

```
nt "\nServer returned an ADO misconfiguration message\nAborting.\n",
b content_start{ # this will take in the server headers my (@in)=@_ ; my $c;for ($c=1;$c<500;$c++){ if($in[$c] =~ /\x0d\x0a/){if ($in[$c+1]
/HTTP/1.[01] [12]00/){ $c++; }else{ return $c+1; }}return -1;}# it should never get here actually
my (@in)=@_ ; my $error=odbc_error(@in);if($error=~ /ADO could not find the specified provider//)
my (@in)=@_ ; my $error=odbc_error(@in);
```

漏洞攻击防范实例配套手册

数百种最新漏洞利用方法 让你随心所欲……



漏洞终极攻防战



著名「中国鹰盟」创始人

万涛

主编

体验炸毁OO快感

抢夺聊天管理权

一把把电脑变肉机

控制网站「走后门」

清除漏洞保权限

对Dos攻击说NO!

FTP主机转个遍

让Word「自动工作」

修改ROOT空密码

邮件服务信息防泄漏



电脑报



山东电子音像出版社出版

漏洞攻击防范实例配套手册

漏洞终极攻防战

山东电子音像出版社出版

```
my (@in)=@_ ; my $error=odbc
sub content_start{ # this will t
=~/'HTTP/1.[01] [12]00/({ $c+
Da/){if ($in[$c+1]=~/\'HTTP/1.[01] [12]00/({ $c++; }else{ return $c+1; }}return -1; }#
if($error=~'/ADO could not find the specified provider/){
server headers my (@in)=@_ ; my $c;for ($c=1;$c<500;$c++){ if($in[$c] =~/\x0d\x0a/){if ($in[$c+1]
rn $c+1; }}return -1; }# it should never get here actually
```

内容简介

计算机中存在大大小小,花样百出的漏洞。这些漏洞小则导致系统崩溃,大则导致非法用户以有机可乘,掌握计算机的控制权,从而给计算机的使用者带来不可估量的损失。那么漏洞究竟是什么?究竟有哪些漏洞?利用这些漏洞困难吗?如何才能封堵自己计算机上的漏洞?在书中我们将会给你明晰的答案。

注:本手册只从技术角度讨论漏洞,不得利用本手册所介绍内容进行不法活动。违者将受到法律制裁,于本社无关。

光盘运行环境

CPU 主频	PII 500 以上
分辨率	800×600 像素以上
内存	32M 以上
显存	8M 以上
光驱	8 倍速以上
操作系统	Win9x/2000/XP

光盘内容简介:中国安全教育网独家授权自创经典黑客歌曲。

扫描软件视频录像全辑——让你轻松学会扫描各种漏洞!

漏洞攻击防范实例

配套手册

策 划:大众网络报社

制 作:山东翔宇软件开发中心

责任编辑:刁 戈

特约编辑:乔康毅 王 洁

作 者:候成岗

出版发行:山东电子音像出版社

装帧设计:敬 婕 朱 艳

光盘定价:19.8 元(本手册随盘赠送)

第一章 软件漏洞

第一节 聊天软件

- 一、QQ 大字体导致程序崩溃 3
- 二、利用 QQ 漏洞将自己添加为好友 5
- 三、利用漏洞加任意号码到 QQ 好友中 6
- 四、MIRC DCC SEND 缓冲区溢出让 MIRC 受到影响 7
- 五、危险的 MIRC DDE 安全权限漏洞 8
- 六、MIRC IRC URL 缓冲区溢出 9
- 七、危险的 AOL Instant Messenger 拒绝服务攻击漏洞 10
- 八、利用 ICQ 漏洞自动增加用户 11
- 九、MSN Messenger 控件存在缓冲区溢出漏洞 13
- 十、Yahoo!Messenger 文件传送导致缓冲区溢出 14
- 十一、腾讯聊天室昵称字符未过滤导致 ID 混乱 15
- 十二、ichat 聊天室的 SQL injection 漏洞泄露管理员密码 16
- 四、LeapFTP 客户端 PASV 应答远程缓冲区溢出漏洞 24
- 五、Lftp Try_Netscape_Proxy 远程缓冲区溢出漏洞 26
- 六、Lftp Try_Squid_Eplf 远程缓冲区溢出让黑客进出自如 29
- 七、WS_FTP 配置文件 ws_ftp.ini 文件口令弱加密漏洞 31
- 八、WS_FTP Pro 远程缓冲区溢出漏洞 32
- 九、Sun Microsystems Solaris FTP 客户端调试模式密码显示漏洞 33

