MoSh0u's Blog

我是墨手！我是传奇！

查看文章

QQ2009 溢出漏洞 简单测试［官方漏洞已修补］

2009-08-02 19:05

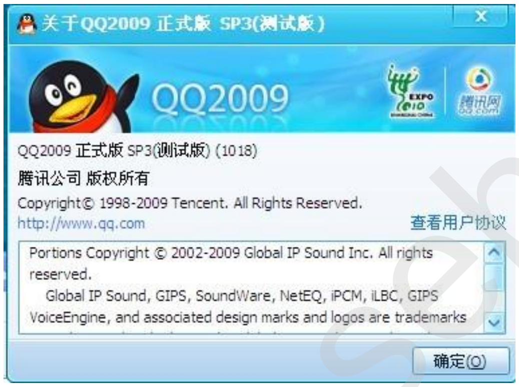
作者:墨手(MoSh0u)

BLOG:http://hi.baidu.com/MoSh0u/

测试时间:2009年8月2日

测试环境:Microsoft Windows XP professional Service Pack 3

测试对象:QQ2009 正式版 SP3(测试版) (1018)
(目前最新版本)


关于QQ2009 正式版 SP3(测试版)

QQ2009 正式版 SP3(测试版) (1018)
腾讯公司 版权所有
Copyright© 1998-2009 Tencent. All Rights Reserved.
http://www.qq.com 查看用户协议

Portions Copyright © 2002-2009 Global IP Sound Inc. All rights reserved.
Global IP Sound, GIPS, SoundWare, NetEQ, iPCM, iLBC, GIPS VoiceEngine, and associated design marks and logos are trademarks

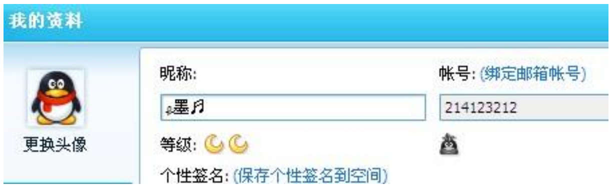
测试QQ:214123212

溢出代码:(不含"="号,中间汉字可任意替换)
========================
↜墨
========================

漏洞范围:QQ2009 所有版本

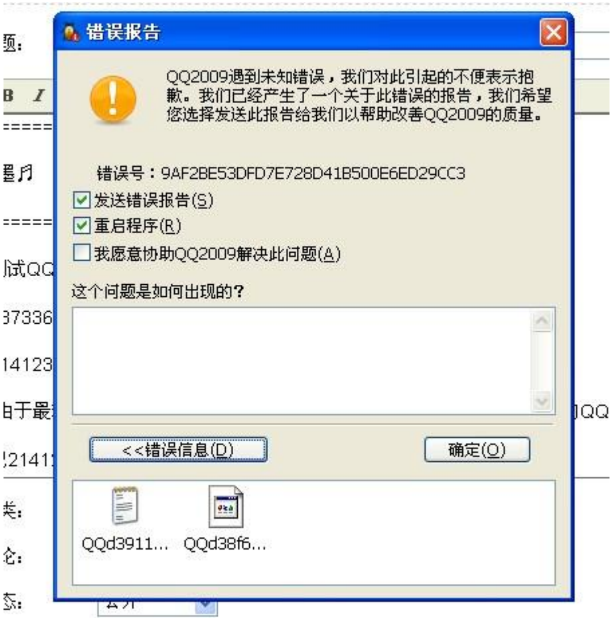
简易测试:

我们将QQ214123212账号的昵称设置为:↜墨


我的资料

昵称: ↜墨♫
帐号: (绑定邮箱帐号) 214123212
等级:
个性签名: (保存个性签名到空间)

点击"确定"后,QQ214123212程序自动关闭,并弹出"错误报告"窗口 ,生成QQd39112.txt文件



错误报告

QQ2009遇到未知错误，我们对此引起的不便表示抱歉。我们已经产生了一个关于此错误的报告，我们希望您选择发送此报告给我们以帮助改善QQ2009的质量。

错误号：9AF2BE53DFD7E728D41B500E6ED29CC3

☑ 发送错误报告(S)
☑ 重启程序(R)
□ 我愿意协助QQ2009解决此问题(A)

这个问题是如何出现的？

QQd39112.txt文件内容如下:

