Quassel IRC - Bug #364

Wild core crash

10/23/2008 11:18 PM - EgS

Status:	Rejected	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Quassel Core	**Estimated time:**	0.00 hour
Target version:			
Version:	0.3.1+	**OS:**	Any

Description

2008-10-23 23:10:27 Info: Client 91.19.83.201 initialized and authenticated successfully as "phon" (UserId: 6).

- glibc detected * **./quasselcore: double free or corruption (!prev): 0x00002aaaad035c70** * ======= Backtrace: =========
  /lib64/libc.so.6[0x2b19f16369ed]
  /lib64/libc.so.6(cfree+0x76)[0x2b19f1638716]
  /usr/lib/libcrypto.so.0.9.8(CRYPTO_realloc_clean+0x8f)[0x2b19f1ccb30f]
  /usr/lib/libcrypto.so.0.9.8(BUF_MEM_grow_clean+0x66)[0x2b19f1d228b6]
  /usr/lib/libcrypto.so.0.9.8[0x2b19f1d2406d]
  /usr/lib/libcrypto.so.0.9.8(BIO_write+0x82)[0x2b19f1d232d2]
  /usr/lib/libssl.so.0.9.8(ssl3_write_pending+0x89)[0x2b19f1b3f999]
  /usr/lib/libssl.so.0.9.8(ssl3_write_bytes+0x79)[0x2b19f1b3ff79]
  /usr/lib64/qt4/libQtNetwork.so.4[0x2b19f086a94d]
  /usr/lib64/qt4/libQtNetwork.so.4(*ZN10QSslSocket11qt_metacallEN11QMetaObject4CallEiPPv+0x9f)[0x2b19f0864c0f]*
  /usr/lib64/qt4/libQtCore.so.4(_ZN11QMetaObject8activateEP7QObjectiiPPv+0x240)[0x2b19efdb2480]
  /usr/lib64/qt4/libQtNetwork.so.4[0x2b19f084aed8]
  /usr/lib64/qt4/libQtNetwork.so.4[0x2b19f083d7a1]
  /usr/lib64/qt4/libQtCore.so.4(_ZN23QCoreApplicationPrivate13notify_helperEP7QObjectP6QEvent+0x5f)[0x2b19efd9f2ef]
  /usr/lib64/qt4/libQtCore.so.4(_ZN16QCoreApplication6notifyEP7QObjectP6QEvent+0x37)[0x2b19efd9f337]
  /usr/lib64/qt4/libQtCore.so.4(_ZN16QCoreApplication14notifyInternalEP7QObjectP6QEvent+0xc8)[0x2b19efd9efa8]
  /usr/lib64/qt4/libQtCore.so.4(_ZN20QEventDispatcherUNIX23activateSocketNotifiersEv+0xbf)[0x2b19efdc81af]
  /usr/lib64/qt4/libQtCore.so.4(_ZN27QEventDispatcherUNIXPrivate8doSelectE6QFlagsIN10QEventLoop17ProcessEventsFlagEEP7timeval+0x43b)[0x2b19efdc861b]
  /usr/lib64/qt4/libQtCore.so.4(_ZN20QEventDispatcherUNIX13processEventsE6QFlagsIN10QEventLoop17ProcessEventsFlagEE+0xb2)[0x2b19efdc87e2]
  /usr/lib64/qt4/libQtCore.so.4(_ZN10QEventLoop13processEventsE6QFlagsINS_17ProcessEventsFlagEE+0x35)[0x2b19efd9e355]
  /usr/lib64/qt4/libQtCore.so.4(_ZN10QEventLoop4execE6QFlagsINS_17ProcessEventsFlagEE+0x98)[0x2b19efd9e4b8]
  /usr/lib64/qt4/libQtCore.so.4(_ZN16QCoreApplication4execEv+0xae)[0x2b19efda01ce]
  ./quasselcore(main+0x3f)[0x45a1d7]
  /lib64/libc.so.6(_libc_start_main+0xf4)[0x2b19f15e51f4]
  ./quasselcore(_ZN7QObject5eventEP6QEvent+0x2e1)[0x45a109]

Additional information:

======= Memory map: ========
00400000-0054c000 r-xp 00000000 fd:00 1142973 /home/dev/quassel/cbuild/quasselcore (deleted)
0074b000-0074c000 r--p 0014b000 fd:00 1142973 /home/dev/quassel/cbuild/quasselcore (deleted)
0074c000-0074d000 rw-p 0014c000 fd:00 1142973 /home/dev/quassel/cbuild/quasselcore (deleted)
0074d000-045b4000 rw-p 0074d000 00:00 0 [heap]
40000000-40001000 ---p 40000000 00:00 0
40001000-40801000 rw-p 40001000 00:00 0
40801000-40802000 ---p 40801000 00:00 0
40802000-41002000 rw-p 40802000 00:00 0
41002000-41003000 ---p 41002000 00:00 0
41003000-41803000 rw-p 41003000 00:00 0
41803000-41804000 ---p 41803000 00:00 0
41804000-42004000 rw-p 41804000 00:00 0
42004000-42005000 ---p 42004000 00:00 0
42005000-42805000 rw-p 42005000 00:00 0
42805000-42806000 ---p 42805000 00:00 0
42806000-43006000 rw-p 42806000 00:00 0

```
43006000-43007000 ---p 43006000 00:00 0
43007000-43807000 rw-p 43007000 00:00 0
43807000-43808000 ---p 43807000 00:00 0
43808000-44008000 rw-p 43808000 00:00 0
44008000-44009000 ---p 44008000 00:00 0
44009000-44809000 rw-p 44009000 00:00 0
44809000-4480a000 ---p 44809000 00:00 0
4480a000-4500a000 rw-p 4480a000 00:00 0
2aaaaaaab000-2aaaaaad5000 rw-p 2aaaaaaab000 00:00 0
2aaaaaadd000-2aaaaaaed000 r-xp 00000000 fd:00 235173     /lib64/libresolv-2.7.so
2aaaaaaed000-2aaaaaced000 ---p 00010000 fd:00 235173     /lib64/libresolv-2.7.so
2aaaaaced000-2aaaaacee000 r--p 00010000 fd:00 235173     /lib64/libresolv-2.7.so
2aaaaacee000-2aaaaacef000 rw-p 00011000 fd:00 235173     /lib64/libresolv-2.7.so
2aaaaacef000-2aaaaacf1000 rw-p 2aaaaacef000 00:00 0
2aaaaacf1000-2aaaaacfb000 r-xp 00000000 fd:00 234803     /lib64/libnss_files-2.7.so
2aaaaacfb000-2aaaaaefa000 ---p 0000a000 fd:00 234803     /lib64/libnss_files-2.7.so
2aaaaaefa000-2aaaaaefb000 r--p 00009000 fd:00 234803     /lib64/libnss_files-2.7.so
2aaaaaefb000-2aaaaaefc000 rw-p 0000a000 fd:00 234803     /lib64/libnss_files-2.7.so
2aaaaaefc000-2aaaaaf00000 r-xp 00000000 fd:00 235429     /lib64/libnss_dns-2.7.so
2aaaaaf00000-2aaaab0ff000 ---p 00004000 fd:00 235429     /lib64/libnss_dns-2.7.so
2aaaab0ff000-2aaaab100000 r--p 00003000 fd:00 235429     /lib64/libnss_dns-2.7.so
2aaaab100000-2aaaab101000 rw-p 00004000 fd:00 235429     /lib64/libnss_dns-2.7.so
2aaaac000000-2aaaae0bb000 rw-p 2aaaac000000 00:00 0
2aaaae0bb000-2aaab0000000 ---p 2aaaae0bb000 00:00 0
2aaab0000000-2aaab040f000 rw-p 2aaab0000000 00:00 0
2aaab040f000-2aaab4000000 ---p 2aaab040f000 00:00 0
2b19efa46000-2b19efa61000 r-xp 00000000 fd:00 235584     /lib64/ld-2.7.so
2b19efa61000-2b19efa63000 rw-p 2b19efa61000 00:00 0
2b19efc60000-2b19efc61000 r--p 0001a000 fd:00 235584     /lib64/ld-2.7.so
2b19efc61000-2b19efc62000 rw-p 0001b000 fd:00 235584     /lib64/ld-2.7.so
2b19efc62000-2b19efe7b000 r-xp 00000000 fd:00 835152     /usr/lib64/qt4/libQtCore.so.4.4.0 (deleted)
2b19efe7b000-2b19f007a000 ---p 00219000 fd:00 835152     /usr/lib64/qt4/libQtCore.so.4.4.0 (deleted)
2b19f007a000-2b19f0083000 r--p 00218000 fd:00 835152     /usr/lib64/qt4/libQtCore.so.4.4.0 (deleted)
2b19f0083000-2b19f0084000 rw-p 00221000 fd:00 835152     /usr/lib64/qt4/libQtCore.so.4.4.0 (deleted)
2b19f0084000-2b19f0085000 rw-p 2b19f0084000 00:00 0
2b19f0085000-2b19f0099000 r-xp 00000000 fd:00 91188      /lib64/libz.so.1.2.3
2b19f0099000-2b19f0198000 ---p 00014000 fd:00 91188      /lib64/libz.so.1.2.3
2b19f0198000-2b19f0199000 rw-p 00013000 fd:00 91188      /lib64/libz.so.1.2.3
2b19f0199000-2b19f01a1000 r-xp 00000000 fd:00 235497     /lib64/librt-2.7.so
2b19f01a1000-2b19f03a0000 ---p 00008000 fd:00 235497     /lib64/librt-2.7.so
2b19f03a0000-2b19f03a1000 r--p 00007000 fd:00 235497     /lib64/librt-2.7.so
2b19f03a1000-2b19f03a2000 rw-p 00008000 fd:00 235497     /lib64/librt-2.7.so
2b19f03a2000-2b19f03b8000 r-xp 00000000 fd:00 234573     /lib64/libpthread-2.7.so
2b19f03b8000-2b19f05b7000 ---p 00016000 fd:00 234573     /lib64/libpthread-2.7.so
2b19f05b7000-2b19f05b8000 r--p 00015000 fd:00 234573     /lib64/libpthread-2.7.so
2b19f05b8000-2b19f05b9000 rw-p 00016000 fd:00 234573     /lib64/libpthread-2.7.so
2b19f05b9000-2b19f05be000 rw-p 2b19f05b9000 00:00 0
2b19f05be000-2b19f05c0000 r-xp 00000000 fd:00 235436     /lib64/libdl-2.7.so
2b19f05c0000-2b19f07c0000 ---p 00002000 fd:00 235436     /lib64/libdl-2.7.so
2b19f07c0000-2b19f07c1000 r--p 00002000 fd:00 235436     /lib64/libdl-2.7.so
2b19f07c1000-2b19f07c2000 rw-p 00003000 fd:00 235436     /lib64/libdl-2.7.so
```

History

#1 - 12/28/2008 01:51 AM - Sputnick

- Priority changed from High to Normal

#2 - 01/26/2009 12:21 AM - EgS

- Status changed from New to Rejected

- Version set to 0.3.1+

since this was more a reminder to myself and it never occured again, I'm closing this BR. Actually this looks pretty much like a NAQP.