第三节 浏览器漏洞

- 一、Microsoft IE 6.0 处理 HTTP 编码不正确漏洞 34
- 二、IE 5.0!externalNavigateAndFind()漏洞 35
- 三、Microsoft Internet Explorer file.writeline 本地文件可写漏洞 36
- 四、Microsoft Internet Explorer 未明远程破坏漏洞 37
- 五、Microsoft Internet Explorer 多个安全漏洞 38
- 六、Microsoft IE5 XML HTTP 重定向错误 39
- 七、IE5 vnd.ms.radio URL 漏洞 40
- 八、Microsoft IE 安全区域设置漏洞 41
- 九、IE 5 绕过“多帧安全机制”漏洞 42
- 十、微软 IE 浏览器访问本地资源漏洞 43

第二节 上传下载软件漏洞

- 一、可怕的 FlashFXP PASV 应答远程缓冲区溢出 19
- 二、FlashFXP 客户端主机名远程缓冲区溢出漏洞 20
- 三、CuteFTP 超长旗标(banner)远程缓冲区溢出漏洞 22

目录

contents

十一、IE5.01 和 Access 2000 执行 VBA 代码漏洞	44
十二、IE 5.01/5.5 DHTML 远程文件读取漏洞	45
十三、微软 IE 和 OE 执行 XML 样式表中的活动脚本的漏洞	46
十四、Netscape 客户端探测工具插件本地缓冲区溢出漏洞	48
十五、Netscape 浏览器 Document.Write 方法交叉域策略漏洞	49
十六、Netscape 样式表远程拒绝服务攻击漏洞	50
十七、Netscape Email 客户端删除消息不完全漏洞	51
十八、Mozilla 浏览器 Browser 交叉域冲突漏洞	51
十九、Mozilla 浏览器 POP3 Mail 处理程序整数缓冲区溢出漏洞	53
二十、Mozilla 浏览器 XMLHttpRequest 文件泄露漏洞	54
二十一、Opera Web Browser Opera: URI 处理器目录遍历漏洞	55

二十二、Opera 浏览器 IFRAME 区域限制绕过漏洞	57
二十三、LiveConnect JavaScript 远程拒绝服务攻击漏洞	58
二十四、Opera 7.10 远程拒绝服务攻击漏洞	59

第四节 办公软件漏洞

一、Microsoft Word Macro 名处理缓冲区溢出漏洞	60
二、微软的 Word/Excel 漏洞可泄露文件内容	63
三、Microsoft Word 中的缺陷可使宏自动运行漏洞	64
四、Out Look Express 错误的 MIME 头漏洞	66
五、Out Look Express XML 存在文件附件脚本远程执行漏洞	69
六、Microsoft Outlook 和 Outlook Express 远程任意程序执行漏洞	70

第二章 系统漏洞

第一节 Windows 系统漏洞

一、Windows 9X 的/con/con 设备名称解析导致系统崩溃	75
二、共享密码校验漏洞让电脑的大门打开	77
三、Windows 98/ME 屏保密码绕过漏洞	80
四、Windows 2000 简体中文版输入法让电脑被控制	81

五、Windows 2000 按键崩溃干扰用户使用电脑	88
六、IPC\$弱口令漏洞打开电脑共享通道	89
七、WorkStation 服务缓冲溢出允许执行代码	96
八、WindowsNT & Windows2000 权限提升漏洞	101