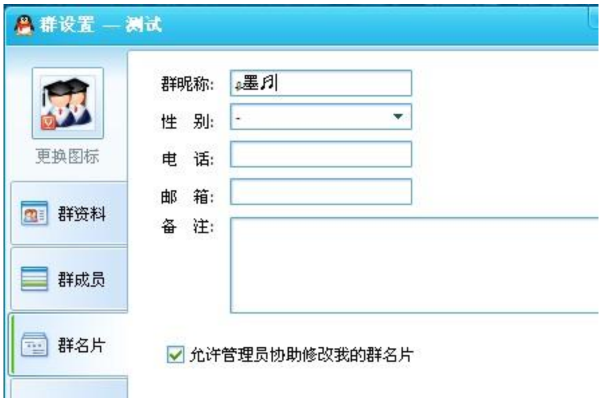
```
========================================================================
Microsoft Windows XP Service Pack 3 [Build 5.1.2600]
QQ2009 24.49.1018 495FF2A593C38ABB1A0CDFB94F147C02
----------------------------------------
Type: EXCEPTION_ACCESS_VIOLATION
Address: 73FB6687
Error: Write address 0x06691000

CallStack:
0x73FA0000[16687] USP10.dll: (33625220,2036,107462908,65535)
0x73FA0000[34A1A] USP10.dll: (33625220,1242004,107462908,65535)
0x30800000[24E6E] GF.dll: (0,33625220,2351464,3)
0x30800000[24FF0] GF.dll: (33625220,-1055504287,107463032,105468896)
0x30800000[25CD9] GF.dll: (107463032,33625220,2080,0)
0x30800000[2647D] GF.dll: (107463032,33625220,1242492,2080)
0x30800000[26580] GF.dll: (107463032,33625220,1242492,2080)
0x30800000[267B0] GF.dll: (33625220,105468868,807322328,4)
0x30800000[129C3] GF.dll: (1242448,3,2,198)
0x30800000[10705] GF.dll: (33625220,3,2,198)
0x30800000[1BC32] GF.dll: (105468784,107462936,3,2)
0x30800000[6DB3F] GF.dll: (46467456,1243012,1243712,1243396)
0x30800000[6E4A4] GF.dll: (46467456,1243012,1243712,1243396)
0x30800000[6EEF5] GF.dll: (46468012,46467456,1243012,1243712)
0x30800000[3DE7C] GF.dll: (46467456,46467456,1243012,1243712)
0x30800000[38731] GF.dll: (46467456,1243012,1243712,1243396)
0x30800000[155D00] GF.dll: (46467456,1243012,1243712,1243396)
0x30800000[1596C1] GF.dll: (0,33625220,107462936,139)
0x30800000[15A2E6] GF.dll: (105556816,107472088,1243584,1243712)
0x30800000[15AC72] GF.dll: (105859216,1243584,1243712,1243624)
0x30800000[15B110] GF.dll: (105556816,0,1243584,1243712)
0x30800000[160D84] GF.dll: (3343548,1243712,0,0)
0x30800000[15E2C4] GF.dll: (15,0,0,1243712)
0x30800000[1618AF] GF.dll: (3343548,15,0,0)
0x30800000[C8A4D] GF.dll: (105476312,15,0,0)
0x77D10000[8734] USER32.dll: (2248424,3343548,15,0)
0x77D10000[8816] USER32.dll: (0,2248424,3343548,15)
0x77D10000[18EA0] USER32.dll: (6635920,15,0,0)
0x77D10000[18EEC] USER32.dll: (1244052,24,6635920,15)
0x7C920000[E473] ntdll.dll: (1244184,0,1244212,4205174)
0x77D10000[8A10] USER32.dll: (1244184,2010223628,13331456,4213015)
0x00400000[2A76] QQ.exe: (-1055499544,2,1,0)
0x00400000[3167] QQ.exe: (4266104,0,4241716,484)
0x00400000[244B] QQ.exe: (4194304,0,132608,1)
0x00400000[7AB4] QQ.exe: (594808,2090008669,2147340288,-1073741819)
0X7C800000[17077] kernel32.dll: (2147340288,-1073741819,1245128,1240808)

Regs:
EAX=00000005, EBX=023872A0, ECX=0667C0B8, EDX=00000001
ESI=00000005, EDI=000053D2, EBP=0012F2D4, ESP=0012F2C4, EIP=73FB6687
Bytes at CS:EIP:
89 04 B9 47 3B 7D 14 7C CF 3B 7D 14 7D 5B 0F B7 C6 3B 45 0C 7E 23 8B 45 FC 66 3B B0 D2 00 00 00
```

```
pid=49244 init_tid=49256 crashtid=49256
Modules:
[00400000,023000] D:\腾迅软件\QQ2009\Bin\QQ.exe [1.31.1025.0,2009-07-23 03:22:09 GMT]
[7C920000,096000] C:\WINDOWS\system32\ntdll.dll [5.1.2600.5755,2009-02-09 10:54:47 GMT]
[7C800000,11E000] C:\WINDOWS\system32\kernel32.dll [5.1.2600.5781,2009-03-21 14:06:57 GMT]
