深入浅出分析Linux系统内核漏洞的问题（3） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022__E6_B7_B1_E5_85_A5_E6_B5_85_E5_c103_144397.htm Linux内核中的整数溢出漏洞 Linux Kernel 2.4 NFSv3 XDR处理器例程远程拒绝服务漏洞在2003年7月29日公布,影响Linux Kernel 2.4.21以下的所有Linux内核版本。 该漏洞存在于XDR处理器例程中，相关内核源代码文件为nfs3xdr.c. 此漏洞是由于一个整形漏洞引起的（正数/负数不匹配）。攻击者可以构造一个特殊的XDR头（通过设置变量int size为负数）发送给Linux系统即可触发此漏洞。当Linux系统的NFSv3 XDR处理程序收到这个被特殊构造的包时，程序中的检测语句会错误地判断包的大小，从而在内核中拷贝巨大的内存，导致内核数据被破坏，致使Linux系统崩溃。 漏洞代码： static inline u32 * decode_fh(u32 *p, struct svc_fh *fhp) { int size. fh_init(fhp, NFS3_FHSIZE). size = ntohl(*p ). if (size > NFS3_FHSIZE) return NULL. memcpy(&amp.fhp->fh_handle.fh_base, p, size). fhp->fh_handle.fh_size = size. return p XDR_QUADLEN(size). } 因为此内存拷贝时在内核内存区域中进行，会破坏内核中的数据导致内核崩溃，所以此漏洞并没有证实可以用来远程获取权限，而且利用此漏洞时攻击者必须可以mount此系统上的目录，更为利用此漏洞增加了困难。 我们的目的在于通过这个漏洞的特点来寻找此种类型的漏洞并更好地修补它。大家可以看到，该漏洞是一个非常典型的整数溢出漏洞，如果在内核中存在这样的漏洞是非常危险的。所以Linux的内核开发人员对Linux内核中关于数据大小的变量都作了处理（使用

了unsigned int），这样就避免了再次出现这种典型的整数溢出。通过对这种特别典型的漏洞原理进行分析，开发人员可以在以后的开发中避免出现这种漏洞。 IP地址欺骗类漏洞 由于tcp/ip本身的缺陷，导致很多操作系统都存在tcp/ip堆栈漏洞，使攻击者进行ip地址欺骗非常容易实现。Linux也不例外。虽然IP地址欺骗不会对Linux服务器本身造成很严重的影响，但是对很多利用Linux为操作系统的防火墙和IDS产品来说，这个漏洞却是致命的。 IP地址欺骗是很多攻击的基础，之所以使用这个方法，是因为IP自身的缺点。IP协议依据IP头中的目的地址项来发送IP数据包。如果目的地址是本地网络内的地址，该IP包就被直接发送到目的地。如果目的地址不在本地网络内，该IP包就会被发送到网关，再由网关决定将其发送到何处。这是IP路由IP包的方法。IP路由IP包时对IP头中提供的IP源地址不做任何检查，认为IP头中的IP源地址即为发送该包的机器的IP地址。当接收到该包的目的主机要与源主机进行通信时，它以接收到的IP包的IP头中IP源地址作为其发送的IP包的目的地址，来与源主机进行数据通信。IP的这种数据通信方式虽然非常简单和高效，但它同时也是IP的一个安全隐患，很多网络安全事故都是由IP的这个缺点而引发的。 黑客或入侵者利用伪造的IP发送地址产生虚假的数据分组，乔装成来自内部站的分组过滤器，这种类型的攻击是非常危险的。关于涉及到的分组真正是内部的，还是外部的分组被包装得看起来像内部分组的种种迹象都已丧失殆尽。只要系统发现发送地址在自己的范围之内，就把该分组按内部通信对待并让其通过。 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