九、Windows 2000 Fat32 磁盘格式普通用户
权限提升漏洞 102

十、Windows Locator 服务存在远程缓冲区溢
出漏洞 103

十一、Windows 2000 Telnet 超时产生拒绝服
务漏洞 107

十二、Windows 2000 索引服务的文件验证漏洞
109

十三、RPC 接口远程任意代码可执行漏洞 110

十四、Windows 2000/XP RPC 服务远程拒绝
服务攻击 112

十五、SharedDocs——XP 默认共享漏洞让你
门户大开 114

十六、快速账号切换功能造成账号锁定 116

第二节 RedHat 漏洞

一、Linux netkit in.telnetd 远程溢出获得 root
权限 117

二、file(1)命令漏洞让骇客执行任意代码 119

三、Linux kernel do_brk()参数边界检查不充
分漏洞 121

第三节 HP-UX 系统漏洞

一、HP-UX 系统 FTPd 格式字符串远程溢出
漏洞 122

二、HP-UX SNMP 守护进程存在漏洞使用本
地攻击者能获得管理员权限 123

三、HP-UX NLSPATH 环境变量权限提升漏洞
125

四、HP-UX dtprintinfo 缓冲溢出漏洞 126

五、HP-UX rwrite 本地缓冲区溢出漏洞得到
权限 128

六、HP-UX rexec 本地缓冲区溢出漏洞 129

第四节 FreeBSD 系统漏洞

一、FreeBSD 系统进程隐藏可绕过漏洞 130

二、FreeBSD 系统 .login_conf 漏洞 132

三、FreeBSD 系统 fpathconf 文件描述符泄露
导致拒绝服务攻击或权限提升 134

四、BSD 内核 exec 调用处理不当可让骇客得
到 root 权限 135

五、FreeBSD 系统 rmuser 密码泄露漏洞 137

六、FreeBSD 系统-SA-00:77 procfs 文件系
统存在多个安全漏洞 137

七、FreeBSD-SA-00:58 chpass 程序格式串漏洞
139

八、FreeBSD-SA-00:54 fingerd 泄漏系统文件
140

九、BSD/Linux telnet 缓冲区溢出漏洞 141

十、FreeBSD 系统 ncurses 缓冲区溢出漏洞 142

十一、FreeBSD 系统 Asmon/Ascpu 安全漏洞
143

十二、FreeBSD 系统 Wmmon 漏洞 144

十三、FreeBSD 系统 Seyon setgid dialer 漏洞
145

十四、FreeBSD 系统 gdc 符号连接漏洞 145

十五、FreeBSD 系统 3.3 seyon 漏洞 146

第五节 Solaris 漏洞

一、Sun Solaris 网络接口拒绝服务缺陷 147

二、Sun Solaris 实时连接器漏洞 150

三、Sun Solaris 网络接口拒绝服务漏洞 151

第三章 服务器漏洞

第一节 WEB 服务器

一、危险的扩展 unicode 解码漏洞	155
二、Windows 2000 ntdll.dll WebDAV 接口远程缓冲区溢出漏洞	159
三、IIS ISAPI Printer 远程溢出漏洞	162
四、IIS 的 index server .ida/.idq ISAPI 扩展存在远程缓冲溢出漏洞	165
五、IIS CGI 文件名错误解码漏洞	169
六、MSADC 执行本地命令漏洞	170
七、IIS 的 INDEX SERVER 服务存在泄露信息的.htw 漏洞	172
八、IIS4.0/5.0 特殊数据格式的 URL 请求远程 DOS 攻击	173

第二节 FTP 服务器

一、Serv-U FTP Server 远程/本地提升权限缺陷	174
二、IPSwitch WS_FTP Server 资源耗竭远程拒绝服务攻击漏洞	175
三、IPSwitch WS-FTP 匿名 FTP 命令缓冲区溢出漏洞	176
四、IPSwitch WS_FTP Server 被动模式会话劫持漏洞	178
五、IPSwitch WS_FTP Server FTP 命令远程缓冲区溢出漏洞	179
六、IPSwitch WS_FTP Server v2.0.3 缓冲区溢出漏洞	181
七、Dynu FTP 服务器存在目录遍历漏洞	182

