开发服务器，而据称，早在11月9日，就已经出现过几次类似的入侵。一时业界哗然。一向以安全性著称的Linux世界顿时蒙上了一层阴影。此时Linux与SCO的版权纠纷依然还是剪不 断理还乱，Linux此时在内核方面出现漏洞问题，无疑是雪上加霜。而在此前不久，RedHat刚从Linux桌面市场上撤退。

“内核里面存在内存分配方面的漏洞，而这个漏洞没有检测参数，导致恶意攻击的时候，普通用户可以轻易获得超级用户的缺陷。简单说来就是通过普通用户权限，然后再获得超级用户权限。”中科红旗主管研发方面的郑忠源博士如此向记者描述这个漏洞。他对记者表示，这个漏洞非常严重。据媒体报道，因为该漏洞出现在Linux内核本，也就意味着几乎目前发布的所有Linux操作系统版本都存在这一漏洞。其波及面之大、危及内核的程度对于Linux来说可谓是前所未有，也有观察人士认为，Linux的安全性也将遭受前所未有的质疑。

但是一位业内人士告诉记者不同的看法，之所以能够在心理上给予大家如此大的冲击，更多的不是因为Linux的内核存在漏洞，而在于漏洞最早是被黑客进行利用。郑忠源博士也对记者表示出相同的看法，“这个漏洞的危害性体现在大家没有发现之前就被黑客所利用。”对于Linux社区的心理冲击大于实际的安全漏洞所带来的冲击，这是事后业内人士普遍的看法，而对于此次内存分配安全漏洞的本身，在解决方案提供后反而很少有人再去关心。

对于黑客入侵事件本身，记者随机采访了一位Linux的中小企业用户，他对记者表示，对于最近的Linux内核漏洞问题他并没有太大的感受，同时也没有太大的影响，毕竟相对于其他操作系统来说，Linux在他心目中依然是非常安全的操作系统，一两次的入侵事件不会有太大的影响，“毕竟完全安全的操作系统是不可能存在的。”但是，观察人士对记者直言，黑客入侵是一个偶然事件，同时，这种入侵很快被发现也是一个偶然事件，随着Linux使用的普及，这种事件会变得越来越不偶然。

安全性，模式对抗的游戏？

然而，对于Linux的安全性质疑并没有像大家当初所预期的那样成为一个异常火爆的话题，中科红旗的郑忠源博士告诉记者，这是因为大家都已经意识到操作系统的安全性问题永远是一个极具争议的话题，“这里面混杂了太多的误解和商业利益”，许多对于Linux负面的言论未必就是完全符合事实本身的。

而在此前，国内Linux界的老前辈孙玉芳在接受记者采访时也曾对记者表示，操作系统的安全问题永远是一个道高一尺、魔高一丈的问题。郑忠源还对记者透露，在中科红旗跟政府和客户交流的结果来看，大多数人还是接受了这样的观点，他同时告诉记者，事实上，Linux之所以能够有“更安全”的信心，主要是因为Linux拥有一个更为先进的开发和维护模式。

但是，记者发现，目前大多数人更喜欢从已发现的操作系统漏洞的数量方面的评比来衡量一个操作系统是否安全，日前的Linux遭受入侵的尴尬事件也使得对于Linux未来的拷问似乎得到了更多的佐证。对此，郑忠源告诉记者，“‘安全’不是一个静态的事情，而是一个动态的过程”。

目前被大多数人所认可的一个观点是，世界上并不存在绝对安全、毫无漏洞的操作系统，目前Linux也希望向大家普及这样一个观念。但是，另一方面，不是大多数人都接受维护模式的对比，Linux的相关厂商往往需要向客户去解释这方面的事情以打消他们对Linux安全问题的顾虑。一位国内Linux厂商的内部员工告诉记者，在日常的销售中，总有客户会对Linux的开放源码有重重顾虑，认为开放的源码会使得黑客的攻击更为轻易，为此，在销售时总是需要作出许多额外的解释。

不过，很显然大多数国内Linux厂商对此并没有太多的忧虑，在记者的采访中发现，Linux厂商对自己产品的安全性问题都没有太大的担心，郑忠源更是对记者直言，“在BUG的发现和改进速度方面，Linux首屈一指。”他告诉记者，在大的范围内，现在每个Linux厂商都提供了在线升级的功能，对于一些新出现的BUG，大家可以很快的就进行修补工作，而对于Linux来说，其意义不仅仅局限于此，因为这不仅仅时某一个厂商发现问题、修补漏洞，实际上每一个厂商都会独立发现一些BUG，由于开放的模式，使得每个公司都可以去进行修补，也就是说一个公司的成果将会很容易就被其他公司所分享。而这些对于一个单独的公司来说就显得非常有限。一位业内人士对这样的说法表示肯定，并且认为，这也是其他操作系统对手在与Linux较量时所不具备的优势。中科红旗郑忠源更是对记者表示，目前大家比的是发现漏洞的速度和修补漏洞的速度，使操作系统受到攻击的影响尽可能的小。

在记者的采访过程中，一些Linux厂商都表示自己还在不断探索对抗黑客恶意入侵的方法，不断提高自己产品的安全性。一位业内人士更是肯定地对记者表示，Linux的先进开发、维护模式使得Linux的安全性依然牢靠，对于其他操作系统竞争对手而言，Linux最强有力的优势就是开放源码的模式。

走出神话迷雾的未来

一位业内人士如此对记者评述此次黑客入侵事件所带来的影响：软件有漏洞一点都不奇怪，但它会让Linux安全的神话再也无法延续下去了，大家会相信，Linux至少并不比Windows更安全。

对于这次黑客利用Linux内核漏洞进行入侵的事件而言，无论是Linux的支持者还是反对者都难以否定其存在的巨大影响。但是，对于Linux出现漏洞并没有简单的局限在黑客入侵事件本身，大多数厂商都对此事件有了一个重新的认识和反应。

中科红旗郑忠源对记者表示，对于日后的安全性问题，如果出现了内核漏洞，已经带有解决方案的中科红旗不会再去重新做，如果只是有一个漏洞描述，而没有解决方案，中科红旗会尽快发布相关补丁。但是他随后对记者表示，并不是大多数公司都有直接对Linux内核进行修改的能力。

不过一位Linux的技术人员对记者表示，由于Linux在维护模式上的开放性，其对漏洞的解决方案都会很快成为共享，研发能力不会在很大程度上成为一个阻碍。

不过，依然有观察人士对记者直言，随着Linux的逐渐普及，其所遭受的安全方面的质疑一定会与日俱增，但他同时表示，这样的质疑并不会成为Linux进一步普及的阻碍因素。而对于此，有关人士对记者表示，目前操作系统用户苦恼的不是漏洞问题，事实上，真正利用这些漏洞进行攻击的人很少，问题的焦点集中在其他系统问题上，比如说数据丢失等等。另一方面，美林投资公司日前发布报告称，对100位公司CIO所作的调查表明，58%的CIO看好开放源码产品，因为它比微软产品的安全性更好。

作者：金磊