[5D170000,09A000] C:\WINDOWS\system32\COMCTL32.dll [5.82.2900.5512,2008-04-14 02:12:49 GMT]
[77DA0000,0A9000] C:\WINDOWS\system32\ADVAPI32.dll [5.1.2600.5755,2009-02-09 10:54:48 GMT]
[77E50000,092000] C:\WINDOWS\system32\RPCRT4.dll [5.1.2600.5795,2009-04-15 14:52:03 GMT]
[77FC0000,011000] C:\WINDOWS\system32\Secur32.dll [5.1.2600.5512,2008-04-14 02:13:21 GMT]
[77EF0000,049000] C:\WINDOWS\system32\GDI32.dll [5.1.2600.5698,2008-10-23 12:38:08 GMT]
[77D10000,090000] C:\WINDOWS\system32\USER32.dll [5.1.2600.5512,2008-04-14 02:13:17 GMT]
[30000000,20A000] D:\腾迅软件\QQ2009\Bin\Common.dll [1.31.1025.0,2009-07-22 03:05:38 GMT]
[71A20000,017000] C:\WINDOWS\system32\WS2_32.dll [5.1.2600.5512,2008-04-14 02:14:32 GMT]
[77BE0000,058000] C:\WINDOWS\system32\msvcrt.dll [7.0.2600.5512,2008-04-14 02:15:27 GMT]
[71A10000,008000] C:\WINDOWS\system32\WS2HELP.dll [5.1.2600.5512,2008-04-14 02:14:33 GMT]
[76680000,0A6000] C:\WINDOWS\system32\WININET.dll [6.0.2900.5835,2009-06-26 16:49:35 GMT]
[765E0000,093000] C:\WINDOWS\system32\CRYPT32.dll [5.131.2600.5512,2008-04-14 02:13:04 GMT]
[76DB0000,012000] C:\WINDOWS\system32\MSASN1.dll [5.1.2600.5512,2008-04-14 02:13:49 GMT]
[770F0000,08B000] C:\WINDOWS\system32\OLEAUT32.dll [5.1.2600.5512,2008-04-14 02:13:17 GMT]
[76990000,13D000] C:\WINDOWS\system32\ole32.dll [5.1.2600.5512,2008-04-14 02:13:16 GMT]
[77F40000,076000] C:\WINDOWS\system32\SHLWAPI.dll [6.0.2900.5512,2008-04-14 02:13:15 GMT]
[76060000,156000] C:\WINDOWS\system32\SETUPAPI.dll [5.1.2600.5512,2008-04-14 02:13:04 GMT]
[77BD0000,008000] C:\WINDOWS\system32\VERSION.dll [5.1.2600.5512,2008-04-14 02:13:19 GMT]
[76BC0000,00B000] C:\WINDOWS\system32\PSAPI.DLL [5.1.2600.5512,2008-04-14 02:12:59 GMT]
[76D30000,018000] C:\WINDOWS\system32\iphlpapi.dll [5.1.2600.5512,2008-04-14 02:12:27 GMT]
[68D60000,0A1000] C:\WINDOWS\system32\dbghelp.dll [5.1.2600.5512,2008-04-14 02:12:18 GMT]
[76320000,047000] C:\WINDOWS\system32\comdlg32.dll [6.0.2900.5512,2008-04-14 02:12:50 GMT]
[7D590000,7F4000] C:\WINDOWS\system32\SHELL32.dll [6.0.2900.5686,2008-09-30 06:20:04 GMT]
[7C630000,01B000] C:\WINDOWS\WinSxS\x86_Microsoft.VC80.ATL_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_cbb27474\ATL80.DLL [8.0.50727.762,2006-12-02 06:55:18 GMT]
[7C420000,087000] C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700\MSVCP80.dll [8.0.50727.762,2006-12-02 06:52:56 GMT]
[78130000,09B000] C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700\MSVCR80.dll [8.0.50727.762,2006-12-02 06:50:32 GMT]
[76C00000,02E000] C:\WINDOWS\system32\WINTRUST.dll [5.131.2600.5512,2008-04-14 02:13:34 GMT]
[76C60000,028000] C:\WINDOWS\system32\IMAGEHLP.dll [5.1.2600.5512,2008-04-14 02:12:42 GMT]
[5FDD0000,055000] C:\WINDOWS\system32\NETAPI32.dll [5.1.2600.5694,2008-10-15 16:35:19 GMT]
[31800000,08B000] D:\腾迅软件\QQ2009\Bin\KernelUtil.dll [1.31.1025.0,2009-07-22 03:07:14 GMT]
[30800000,294000] D:\腾迅软件\QQ2009\Bin\GF.dll [1.31.1025.0,2009-07-22 03:14:32 GMT]