八、Dynu FTP 服务器缓冲区溢出导致文件泄密	183
九、WZDftpD FTP 服务器畸形 PORT 命令远程拒绝服务攻击	184
十、WZFTPD DoS 漏洞	185
十一、Xlight FTP 服务器存在缓冲溢出缺陷	187
十二、Xlight FTP 服务器存在目录遍历/DoS 缺陷	189
十三、Nite Server FTPD 远程目录遍历偷取文件	189
十四、Meteor FTP Server USER 命令内存破坏漏洞	191
十五、Platinum FTP Server 命令行参数格式串处理漏洞	192
十六、AppleShare IP FTP Server RMD 命令远程拒绝服务漏洞	193
十七、Wu-FTPD 错误配置路径导致通过 SITE EXEC 可执行系统命令漏洞	193
十八、WFTPD v240 FTPServer 远程溢出漏洞	195
十九、ExpressFS 2x FTPServer 远程溢出漏洞	196
二十、Gene6 G6 FTP Server 缓存溢出造成的拒绝服务漏洞	196
二十一、glFtpD 服务器漏洞	197
二十二、PowerFTP 远程拒绝服务攻击漏洞	198
二十三、Broker FTP 服务程序远程文件泄露漏洞	200
二十四、Broker FTP 服务程序远程缓冲区溢	

出漏洞	200
二十五、Platinum FTP Server 目录遍历漏洞	201
二十六、BisonFTP 远程信息泄露漏洞	202
二十七、Xynph FTP Server 相对路径目录遍历漏洞	203
二十八、Netscape Professional Services FTP Server chroot 漏洞	204

第三节 邮件服务器漏洞

一、IPSwitch iMail Web 日志服务 HTTP POST 远程拒绝服务攻击漏洞	206
二、Ipswitch iMail 7.04 存在多个安全问题	207
三、IPSwitch iMail 6.x 的附件漏洞	210
四、IPSwitch iMail 服务器拒绝服务漏洞	211
五、WebEasyMail SMTP 服务远程格式串溢出漏洞	212
六、WebEasyMail POP3 服务合法用户名远程信息泄露漏洞	213
七、MERCUR Mailserver Control-Service 存在缓冲溢出漏洞	213

第四节 数据库服务器漏洞

一、MS SQL 服务器空密码配置错误漏洞	215
二、Microsoft SQL Server 2000 Resolution 服务远程栈缓冲区溢出漏洞	216
三、Microsoft SQL Server Agent 作业提交漏洞	218
四、Microsoft SQL Server 有名管道文件名本地权限提升漏洞	220

五、Microsoft SQL Server/MSDE 扩展存储过程远程缓冲区溢出漏洞	221
六、Microsoft SQL Server xp_dirtree 远程缓冲区溢出漏洞	222
七、MySQL 默认配置存在空 ROOT 密码	223
八、MySQL COM_CHANGE_USER 功能口令认证缺陷漏洞	225
九、MySQL 超长 Password 字段缓冲区溢出漏洞	227
十、MySQL GRANT 权限可改变任意用户口令	228
十一、MySQL AB ODBC Driver 明文储存口令漏洞	230

第五节 流媒体服务漏洞

一、Microsoft Windows Media Services NSIISlog.DLL 远程缓冲区溢出漏洞	231
二、Real Server 8.0 缓冲区溢出漏洞	234
三、Real Networks Helix Universal Server 远程缓冲区溢出漏洞	236
四、Apple QuickTime Content-type 上存在远程缓冲溢出漏洞	238

第六节 脚本漏洞

一、Dvbbs5.0 论坛 Cookie 可利用漏洞	244
二、Dvbbs 免费版未过滤关键字漏洞	245
三、Cookie 漏洞的两大利用总结	246
四、SQL injection——SQL 注射漏洞攻击	247
五、BBSXP 论坛的破解口令漏洞	248
六、Dvbbs6.0 跨站脚本漏洞	250
七、Dvbbs 可随意移动文件漏洞	251

