Unix/Linux 操作系统安全(五)

卿斯汉 (中科院信息安全技术工程研究中心 100080)

4 Unix 安全漏洞

4.1 arp 问题

影响的系统：SunOS 4.1.x

描述：/usr/etc/arp 能够被用来查看系统内存的内容。

$arp -f /dev/kmem | string >mem,

运行该命令后，会将当前内存的信息写入当前目录下的 mem 文件，通过普通的文本编辑器就可以查看内存的情况。

解决方法：将文件/usr/etc/arp 的可执行权限关闭。

4.2 GUN in.fingerd 问题

影响的系统：运行 GUN in.fingerd(8)1.37 的系统

描述：在 GUN in.fingerd 的 1.37 版本的 lib/site/userinfo.c 模块中有漏洞，该漏洞允许系统上的任何用户以 root 的 gid 身份执行 ~/.fingerc 文件中的命令。

解决方法：升级 in.fingerd，或者安装补丁程序。

4.3 mountd 问题

影响的系统：SunOS4.1.1, 4.1.2, 4.1.3 和 4.1.3c, 不包括 SunOS 4.1.3.u.1

解决方法：升级 in.fingerd，或者安装补丁程序。

4.4 eject 问题

影响的系统：SunOS versions 5.3, 5.4, 5.5, 5.5-x86, 5.5.1,5.5.1-x86，Solaris

描述:在 Solaris 2.4 上的开启 Sun CD-ROM 的程序 eject 有缓冲区溢出漏洞，将导致 用户获取 root 权限。

建议: chmod 555 /usr/bin/eject

4.5 OS fdformat 溢出漏洞

影响的系统: SunOS versions 5.3, 5.4, 5.5, 5.5-x86, 5.5.1, 5.5.1-x86

描述:fdformat是用来格式化磁盘的程序，它导致的溢出漏洞将使用户获取 root 权限。

解决方法：暂无

4.6 Solaris Xsun 缓冲区溢出漏洞

影响的系统: Sun Solaris 7.0-x86, Sun Solaris 7.0 SPARC

描述:Solaris 7 的 X11 服务程序 Xsun 存在一个缓冲区溢出漏洞，它的 -dev 参数是用来设置 Xwindow输出的设备的，但当给它输入一个很长的参数时，将可能使 Xsun 以 root 组权限执行任意代码。攻击者可能利用root组权限进一步获得 root 用户的权限。

临时解决方法：chmod g-s `which Xsun`

4.7 Sun的Java Web服务器远程命令执行漏洞

影响的系统：Solaris；使用 Sun Java Web Server 的所有版本

描述：Sun的Java Web服务器缺省配置存在一个漏洞。使用 Java Web 服务器提供的公告牌示例应用，就有可能在目标机系统上远程执行任何命令。

com.sun.server.http.pagecompile.jsp.runtime.JspServlet 处理 Java Web 服务器的 JSP 页面，它编译 JSP 页面（如果还没有编译）并在 Java 运行时环境中执行它们，然后将结果回送 web 服务器。通过在 URL 中使用 /servlet/ 前缀手工调用这个 servlet 是可能的，然后将它指向 web 服务器上将要编译的任意文件，把它当成 JSP 文件执行。特别是，普通的 HTML 文件也能被编译，然后象

JSP文件那样执行，如果JSP代码能够嵌入HTML文件，就有可能执行服务器上的任意命令。Java Web服务器带有一个示例公告牌应用，它在web文档根目录创建"board.html"文件，然后存储远程用户递送来的消息。公告牌应用可以访问：

http://jws.site/examples/applications/bboard/bboard-frames.html

在公告牌上有一个让用户邮递注释的文本输入区。将要上载的代码需要在这里输入，然后通过单击"Post to Board"按钮上载到"board.html"，如果JSP代码已经递送到"board.html"，就有可能得到编译的代码，并通过引用如下的URL执行：

http://jws.site/servlet/com.sun.server.http.pagecompile.jsp.runtime.JspServlet/board.html

编写一段Java代码，它允许利用Runtime.getRuntime().exec()方法在下面的操作系统上执行任意命令，这是可能的。

解决方法：查阅"How to secure a web site that uses the Java Web Server"中关于JavaWeb服务器部分和下面的Sun's Java Web Server FAQ：

http://www.sun.com/software/jwebserver/faq/jwsca-2000-02.html

这两个文档都描述了锁定并加强（lock down and harder）Java Web服务器的详细步骤，简单地删除示例目录下的例子就能够解决问题，这在两个文档里都有描述。