[76300000,01D000] C:\WINDOWS\system32\IMM32.dll [5.1.2600.5512,2008-04-14 02:13:07 GMT]
[4AE90000,1A6000] C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5581_x-ww_dfbc4fc4\gdiplus.dll [5.1.3102.5581,2008-04-15 17:47:47 GMT]
[762F0000,005000] C:\WINDOWS\system32\MSIMG32.dll [5.1.2600.5512,2008-04-14 02:14:46 GMT]
[73FA0000,06B000] C:\WINDOWS\system32\USP10.dll [1.420.2600.5512,2008-04-14 02:13:19 GMT]
[75C60000,0A0000] C:\WINDOWS\system32\urlmon.dll [6.0.2900.5835,2009-06-26 16:49:35 GMT]
[61210000,1D2000] D:\腾迅软件\QQ2009\Bin\AppUtil.dll [1.31.1025.0,2009-07-23 02:20:30 GMT]
[76B10000,02A000] C:\WINDOWS\system32\WINMM.dll [5.1.2600.5512,2008-04-14 02:13:53 GMT]
[62C20000,009000] C:\WINDOWS\system32\LPK.DLL [5.1.2600.5512,2008-04-14 02:12:47 GMT]
[77180000,103000] C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll [6.0.2900.5512,2008-04-14 02:11:56 GMT]
[5AD70000,038000] C:\WINDOWS\system32\uxtheme.dll [6.0.2900.5512,2008-04-14 00:11:10 GMT]
[10000000,02F000] C:\Program Files\360\360Safe\safemon\safemon.dll [5.0.0.1021,2009-07-29 04:21:26 GMT]
[74680000,04C000] C:\WINDOWS\system32\MSCTF.dll [5.1.2600.5512,2008-04-14 02:13:55 GMT]
[76FA0000,07F000] C:\WINDOWS\system32\CLBCATQ.DLL [2001.12.4414.700,2008-04-14 02:12:34 GMT]
[77020000,09A000] C:\WINDOWS\system32\COMRes.dll [2001.12.4414.700,2008-04-14 02:12:55 GMT]
[5DD50000,114000] C:\WINDOWS\system32\msxml3.dll [8.100.1048.0,2008-09-04 17:15:01 GMT]
[61C00000,1FA000] D:\腾迅软件\QQ2009\Bin\MainFrame.dll [1.31.1025.0,2009-07-23 02:33:13 GMT]
[73640000,02E000] C:\WINDOWS\system32\msctfime.ime [5.1.2600.5768,2009-02-27 04:56:13 GMT]
[74CF0000,091000] C:\WINDOWS\system32\mlang.dll [6.0.2900.5512,2008-04-14 02:12:56 GMT]
[60B30000,061000] D:\腾迅软件\QQ2009\Bin\MSVCP60.dll [6.0.8168.0,2006-01-10 11:15:44 GMT]
[68000000,036000] C:\WINDOWS\system32\rsaenh.dll [5.1.2600.5507,2008-03-18 14:39:32 GMT]
[02510000,549000] C:\WINDOWS\system32\xpsp2res.dll [5.1.2600.5512,2008-04-13 17:39:24 GMT]
[31000000,326000] D:\腾迅软件\QQ2009\Bin\IM.dll [1.31.1025.0,2009-07-22 03:19:43 GMT]
[73D30000,0FE000] C:\WINDOWS\system32\MFC42.DLL [6.2.4131.0,2008-04-14 02:12:46 GMT]
[61BE0000,00D000] C:\WINDOWS\system32\MFC42LOC.DLL [6.0.8665.0,2001-08-31 23:01:06 GMT]
[61FE0000,040000] D:\腾迅软件\QQ2009\Bin\TaskTray.dll [1.31.1025.0,2009-07-23 02:35:04 GMT]
[32000000,00A000] D:\腾迅软件\QQ2009\Bin\TXPFProxy.dll [1.31.1025.0,2009-07-22 03:06:41 GMT]
[030D0000,057000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.QQShow\Bin\FlashAvatarDll.dll [1.26.1.26,2009-05-15 06:32:51 GMT]
[72C90000,009000] C:\WINDOWS\system32\wdmaud.drv [5.1.2600.5512,2008-04-14 02:13:33 GMT]
[72C80000,008000] C:\WINDOWS\system32\msacm32.drv [5.1.2600.0,2001-08-31 22:59:06 GMT]
[77BB0000,015000] C:\WINDOWS\system32\MSACM32.dll [5.1.2600.5512,2008-04-14 02:13:34 GMT]
[77BA0000,007000] C:\WINDOWS\system32\midimap.dll [5.1.2600.5512,2008-04-14 02:12:51 GMT]
[31400000,04C000] D:\腾迅软件\QQ2009\Bin\KernelMisc.dll [1.31.1025.0,2009-07-22 03:16:05 GMT]