MS66/05

目录

contents

八、雷傲删除文件操作漏洞	254	十八、Discuz! 论坛个人属性及附件的两个欺骗漏洞	268
九、BBS3000 DoS 漏洞	255	十九、LB5000 post.cgi 文件过滤不足漏洞	269
十、BBS3000 在线注册 DoS 漏洞	256	二十、LB 论坛所有版本的跨站脚本漏洞	271
十一、BBS3000 Cookie 泄密漏洞	257	二十一、LB5000 search.cgi 隐式输入漏洞	272
十二、BBS3000 bbs.cgi 文件变量未过滤漏洞	258	二十二、DCP-Portal 未过滤用户变量漏洞	273
十三、BBS3000 favoritecgi 文件变量未过滤漏洞	259	二十三、VBB 图像连接跨站脚本漏洞	274
十四、BBSXP friend.asp 未过滤特殊字符漏洞	259	二十四、VBB session 劫持漏洞	275
十五、BBSXP faction.asp 未过滤特殊字符漏洞	260	二十五、紫桐汉化论坛的重大漏洞	276
十六、BBSXP 最新版的若干漏洞	262	二十六、PHP-Nuke mailattach.php 文件上传漏洞	276
十七、Discuz! 论坛短消息未限制发送次数漏洞	267	二十七、PHP-Nuke admin.php 用户验证漏洞	278

```
~\x0d\x0a/){if ($in[$c+1]=~/HTTP\/1.[01] [12]00/){ $c++; }else{ return $c+1; }}return -1;}#  
b content_ in the server headers my (@in)=@_ ; my $c;for ($c=1;$c<500;$c++){ if ($in[$c] =~/\x0d\x0a/){if ($in[$c+1]=~/HTTP\/1.[01] [12]00/){  
++; }else{ return $c+1; }}}return -1;}# it should never get here actually  
Y (@in)=@_ ; my $error=odbc_error(@in);if($error=~/ADO could not find the specified provider/){
```

第一章 软件漏洞

第一章要讲到的是漏洞篇中最常见的软件漏洞。众所周知,软件是我们平时上网用得最多的东西,像聊天用的软件:QQ、MSN等,浏览网页要用浏览器软件:Internet Explorer、Netscape等,上传网页要用到上传软件:Cutftp、Leapftp等。它们虽然给我们带来了很大的方便,但是都有漏洞存在,大多数漏洞可以导致入侵者直接进入我们的电脑,破坏我们的数据。那么我们经常使用的这些软件到底漏洞在哪里呢?在这一章中,就为大家依次分析一些危险大、传播广的软件漏洞,好让大家在懂得其危害的同时,采取措施防范漏洞。

第一节 聊天软件

说到聊天,我估计在坐的每一个朋友都经历过吧!先不说早期网络上流行至今的IRC,就拿目前国内的一些娱乐站点的聊天室,飞速发展的即时通讯软件(例如:QQ、MSN等)来说,就可以看出聊天在我们网络生活中占有多大的份量。

这些聊天软件在方便我们与朋友交流、与家人联系、与同事工作的同时,难道真的就是那么尽如人意吗?其实不然,相当一部分聊天软件都存在漏洞。这些漏洞轻则导致系统不能正常使用,重则导致机密文件泄露或是系统崩溃。到底这些聊天软件的漏洞危害在哪里?我们大家又如何防范?在这一节,大家将会全面接触到。

一、QQ 大字体导致程序崩溃

漏洞概述:大家知道,理论上在QQ中最大只能发送22号大的文字给对方,但实际上可以突破这种限制发送任意大的字给对方,这时候QQ会调用Riched20.dll文件,而该文件存在一个缓冲区溢出漏洞。就是这个漏洞可导致使用此DLL模块相应功能的应用程序崩溃。经分析得出结论,当字体大小数字串长度超过32字节时,就会引发缓冲区溢出,当超过34字节以后就有可能导致应用程序崩溃。