4.8 Qualcomm POP Server 2.4 缓冲区溢出漏洞

影响的系统：Linux；*BSD；SCO

描述:在版本低于2.5的Qualcomm的qpopper程序中包含有一个缓冲区溢出漏洞，有可能导致远程攻击者在运行了该版本的qpopper的主机上执行任意命令。Qpop没有正确检查用户输入的pop命令的长度,比如USER,PASS等等。用户可能提供一个超过1024字节长的命令导致缓冲区溢出。

解决方法：升级到最新的QPOP版本.下载地址：ftp://ftp.qualcomm.com/

4.9 UnixWare 7 问题

影响的系统：SCO UNIX+UnixWare 7

描述：SCO UnixWare 7 的su命令在进行用户名(via argv [1])处理时没有进行适当的边界检查，因此当使用一个超长的用户名时产生了溢出。

SCO UnixWare 7 的xlock命令在进行用户名(via argv [1])处理时没有进行适当的边界检查，因此当使用一个超长的用户名时产生了溢出。

SCO UnixWare 7 的Xsco命令因为没有进行适当的边界检查，当使用一个超长的参数(argv [1])时产生了溢出问题。同时因为Xsco是以超级用户的权限来运行，因此通过溢出程序可以获得更高的权限。

UnixWare 7.1 的libc中存在一系列漏洞。gethostbyname()中存在的一个缓存溢出可以让任何用户提升自己的权限。

Unixware 7.1 中的一些包install/removal程序可以读取系统中的任何文件，并没有考虑其权限设置。原因是这些包命令(pkginfo，pkgcat，pkgparam等等)扩展了访问权限。

解决方法：以上问题暂无解决方法

4.10 Communigate Pro Web Admin 拒绝服务

影响的系统：使用 Stalker Communigate Pro 3.1

描述:Communigate Pro 3.1 在远程管理中存在漏洞，可以造成远程拒绝服务问题。连接到8010口（web admin port）发出70000个字符到缓冲区，再连接到服务器的其他口上时，会造成服务器崩溃。

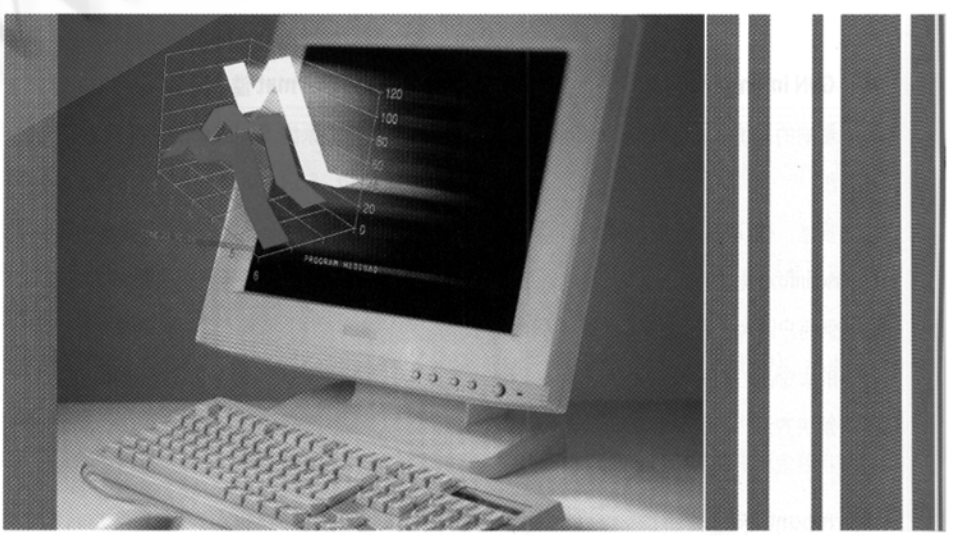
解决方法：Stalker Communigate Pro 3.2, 3.2b5 和 3.2b7 已经修复了这个漏洞：ftp://ftp.stalker.com/pub/CommuniGatePro/

4.11 /bin/doctor 安全漏洞

影响的系统：SCO openserver 5.0.5；SCO openserver 5.0.4

描述:SCO openserver中/bin/doctor缺省属主是root，并且被设置了setuid位，Bugtraq中已经有人报告说普通用户可以通过doctor提供的菜单以root身份执行任何命令.但只有在root运行doctor进行一些必要的设置后,普通用户才可以访问到它的菜单.因此,如果root没有运行过doctor,普通用户就不能利用这个漏洞.但lgwu发现doctor存在一个更严重的漏洞,doctor的-s参数允许任何用户在命令行运行一个shell脚本.因此,普通用户可以轻易得到root权限。另外,如果用任意的系统文件做-s的参数,该文件的第一行将被显示。