[610A0000,140000] D:\腾迅软件\QQ2009\Bin\AppMisc.dll [1.31.1025.0,2009-07-23 02:23:59 GMT]
[61030000,069000] D:\腾迅软件\QQ2009\Bin\AppCtrl.dll [1.31.1025.0,2009-07-23 02:44:13 GMT]
[61500000,128000] D:\腾迅软件\QQ2009\Bin\ChatFrame.dll [1.31.1025.0,2009-07-23 02:27:14 GMT]
[61700000,0A7000] D:\腾迅软件\QQ2009\Bin\ConfigCenter.dll [1.31.1025.0,2009-07-23 02:42:10 GMT]
[61A00000,084000] D:\腾迅软件\QQ2009\Bin\CustomFace.dll [1.31.1025.0,2009-07-23 02:28:24 GMT]
[31C00000,0E3000] D:\腾迅软件\QQ2009\Bin\LongCnn.dll [1.31.1025.0,2009-07-22 03:20:56 GMT]
[61900000,0BB000] D:\腾迅软件\QQ2009\Bin\ContactInfoFrame.dll [1.31.1025.0,2009-07-23 02:37:30 GMT]
[65000000,0D4000] D:\腾迅软件\QQ2009\Bin\MsgMgr.dll [1.31.1025.0,2009-07-23 02:39:53 GMT]
[61F20000,038000] D:\腾迅软件\QQ2009\Bin\SkinMgr.dll [1.31.1025.0,2009-07-23 02:42:47 GMT]
```

```
[61F00000,01A000] D:\腾迅软件\QQ2009\Bin\QInterLive.dll [1.31.1025.0,2009-07-23 02:40:09 GMT]
[65100000,083000] D:\腾迅软件\QQ2009\Bin\SystemMsg.dll [1.31.1025.0,2009-07-23 02:34:24 GMT]
[62E00000,0F5000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.PaiPai\Bin\PaiPai.dll [1.31.1025.0,2009-07-23 03:01:17
[62100000,137000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.AudioVideo\Bin\AudioVideo.dll [1.31.1025.0,2009-07-23
[62A00000,044000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.MMOG\Bin\MMOG.dll [1.31.1025.0,2009-07-23 03:12:12
[64100000,03E000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.Soso\Bin\Soso.dll [1.31.1025.0,2009-07-23 03:09:27 GM
[63D00000,0A5000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.Qzone\Bin\Qzone.dll [1.31.1025.0,2009-07-23 02:55:03
[64700000,030000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.Weather\Bin\Weather.dll [1.31.1025.0,2009-07-23 03:11:
[64000000,018000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.SoBar\Bin\SoBar.dll [1.31.1025.0,2009-07-23 03:13:52 GMT]
[62F00000,048000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.PaiPaiGift\Bin\PaiPaiGift.dll [1.31.1025.0,2009-07-23 03:12:56 GMT]
[63500000,018000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.QQLive\Bin\QQLive.dll [1.31.1025.0,2009-07-23 03:03:49 GMT]
[63600000,051000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.QQMusic\Bin\QQMusic.dll [1.31.1025.0,2009-07-23 03:03:34 GMT]
[64300000,01B000] D:\腾迅软件\QQ2009\Plugin\Com.Tencent.taotao\Bin\Taotao.dll [1.31.1025.0,2009-07-23 03:11:48 GMT]
[05090000,07E000] C:\Program Files\Common Files\Tencent\TXSSO\Bin\SSOPlatform.dll [1.1.1.11,2009-07-17 12:41:16 GMT]
[05110000,0B1000] C:\Program Files\Common Files\Tencent\TXSSO\Bin\SSOCommon.DLL [1.1.1.3,2009-07-17 12:36:19 GMT]
[05300000,070000] D:\腾迅软件\QQ2009\Bin\BasicCtrlDll.dll [8.0.773.1801,2008-03-27 12:52:02 GMT]
[73AF0000,012000] C:\WINDOWS\system32\AVICAP32.dll [5.1.2600.0,2001-08-31 22:58:59 GMT]
[73B40000,020000] C:\WINDOWS\system32\MSVFW32.dll [5.1.2600.5512,2008-04-14 02:15:28 GMT]
[71A40000,00B000] C:\WINDOWS\system32\WSOCK32.dll [5.1.2600.5512,2008-04-14 02:14:44 GMT]