适用环境:QQ2000c、QQ2003、QQ2003II和QQ2003III测试版

攻击原理:相信大家知道,在QQ中最大只能发送22号的字体给对方,有没有别的办法让我们突破这种限制发送任意大的字号或图形给对方呢?答案是有!这就是本文所要讲的一个关于“大字体导致缓冲区溢出漏洞”。下面告诉大家该怎样做。首先,要求接收方使用最新版的QQ,发送方可以使用任意版本的QQ,在QQ好友名单中选定一个好友的头像,选择“收发消息”,在出现的“发送消息”窗口,输入如下字符串:

```
{\urtf\deflang2052{\fonttbl{\f0\prq2\ a comic sans ms;}{\f1\ a 宋体}}
{\colortbl ;\red250\green50\blue199;\red20\green230\blue100;\red250\green180\blue0;\red100\
```



图 1-1

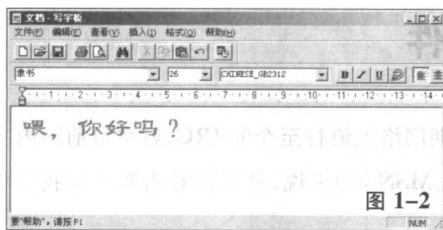


图 1-2



图 1-3



图 1-4

```
green200\blue250;)\pard\cf1\fs100 Hap\cf2\fs80 Py  
n\cf3\fs50 eW y\cf4\fs120 eaR\cf0\fs18 \par }
```

点击“送讯息”按钮，对方就会收到特大的一行文字：**Happy new year**(如图 1-1)，不但字母大小不一，而且每一个字的颜色都不一样！你的 QQ 好友一定会惊喜不已，因为在正常的情况下对方是不会收到这么大的文字的！

那么如何得到以上代码呢？这是用写字板和 16 进制文件编辑器 UltraEdit-32 得到的。首先，在 Windows 自带的写字板中输入你想发送的内容并编辑这些内容，比方说你可以在写字板中选择字体为隶书，然后给每一个要发送的字选择不同的颜色，要发送的内容的大小也可以在写字板中选择，在文号下拉列表框中填入你想发送的字符的大小即可（如图 1-2）。

然后在写字板的“文件”菜单中选择“另存为”，在“保存类型”下拉列表框中找到“Rich Text 格式 (RTF)”，将其保存为 RTF 文件即可（如图 1-3）。

现在，运行 UltraEdit-32，用它打开这个编辑好的 RTF 文件，你会看到这个 RTF 文件的内容就是我们上面输入的那些代码！

在通常情况下，最上面的一行代码“{\rtf1\ansi\ansicpg936\deff0 {\fonttbl {\f0\fnil\prq2 comic sans ms;}{\f1\fnil\charset134 \cb\ce\ce\ce5;}}”不能起到作用，把它改成以下代码“{\urtf\deflang2052{\fonttbl{\f0\prq2\comic sans ms;}{\f1\宋体}}”，这样，所有版本的 QQ 就都能接收到你发的超大型文字了。包括 QQ2003III 系列的最新版本。

把所有的代码写到 QQ 中，然后发给你的朋友，对方就会看到你精心准备的这些内容！如果你想临时改变发送文字的大小，可以在 QQ 中将上面那些代码“\pard\cf1\fs100 Hap\cf2\fs80 Py n\cf3\fs50 eW y\cf4\fs120 eaR\cf0\fs18 \par }”中任何一个“fs”后面的数值改成你所要的大小即可。如果想再简单一点，可以直接在 QQ 的信息栏中在上面这一行代码中修改你想要发的文字。按照这个原理和方法，不仅能发送文字，还可以发送特殊字符，效果非常好（如图 1-4）。

防范方法:使用 **QQ2003III** 系列的新版本 **QQ** 不会受此漏洞影响,你可以把给你发送这种恶意代码的人加入到“黑名单”中,这样他就没法骚扰你了。或者在“好友个人设定”标签中,找到“不接收该好友发来的任何消息”,在前面打上“√”,也可以防范对方发送这样的代码给你,或者可以在 <http://hacker.popunet.com/download/ms-qool.RAR> 下载相



步骤2 接下来再把这个“坏人”(即自己的QQ号)拖到“我的好友”组中去,这时候会出现系统消息,XXXX请求身份验证,通过身份验证。

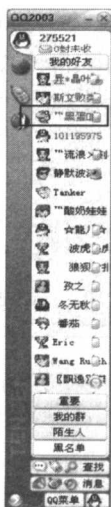


图 1-8

这时会弹出“不能添加自己”的提示,不理睬它,直接退出 QQ。

步骤 3 再一次用注册向导登录时(注意这里一定要用注册向导方式进行登录,而不要直接登录),上线之后就可以看见自己的头像已经在自己的好友 QQ 列表中了(如图 1-8),而且,还可以和“自己”说话呢!

