Quassel IRC - Bug #1089

Preview of website with WebGL makes Quassel crash

08/02/2011 01:23 PM - quazgar

Status:	Resolved	**Start date:**	08/02/2011
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	0.7.4		
Version:	0.7.2	**OS:**	Any

Description

Application: quassel (v0.7.2 (dist-f93ace0))
KDE Platform Version: 4.6.2 (4.6.2)
Qt Version: 4.7.2
Operating System: Linux 2.6.38-10-generic x86_64
Distribution: Ubuntu 11.04

-- Information about the crash:

Quassel crashes on Kubuntu 11.04 when trying to display a preview
(hovering the mouse over the link) of a web page which happens to
contain some WebGL code. The backtrace follows.

Reproducible: Yes, every time.

Example link to make Quassel crash:
http://www.ibiblio.org/e-notes/webgl/gpu/waves/barkley.html

```
-- Backtrace:
Application: Quassel IRC (quassel), signal: Aborted
[Current thread is 1 (Thread 0x7f8b61992820 (LWP 25052))]

Thread 7 (Thread 0x7f8b44a2e700 (LWP 25053)):
#0  __lll_lock_wait_private () at ../nptl/sysdeps/unix/sysv/linux/x86_64/lowlevellock.S:97
#1  0x00007f8b5b36f845 in _L_lock_12280 () from /lib/x86_64-linux-gnu/libc.so.6
#2  0x00007f8b5b36dafd in __libc_realloc (oldmem=0x7f8b5b6801c0, bytes=1024) at malloc.c:3813
#3  0x00007f8b613eb9bb in QString::realloc (this=0x2803478, alloc=496) at tools/qstring.cpp:1319
#4  0x00007f8b613ebe0f in QString::append (this=0x2803478, str=...) at tools/qstring.cpp:1534
#5  0x00007f8b614374e0 in write (this=0x2803480, string=<value optimized out>) at io/qtextstream.cpp:915
#6  putString (this=0x2803480, string=<value optimized out>) at io/qtextstream.cpp:996
#7  QTextStream::operator<< (this=0x2803480, string=<value optimized out>) at io/qtextstream.cpp:2525
#8  0x0000000000520466 in ?? ()
#9  0x00007f8b6139aa7e in qt_message_output (msgType=QtWarningMsg, buf=<value optimized out>) at global/qglobal.cpp:2228
#10 0x00007f8b6139ac8f in qt_message(QtMsgType, const char *, typedef __va_list_tag __va_list_tag *) (msgType=QtWarningMsg,
msg=0x7f8b61548970 "QSocketNotifier: Invalid socket %d and type '%s', disabling...", ap=0x7f8b44a2da90) at
global/qglobal.cpp:2328
#11 0x00007f8b6139b3f1 in qWarning (msg=<value optimized out>) at global/qglobal.cpp:2410
#12 0x00007f8b614b5e4c in socketNotifierSourceCheck (source=0x2b1b680) at kernel/qeventdispatcher_glib.cpp:90
#13 0x00007f8b5aa1f854 in g_main_context_check () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#14 0x00007f8b5aa20122 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#15 0x00007f8b5aa20639 in g_main_context_iteration () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#16 0x00007f8b614b63ef in QEventDispatcherGlib::processEvents (this=0x2b1bac0, flags=<value optimized out>) at
kernel/qeventdispatcher_glib.cpp:422
#17 0x00007f8b6148a882 in QEventLoop::processEvents (this=<value optimized out>, flags=...) at kernel/qeventloop.cpp:149
#18 0x00007f8b6148aabc in QEventLoop::exec (this=0x7f8b44a2dd30, flags=...) at kernel/qeventloop.cpp:201
#19 0x00007f8b613a1924 in QThread::exec (this=<value optimized out>) at thread/qthread.cpp:492
#20 0x00007f8b6146cc2f in QInotifyFileSystemWatcherEngine::run (this=0x2b1afe0) at io/qfilesystemwatcher_inotify.cpp:248
#21 0x00007f8b613a4175 in QThreadPrivate::start (arg=0x2b1afe0) at thread/qthread_unix.cpp:320
#22 0x00007f8b5da0ad8c in start_thread (arg=0x7f8b44a2e700) at pthread_create.c:304
#23 0x00007f8b5b3d704d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:112