[39700000,0EB000] D:\腾迅软件\QQ2009\Bin\RICHED20.dll [5.50.99.2012,2005-12-14 06:52:32 GMT]
[719C0000,03E000] C:\WINDOWS\System32\mswsock.dll [5.1.2600.5625,2008-06-20 17:46:00 GMT]
[76EF0000,027000] C:\WINDOWS\system32\DNSAPI.dll [5.1.2600.5625,2008-06-20 17:46:00 GMT]
[76F90000,006000] C:\WINDOWS\system32\rasadhlp.dll [5.1.2600.5512,2008-04-14 02:12:55 GMT]
[60FD0000,055000] C:\WINDOWS\system32\hnetcfg.dll [5.1.2600.5512,2008-04-14 02:12:29 GMT]
[71A00000,008000] C:\WINDOWS\System32\wshtcpip.dll [5.1.2600.5512,2008-04-14 02:14:42 GMT]
[76F80000,008000] C:\WINDOWS\System32\winrnr.dll [5.1.2600.5512,2008-04-14 02:13:24 GMT]
[76F30000,02C000] C:\WINDOWS\system32\WLDAP32.dll [5.1.2600.5512,2008-04-14 02:13:39 GMT]
[75AF0000,011000] C:\WINDOWS\system32\devenum.dll [6.5.2600.5512,2008-04-14 02:12:29 GMT]
[73620000,007000] C:\WINDOWS\system32\msdmo.dll [6.5.2600.5512,2008-04-14 02:14:14 GMT]
[7E550000,173000] C:\WINDOWS\system32\shdocvw.dll [6.0.2900.5848,2009-07-18 16:02:44 GMT]
[75430000,071000] C:\WINDOWS\system32\CRYPTUI.dll [5.131.2600.5512,2008-04-14 02:13:10 GMT]
[61B00000,0CE000] D:\腾迅软件\QQ2009\Bin\GroupApp.dll [1.31.1025.0,2009-07-23 02:45:47 GMT]
[71800000,07C000] C:\WINDOWS\system32\shdoclc.dll [6.0.2900.5512,2008-04-13 17:03:19 GMT]
[7E210000,2F8000] C:\WINDOWS\system32\mshtml.dll [6.0.2900.5848,2009-07-18 16:02:42 GMT]
[74620000,027000] C:\WINDOWS\system32\msls31.dll [3.10.349.0,2001-08-31 22:58:54 GMT]
[63F00000,03A000] D:\腾迅软件\QQ2009\Plugin\com.tencent.snsapp\Bin\SNSApp.dll [1.30.860.0,2009-07-23 02:48:11 GMT]
[63000000,03A000] D:\腾迅软件\QQ2009\Plugin\com.tencent.paycenter\Bin\PayCenter.dll [1.31.1025.0,2009-07-23 02:55:53 GMT]
[63100000,022000] D:\腾迅软件\QQ2009\Plugin\com.tencent.qbar\Bin\QBar.dll [1.31.1025.0,2009-07-23 03:10:33 GMT]
[63B00000,024000] D:\腾迅软件\QQ2009\Plugin\com.tencent.qqvipmisc\Bin\QQVipMisc.dll [1.31.1025.0,2009-07-23 03:10:13 GMT]
[64800000,03A000] D:\腾迅软件\QQ2009\Plugin\com.tencent.wenwen\Bin\WenWen.dll [1.31.1025.0,2009-07-23 03:08:52 GMT]
[62B00000,014000] D:\腾迅软件\QQ2009\Plugin\com.tencent.NetBar\Bin\NetBar.dll [1.31.1025.0,2009-07-23 03:14:06 GMT]
[64A00000,087000] D:\腾迅软件\QQ2009\Plugin\com.tencent.wireless\Bin\Wireless.dll [1.31.1025.0,2009-07-23 03:02:47 GMT]
[63900000,0B8000] D:\腾迅软件\QQ2009\Plugin\com.tencent.qqshow\Bin\QQShow.dll [1.31.1025.0,2009-07-23 02:57:31 GMT]
[62300000,034000] D:\腾迅软件\QQ2009\Plugin\com.tencent.crm\Bin\CRM.dll [1.31.1025.0,2009-07-23 03:15:24 GMT]
[64600000,01F000] D:\腾迅软件\QQ2009\Plugin\com.tencent.vas\Bin\VAS.dll [1.31.1025.0,2009-07-23 03:05:52 GMT]
[63A00000,019000] D:\腾迅软件\QQ2009\Plugin\com.tencent.qqvip\Bin\QQVip.dll [1.31.1025.0,2009-07-23 03:15:43 GMT]
[76D10000,018000] C:\WINDOWS\system32\MPRAPI.dll [5.1.2600.5512,2008-04-14 02:13:17 GMT]
[77C90000,032000] C:\WINDOWS\system32\ACTIVEDS.dll [5.1.2600.5512,2008-04-14 02:12:04 GMT]
[76DE0000,025000] C:\WINDOWS\system32\adsldpc.dll [5.1.2600.5512,2008-04-14 02:12:15 GMT]