漏洞防范:

这个漏洞未对 QQ 用户造成任何攻击和危害,带来的只是好玩和新奇,所以不用防范。

三、利用漏洞加任意号码到 QQ 好友中

漏洞描述:QQ 存在漏洞,可以使攻击者在未曾通过用户身份验证的时候,直接加对方为 QQ 好友,进而可以得到对方的 IP 地址等危险信息。

大家知道,向 QQ 好友发送消息时,他的 QQ 号码会出现在内存地址中,并以明文的方式保存。如果能找到这个好友的 QQ 号码在内存中的地址,并将这个内存地址中的数据,即

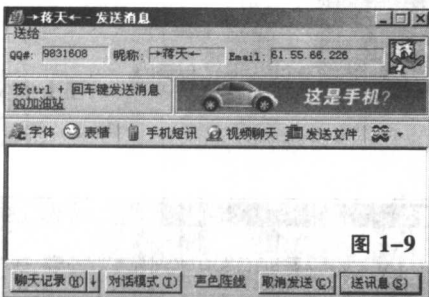


图 1-9

该 QQ 号码换为想加入的那个人的 QQ 号,并锁定该数据,这样只要不关机,无论怎么开、关 QQ,内存地址中“记住”的永远都是这个新 QQ 号。点击这个 QQ 好友准备发送消息,更新资料,会发现他的号码变为你想加入的那个人的 QQ 号码了!利用这个特性,可以尝试将任何号码加入到 QQ 号码中。

适用版本:任何 QQ 版本

攻击原理:当攻击者想加某人到自己的 QQ 好友中,进而获取其 IP 地址等危险信息的时候,如果对方拒绝,那该怎么办?攻击者使用一个方法可以随意加任何人到你的 QQ 好友名单中!首先攻击者得准备一款游戏修改软件,如 FPE2001 或 Game Master 8.0 都行。以 Game Master 8.0 为例。

步骤 1 假设攻击者要加的 QQ 号码是 821661,前提条件是必须要有身份验证号,但不要直接发消息请求加入。先找一个自己本身的 QQ 好友,假设是 9831608,然后打开发送信息框(如图 1-9)。

步骤 2 启动 Game Master 8.0,点左侧的“资料搜寻”,点右上方的下拉菜单,在其中找到“发送信息”一项,然后向修改游戏一样,在搜索目标中填入 9831608 这个号码,点右侧“搜寻”,一般情况下你会找到好多这样的地址(如图 1-10)。

将它们全都选中,然后点右键,在弹出菜单中选择“把所有记号都加入”,在数值项中填入我们要加的 QQ 号并在“自



图 1-10



图 1-11

步骤3 重新运行一下QQ,在好友里就会出现821661这个号码了(如图1-12),但是对他发的消息只能出现在对方的“陌生人”名单里。OK,已经成功地将这个号加为好友了。此漏洞暂时没有解决办法,就连“拒绝任何人加为好友”也不管用了。

漏洞防范:惟一要做的就是当这种人出现你的陌生中,立



四、MIRC DCC SEND 缓冲器溢出让 MIRC 受到影响

漏洞描述:英国 MIRC 公司出品的 IRC 类客户端软件,目前风靡于全世界。界面优美,彩色文本行,具有全 **dcc**、**xdcc** 文件发送和接收能力,**aliases**, 能远程命令和事件操作与位置相关的下拉菜单、**www** 和声音支持。世界相当多国家的人都在使用 **mIRC** 进行交流! **MIRC DCC SEND** 缓冲器溢出漏洞可能允许远程攻击者导致 **mIRC** 客户系统崩溃。来自“**DCC SEND**”的一个请求能够引起致命的错误,导致受影响的 **mIRC** 客户系统崩溃。攻击者可以利用这个漏洞使 **mIRC** 遭受影响。