临时解决办法：chmod 700 /bin/doctor



4.12 SNMPd 缺省通信字安全问题

影响的系统: SCO OpenServer 5.0.5

描述: SCO OpenServer缺省配置允许本地用户通过一个缺省的可写通信字获取SNMPd的读/写权限。本地用户可能会据此获得更多的权限甚至控制系统。

SCO OpenServer 5.0.5 的 SNMPd 守护程序缺省配置了一个可写通信字(private)，它允许任何本地用户获得对SNMPd设备的全部管理员权限。这些权限包括修改主机名、网络接口状态、IP转发和路由、网络套接字状态（包括关闭TCP会话和监听套接字）和ARP缓存，同时攻击者拥有对所有 SNMP 属性的读权限。

解决方法：通信字在/etc/snmpd.comm文件中定义。删除或修改这些通信字并重启 SNMPd 守护进程。如果主机不需要 SNMP，建议杀掉 SNMPd 进程和将其从系统启动文件中清除。

4.13 Tru64 V5.1 inetd 的 DoS 漏洞

影响的系统：Compaq's Tru64 UNIX V5.1

描述：Compaq's Tru64 UNIX V5.1 中发现了一个潜在的安全漏洞，它存在于 inetd 程序之中，可以使它停止接收连接。这导致 inetd 处理的所有服务不可访问，包括ftp, telnet, rsh, rlogin, rexec, pop3, imap, radius, 等等。

这个问题只存在于 Tru64 UNIX 5.1 inetd 之中。/usr/sbin/inetd 是许多服务的管理幽灵程序。inetd可能停止响应请求，如果它的一个服务在启动后发生 core。但 inetd 会继续运行。netstat -An 命令可能显示许多连接到相同PCB的链接。如果你正在 Tru64 UNIX 5.1 上安装 Open Source Internet Sollutions，强烈建议你安装这个补丁包。如果你正在Tru64 UNIX 5.1 TruCluster 系统上安装 Open Source Internet Sollutions，你必须在安装 Open Source Internet Sollutions 之前安装这个补丁包，因为没有它，inetd失败会导致安装失败，这主要是由于它会和intra-cluster通信相互干扰。

解决方法：Compaq Tru64 UNIX 工程师已经为这个问题提供了一个补丁。但是在 Compaq 的补丁站点没有。如果需要，可以和 Compaq Services support channel 联系，使用 SSRT0708U 请求补丁。

4.14 Lotus Domino Server 5.0.1 ESMTP 缓冲区溢出漏洞

影响的系统: 使用 Lotus Domino Enterprise Server 5.0.1 的系统

描述: Lotus Domino Server 5.0.1 的 ESMTP 服务程序有没有缺乏对用户输入进行合法性检查，因而存在一个缓冲区溢出漏洞。当 ESMTP server 接收到一个 ´from´ 命令时，若它带的参数长度超过 4k, Lotus Domino Server 就会崩溃，必须重新启动才能恢复正常工作。

攻击者也可能远程获取服务器的管理权限。

解决方法：暂无

4.15 HP-UX 的 ftpd 漏洞

影响的系统：HP-UX release 11.00 - 存在下面描述的两个问题;

HP-UX release 10.20 - 只存在下面描述的第二个问题：setproctitle()。

描述：HP－UX 上的 ftpd 存在两个问题：

(1) ftpd处理SITE EXEC命令时允许远程用户获得根访问权。这只在 HP－UX 11.0 的 ftpd 缺省配置中才成为可能。

(2) ftpd不能正确格式化setproctitle()函数的参数，导致用户得到根访问权，11.0和10.X中都有这个问题。

解决方法：安装临时二进制文件直到发布正式补丁。只要简单地将该文件替换原来的二进制文件即可，两个临时的ftpd二进制文件（用于HP－UX 11.0 和 HP-UX 10.20）位于：

ftp://ftp.cup.hp.com/dist/networking/ftp/ftpd.11.0

MD5: AF10975274481D5E2839F860CB9F3D77

cksum(1): 646427018 151552

ftp://ftp.cup.hp.com/dist/networking/ftp/ftpd.10.20

MD5: E6024191E3EA8E3000B7E73F4111138E

cksum(1): 3969082595 90112

ftp://ftp.cup.hp.com/dist/networking/ftp/ftpd.10.00-10.10

MD5: 1EE2AE4CC4476B60CE736E8094642E46

cksum(1): 2137777529 86016

4.16 HP-UX 的 bdf -t 选项缓冲溢出漏洞

影响的系统：HP-UX

描述：bdf 是报告自由磁盘块数目的程序（Berkeley 版本），-t选项指定文件系统的类型，如 nfs，hfs 等。bdf 程序有 SUID 许可权，利用 -t 选项指定一个长字符串时，如果长度大于 2415 个字符，bdf就会发生段错误。也许，bdf 没有检测字符串边界。