[76AF0000,011000] C:\WINDOWS\system32\ATL.DLL [3.5.2284.1,2008-04-14 02:12:57 GMT]
[76E50000,00E000] C:\WINDOWS\system32\rtutils.dll [5.1.2600.5512,2008-04-14 02:13:11 GMT]
[71B70000,013000] C:\WINDOWS\system32\SAMLIB.dll [5.1.2600.5512,2008-04-14 02:13:00 GMT]
[62500000,038000] D:\腾迅软件\QQ2009\Plugin\com.tencent.gamelife\Bin\GameLife.dll [1.31.1025.0,2009-07-23 03:14:48 GMT]
[084C0000,4A3000] C:\WINDOWS\system32\Macromed\Flash\Flash10c.ocx [10.0.32.18,2009-07-18 03:11:53 GMT]
[73AA0000,015000] C:\WINDOWS\system32\mscms.dll [5.1.2600.5627,2008-06-24 16:42:47 GMT]
[72F70000,026000] C:\WINDOWS\system32\WINSPOOL.DRV [5.1.2600.5512,2008-04-14 02:13:30 GMT]
[767C0000,027000] C:\WINDOWS\system32\schannel.dll [5.1.2600.5721,2008-12-05 06:55:58 GMT]
[759D0000,0AF000] C:\WINDOWS\system32\USERENV.dll [5.1.2600.5512,2008-04-14 02:13:18 GMT]
[63300000,067000] D:\腾迅软件\QQ2009\Plugin\com.tencent.qqgame\Bin\QQGame.dll [1.31.1025.0,2009-07-23 03:04:39 GMT]
[63700000,036000] D:\腾迅软件\QQ2009\Plugin\com.tencent.qqpet\Bin\QQPet.dll [1.31.1025.0,2009-07-23 03:09:50 GMT]
[63800000,039000] D:\腾迅软件\QQ2009\Plugin\com.tencent.qqring\Bin\QQRing.dll [1.31.1025.0,2009-07-23 03:05:33 GMT]
[62900000,04D000] D:\腾迅软件\QQ2009\Plugin\com.tencent.memo\Bin\Memo.dll [1.31.1025.0,2009-07-23 03:16:26 GMT]
[09990000,091000] D:\腾迅软件\QQ2009\Bin\InformationBox.dll [1.31.1025.0,2009-07-23 02:47:21 GMT]
[62400000,08B000] D:\腾迅软件\QQ2009\Plugin\com.tencent.filetransfer\Bin\FileTransfer.dll [1.31.1025.0,2009-07-23 02:49:15 GMT]
[0A270000,053000] D:\腾迅软件\QQ2009\Plugin\com.tencent.advertisement\Bin\Advertisement.dll [1.31.1025.0,2009-07-23 02:58:46 GMT]
[62700000,02F000] D:\腾迅软件\QQ2009\Plugin\com.tencent.mail\Bin\Mail.dll [1.31.1025.0,2009-07-23 03:01:46 GMT]
[64400000,01D000] D:\腾迅软件\QQ2009\Plugin\com.tencent.today\Bin\Today.dll [1.31.1025.0,2009-07-23 02:57:53 GMT]
[63C00000,02B000] D:\腾迅软件\QQ2009\Plugin\com.tencent.qqwebsite\Bin\QQWebsite.dll [1.31.1025.0,2009-07-23 03:13:37 GMT]
[74650000,02A000] C:\WINDOWS\system32\MSIMTF.dll [5.1.2600.5512,2008-04-14 02:14:47 GMT]
[75BC0000,07D000] C:\WINDOWS\system32\jscript.dll [5.7.0.18066,2008-05-09 10:53:48 GMT]
[76D70000,022000] C:\WINDOWS\system32\apphelp.dll [5.1.2600.5512,2008-04-14 02:12:38 GMT]
[757D0000,013000] C:\WINDOWS\system32\cryptnet.dll [5.131.2600.5512,2008-04-14 02:13:08 GMT]
[72240000,005000] C:\WINDOWS\system32\SensApi.dll [5.1.2600.5512,2008-04-14 02:13:00 GMT]
[4A410000,059000] C:\WINDOWS\system32\WINHTTP.dll [5.1.2600.5512,2008-04-14 02:13:49 GMT]
[04D50000,012000] C:\Documents and Settings\Administrator\Application Data\Tencent\QQ\SafeBase\TSEH.dat [2008.12.9.2,2008-12-09 01:56:33
GMT]
[0AA10000,011000] C:\Documents and Settings\Administrator\Application Data\Tencent\QQ\SafeBase\TSELoder.DAT [2008.1.28.13,2008-01-28 0
6:06:15 GMT]
[0AF50000,0D7000] C:\WINDOWS\system32\JJ.IME [5.1.0.0,2008-12-31 03:23:16 GMT]
----------------------------------------
Crash Signature: 9AF2BE53DFD7E728D41B500E6ED29CC3
```