适用系统:

Khaled Mardam-Bey mIRC 6.1

Khaled Mardam-Bey mIRC 6.11

不受影响系统:

Khaled Mardam-Bey mIRC 6.12

攻击原理:

攻击者只需要在使用 **mICR** 聊天的过程中(如图 1-13), 输入以下请求(如图 1-14):

/quote PRIVMSG #mirc :^ADCC SEND "a a a a a



a a a a a a a a a a a a a a a a
a
a a a a a a a a a a a a a a a a
a
a a a a a a a a a a a a a a a a
a
a
a a a a a a a a a a a a a a a a

a a" 1363975063 3500 4^A





就能使 **MIRC** 客户系统崩溃,严重影响客户的正常使用!

漏洞防范: 可以使用 **IRC** 中的命令来禁止有 **DCC Chat** 有关的连接,这个命令是: **/ignore** 命令(即忽略),它用来把某个用户加入您的“坏人黑名单”。一旦某个用户进入了你的 **IRC** 的黑名单,他说的任何话都将不会显示在您的终端上,这样就达到了防范的目的!

/ignore 命令的基本格式是: **/ig(nore)** 用户昵称

具体的防范命令是:

"/ignore -d * 或者 **"/ignore -wd ***(如图 1-15)。

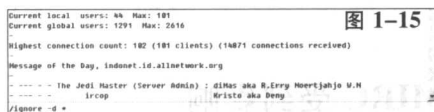


图 1-15

当然也可以升级 **MIRC** 的程序版本来防止这个漏洞,前面说过不受影响系统是: **Khaled Mardam-Bey MIRC 6.12**, 可以去 **MIRC** 的官方主页下载: <http://www.mirc.com/get.html>。

注意: **IRC** 的聊天方式经常以命令开头代表某种方式,例如: **/exit**, 断开服务器的连接,并关闭 **mIRC**; **/help**, 弹出 **mIRC** 的 **help** 窗口; **/Join** 命令加入一个指定的频道,例如: **/Join #China** 等。

上面提到的 **/quote** 命令也是 **IRC** 常用命令之一。

小知识:

1. **IRC(Internet Relay Chat, 国际互联网中继交谈)**。简单来说就是来自世界各地的 **IRC** 用户登录上 **IRC** 服务器,由 **IRC** 服务器把他们彼此的交谈信息中继给彼此,但是 **RFC1459** 协议赋予了 **IRC** 更强大的功能。目前世界上较大的国际性 **IRC** 服务网络有美国的 **Undernet**, **DalNet**, **EFNet**, 中国大陆的 **IRC** 网络有 **SunNet**, **263** 首都在线, **PCHome**。

IRC 被称为是互联网出现以来最激动人心的服务,它和目前风行的 **ICQ** 具有本质的不同。**IRC** 具有真正的社区性。

2. **DCC(Direct Client To Client)** 是一个 **IRC** 中的 **CTCP** 协议下面的子协议,通常直接客户对客户交谈、直接客户对客户文件传输即是通过这个协议实现的。

Dcc Chat 跟普通的私聊不同之处在于,两个人的聊天信息不需要服务器中继,这样不但更加安全,而且也不必受限于 **IRC** 服务器的速度,但是必须双方都能够互相联接上对方。比如上海 **8888VIP** 用户就无法跟一个 **163ChinaNet** 用户进行 **DCC Chat**,因为他们彼此无法联接上对方。

五、危险的 MIRC DDE 安全权限漏洞

漏洞描述: 聊天客户端: **mIRC** 中的 **DDE (Dynamic Data Exchange)** 存在一个漏洞可以导致一般权利程序来执行权限更高的程序。如当管理员在执行 **DDE** 服务时,一般用户可以利用漏洞以管理员身份运行其他命令。

适用系统: **MIRC** 所有版本。

攻击原理: 攻击者可以通过下面的方法来达到利用 **mIRC** 中的 **DDE** 存在漏洞的目的。