解决方法：目前还不知道。

4.17 glibc 域名解析 ID 可以预测

影响的系统: GNU glibc 2.1.3, 2.1.2, 2.1.1, 2.1, 2.0; BIND 8.2.2-p5

描述:在glibc 2.1.3的域名解析函数中存在一个问题，它使用主机的时间信息与进程id一起产生一个随机ID，这个ID是相当容易猜测的，而且glibc会丢弃那些不匹配的ID,理论上允许攻击者暴力猜测DNS ID.这个ID是用来校验主机收到的DNS信息是否真的是从正确的DNS服务器发来的。如果可以预测这个ID号，攻击者就有可能伪造返回的查询信息，或者执行一些其他的DNS攻击。

问题代码如下:

```
u-int
res-randomid()
{
struct timeval now;
--gettimeofday(&now, NULL);
return (0xffff & (now.tv-sec ^ now.tv-usec ^
--getpid()));
}
```

这段代码也同样出现在BIND 8.2.2-p5 src/lib/resolv/res_init.c 中，因此这个问题并不仅仅是glibc 的问题。

解决方法：暂无。

4.18 Bind 漏洞导致域名服务器流量增大以及 NS 查询"路由"被发现

影响的系统: 使用 ISC BIND 8.2.2, ISC BIND 8.2.1, ISC BIND 8.2,ISC BIND 8.1.2, ISC BIND 8.1.1, ISC BIND 8.1, ISC BIND 4.9.7-T1B, ISC BIND 4.9.7

描述：很多 DNS 服务器的缺省设置存在一个漏洞，可能导致拒绝服务攻击。如果一个域名服务器允许远程主机向它查询其他域(它本身并不管理这些域)的域名，就是所谓允许递归查询，就可能导致网络流量的异常增大。单个主机引起的流量增大可能并不能导致拒绝服务攻击的产生，但是利用DNS的分级方式的弱点，可能引发对单个站点的大量数据流量，阻塞正常的网络交通服务。

这个问题出在当域名服务器收不到某域权威服务器的域名解析应答时的处理方式上。当域名服务器接收到一个域名解析请求时，它往往会转发给上一级的DNS服务器.如果这个查询请求不能被解析，因为其权威域名服务器上没有启动DNS服务或是没有应答,每个转发的服务器将会试图自己解析，通常会重试三次（分别在0秒，12秒，24秒时）甚至更多。在这种情况下，该域名所在网络的流量就明显增大了。通过使用大量的域名服务器做这种查询，可能导致向目标网络发送大量数据,造成拒绝服务攻击。攻击者也可利用这种漏洞来发现目标网络的域名查询的路线。

解决方法：禁止来自其他主机的递归查询，只允许从信任主机或网络查询可以避免使你的主机成为这种攻击的工具。对于被攻击的主机，没有很容易的方法来使其免遭攻击,对于没有运行DNS服务器的主机,应过滤掉所有流向它们的53号端口的数据包,但这只能使这种类型的包不能到达防火墙后，这些包仍然会占用你的带宽。另一种可能的方法是,在正受攻击的主机上建立一个假的DNS server,对于所有的查询都应答一些虚假信息。

4.19 IBM AIX文件系统漏洞导致用户越权访问文件

影响的系统: IBM AIX(r) versions 3.2.x, 4.1.x, 4.2.x, 4.3.x

描述: IBM AIX系统在文件系统处理中存在安全漏洞，本地或者远程攻击者可以访问通过NFS mount的文件系统中的某些文件，并对这些本来不属于他们或者本来不该能访问的文件拥有读写权限。

解决方法: IBM已经提供了针对这个漏洞的补丁，您可以在下列地址下载: http://techsupport.services.ibm.com/rs6k/fixes.html，补丁名称与系统版本的对应关系如下:

AIX 3.2.x: APAR IY10111

AIX 4.1.x: APAR IY10031

AIX 4.2.x: APAR IY10001

AIX 4.3.x: APAR IY09941

另外，对于AIX 4.3.2系统IBM提供了一个紧急修复文件，可以在下列地址下载：ftp://aix.software.ibm.com/aix/efixes/iy09941

(全文完)

* 注：关于Linux安全漏洞，因篇幅太长(将近30页)本刊略，有兴趣的读者可与编辑部联系。