==

攻击测试:
将QQ214123212的QQ群(非管理)昵称改为:墨

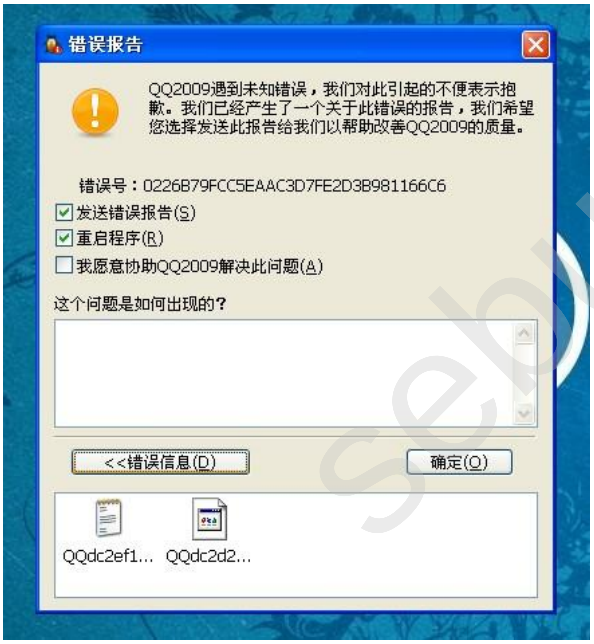


群设置 — 测试

群昵称: 墨♪
性　别: -
电　话:
邮　箱:
备　注:

☑ 允许管理员协助修改我的群名片

QQ群内的所有QQ2009用户都将自动关闭,都将弹出"错误报告"窗口



错误报告

QQ2009遇到未知错误，我们对此引起的不便表示抱歉。我们已经产生了一个关于此错误的报告，我们希望您选择发送此报告给我们以帮助改善QQ2009的质量。

错误号：0226B79FCC5EAAC3D7FE2D3B981166C6

☑ 发送错误报告(S)
☑ 重启程序(R)
□ 我愿意协助QQ2009解决此问题(A)

这个问题是如何出现的？

若QQ214123212不改掉QQ昵称的话,所有QQ群内用户都将无法登陆此QQ群.

测试结束:
(总结:略(有无0day可开发?问那些大牛吧,总之可以根据此原理制作成攻击器.))
(声明:任何人不得利用此漏洞进行任何违法行为,后果自负!)

类别：七嘴八舌 | 添加到搜藏 | 浏览(835) | 评论 (14)

上一篇：细数仙剑奇侠传三那些被糟蹋掉的...

最近读者：

登录后，您就出现在这里。

admi520 堕落の青春 niashoi unixshell bingehaolv pwwhj zk65158502 dyzztxb

3

网友评论：

1

龟派气功

2009-08-03 02:58 | 回复
有意思，测试去了。

2

7overlord

2009-08-03 11:05 | 回复

3

eanalysis

2009-08-03 11:09 | 回复
多谢提醒，我们已经安排技术人员去处理了。后面有类似问题，您也可以发送到security@tencent.com,我们会有专职技术同事负责处理。腾讯TST团队，也会准备一下小礼物表示感谢。：）

4 匿名网友

2009-08-03 11:20 | 回复
前几天盛大的人放出来的

5

Coke_Coca Cola

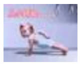
2009-08-03 13:16 | 回复
SOGA

6

黑羽菠萝

2009-08-03 13:19 | 回复
Masaka

7


ks_tiejun

2009-08-03 14:13 | 回复
qq2009 SP2也崩了

8 匿名网友

2009-08-03 15:19 | 回复
完了，我加了1246270967，但是还没有接受，接受之后我的QQ是不是会自动关闭，而且我把群名字也改了，打不开了！ 我想恢复，怎么解决啊！

9 匿名网友

2009-08-03 15:22 | 回复
只有一个办法了，退群重加5555555555555！我加了1246270967，要是 是你接受的话我会不会自动关闭！ 哭！

10 网友:墨手

2009-08-03 15:28 | 回复
回复匿名网友：用QQ2008登陆修改

11 网友:银√鹰

2009-08-03 20:37 | 回复
用2008把Q上的昵称改掉！（群里的不要改）！然后在用2009登陆！那样自己的Q就不会跳掉！如果有人去访问群(已经被我设置了的)！！就自动跳！！

12 匿名网友

2009-08-03 22:19 | 回复
我是QQ2009，把别人的备注改为那个墨 后QQ自动关闭了，2009不能登录了怎么办？

13

MoSh0u

2009-08-03 22:52 | 回复
回复匿名网友：用QQ2008登陆修改昵称.给大家造成的不便很抱歉~

15 网友:我此成为次 2009-08-04 09:35 | 回复

真是好奇害死猫啊 我疯了QQ上不了了。
我下2008几次了

发表评论：

姓 名：	注册 | 登录
网址或邮箱：	(选填)
内 容：	插入表情 ▼ 闪光字
验证码：	请点击后输入四位验证码，字母不区分大小写
	发表评论

©2009 Baidu