#24 0x0000000000000000 in ?? ()
```

```
Thread 6 (Thread 0x7f8b3f7fe700 (LWP 25055)):
#0  0x00007f8b5b3c9f03 in __poll (fds=<value optimized out>, nfds=<value optimized out>, timeout=<value optimized out>) at
../sysdeps/unix/sysv/linux/poll.c:87
#1  0x00007f8b5aa20104 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#2  0x00007f8b5aa209f2 in g_main_loop_run () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#3  0x00007f8b55876c44 in ?? () from /usr/lib/x86_64-linux-gnu/libgio-2.0.so.0
#4  0x00007f8b5aa473e4 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#5  0x00007f8b5da0ad8c in start_thread (arg=0x7f8b3f7fe700) at pthread_create.c:304
#6  0x00007f8b5b3d704d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:112
#7  0x0000000000000000 in ?? ()

Thread 5 (Thread 0x7f8b3ea1b700 (LWP 25056)):
#0  __lll_lock_wait_private () at ../nptl/sysdeps/unix/sysv/linux/x86_64/lowlevellock.S:97
#1  0x00007f8b5b36f845 in _L_lock_12280 () from /lib/x86_64-linux-gnu/libc.so.6
#2  0x00007f8b5b36dafd in __libc_realloc (oldmem=0x7f8b5b6801c0, bytes=1024) at malloc.c:3813
#3  0x00007f8b613eb9bb in QString::realloc (this=0x2803478, alloc=496) at tools/qstring.cpp:1319
#4  0x00007f8b613ebe0f in QString::append (this=0x2803478, str=...) at tools/qstring.cpp:1534
#5  0x00007f8b614374e0 in write (this=0x2803480, string=<value optimized out>) at io/qtextstream.cpp:915
#6  putString (this=0x2803480, string=<value optimized out>) at io/qtextstream.cpp:996
#7  QTextStream::operator<< (this=0x2803480, string=<value optimized out>) at io/qtextstream.cpp:2525
#8  0x0000000000520466 in ?? ()
#9  0x00007f8b6139aa7e in qt_message_output (msgType=QtWarningMsg, buf=<value optimized out>) at global/qglobal.cpp:2228
#10 0x00007f8b6139ac8f in qt_message(QtMsgType, const char *, typedef __va_list_tag __va_list_tag *) (msgType=QtWarningMsg,
msg=0x7f8b61548970 "QSocketNotifier: Invalid socket %d and type '%s', disabling...", ap=0x7f8b3ea1aaa0) at
global/qglobal.cpp:2328
#11 0x00007f8b6139b3f1 in qWarning (msg=<value optimized out>) at global/qglobal.cpp:2410
#12 0x00007f8b614b5e4c in socketNotifierSourceCheck (source=0x2bbb8b0) at kernel/qeventdispatcher_glib.cpp:90
#13 0x00007f8b5aa1f854 in g_main_context_check () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#14 0x00007f8b5aa20122 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#15 0x00007f8b5aa20639 in g_main_context_iteration () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#16 0x00007f8b614b63ef in QEventDispatcherGlib::processEvents (this=0x2bf9c60, flags=<value optimized out>) at
kernel/qeventdispatcher_glib.cpp:422
#17 0x00007f8b6148a882 in QEventLoop::processEvents (this=<value optimized out>, flags=...) at kernel/qeventloop.cpp:149
#18 0x00007f8b6148aabc in QEventLoop::exec (this=0x7f8b3ea1ad40, flags=...) at kernel/qeventloop.cpp:201
#19 0x00007f8b613a1924 in QThread::exec (this=<value optimized out>) at thread/qthread.cpp:492
#20 0x000000000056aed3 in ?? ()
#21 0x00007f8b613a4175 in QThreadPrivate::start (arg=0x2bf9c20) at thread/qthread_unix.cpp:320
#22 0x00007f8b5da0ad8c in start_thread (arg=0x7f8b3ea1b700) at pthread_create.c:304
#23 0x00007f8b5b3d704d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:112
#24 0x0000000000000000 in ?? ()

Thread 4 (Thread 0x7f8b3e21a700 (LWP 25057)):
#0  pthread_cond_wait@@GLIBC_2.3.2 () at ../nptl/sysdeps/unix/sysv/linux/x86_64/pthread_cond_wait.S:162
#1  0x00007f8b600372a2 in QTWTF::TCMalloc_PageHeap::scavengerThread (this=0x7f8b60350180) at
../3rdparty/javascriptcore/JavaScriptCore/wtf/FastMalloc.cpp:2359
#2  0x00007f8b600372d9 in QTWTF::TCMalloc_PageHeap::runScavengerThread (context=0x7f8b6035e254) at
../3rdparty/javascriptcore/JavaScriptCore/wtf/FastMalloc.cpp:1464
#3  0x00007f8b5da0ad8c in start_thread (arg=0x7f8b3e21a700) at pthread_create.c:304
#4  0x00007f8b5b3d704d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:112
#5  0x0000000000000000 in ?? ()

Thread 3 (Thread 0x7f8b3ce9d700 (LWP 29249)):
#0  pthread_cond_wait@@GLIBC_2.3.2 () at ../nptl/sysdeps/unix/sysv/linux/x86_64/pthread_cond_wait.S:162
#1  0x00007f8b5f1a6832 in ?? () from /usr/lib/libQtWebKit.so.4
#2  0x00007f8b5da0ad8c in start_thread (arg=0x7f8b3ce9d700) at pthread_create.c:304
#3  0x00007f8b5b3d704d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:112
#4  0x0000000000000000 in ?? ()

Thread 2 (Thread 0x7f8b3ffff700 (LWP 29250)):
#0  pthread_cond_timedwait@@GLIBC_2.3.2 () at ../nptl/sysdeps/unix/sysv/linux/x86_64/pthread_cond_timedwait.S:216
#1  0x00007f8b613a479e in wait (this=<value optimized out>, mutex=0x2d9b0a0, time=30000) at thread/qwaitcondition_unix.cpp:86
#2  QWaitCondition::wait (this=<value optimized out>, mutex=0x2d9b0a0, time=30000) at thread/qwaitcondition_unix.cpp:160
#3  0x00007f8b61399218 in QThreadPoolThread::run (this=0x2d9ac10) at concurrent/qthreadpool.cpp:140
#4  0x00007f8b613a4175 in QThreadPrivate::start (arg=0x2d9ac10) at thread/qthread_unix.cpp:320
#5  0x00007f8b5da0ad8c in start_thread (arg=0x7f8b3ffff700) at pthread_create.c:304
#6  0x00007f8b5b3d704d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:112
#7  0x0000000000000000 in ?? ()
```

```
Thread 1 (Thread 0x7f8b61992820 (LWP 25052)):
[KCrash Handler]
#6  0x00007f8b5b324d05 in raise (sig=6) at ../nptl/sysdeps/unix/sysv/linux/raise.c:64
#7  0x00007f8b5b328ab6 in abort () at abort.c:92
#8  0x00007f8b5b35dd7b in __libc_message (do_abort=2, fmt=0x7f8b5b446400 "*** glibc detected * s: %s: 0x%s \n") at ../sysdeps/unix/sysv/linux/libc_fatal.c:189
#9  0x00007f8b5b369a8f in malloc_printerr (av=<value optimized out>, p=0x7fffe9ed5810) at malloc.c:6283
#10 _int_free (av=<value optimized out>, p=0x7fffe9ed5810) at malloc.c:4795
#11 0x00007f8b5b36d8e3 in __libc_free (mem=<value optimized out>) at malloc.c:3738
#12 0x00007f8b6149dc14 in QObjectPrivate::deleteChildren (this=0x2f99680) at kernel/qobject.cpp:1964
#13 0x00007f8b60894ef2 in QWidget::~QWidget (this=0x31cab70, __in_chrg=<value optimized out>) at kernel/qwidget.cpp:1631
#14 0x00007f8b5ef11b99 in QWebView::~QWebView() () from /usr/lib/libQtWebKit.so.4
#15 0x00007f8b60e35144 in QGraphicsProxyWidget::~QGraphicsProxyWidget (this=<value optimized out>, __in_chrg=<value optimized out>) at graphicsview/qgraphicsproxywidget.cpp:554
#16 0x00007f8b60e35199 in QGraphicsProxyWidget::~QGraphicsProxyWidget (this=0x7f8b38004820, __in_chrg=<value optimized out>) at graphicsview/qgraphicsproxywidget.cpp:556
#17 0x00007f8b60e22275 in QGraphicsItem::~QGraphicsItem (this=0x3173a30, __in_chrg=<value optimized out>) at graphicsview/qgraphicsitem.cpp:1481
#18 0x00000000004dbd69 in ?? ()
#19 0x00000000004bbba8 in ?? ()
#20 0x00000000004dd9f3 in ?? ()
#21 0x00007f8b614a05f8 in QMetaObject::activate (sender=0x2e18240, m=<value optimized out>, local_signal_index=<value optimized out>, argv=0x0) at kernel/qobject.cpp:3287
#22 0x00007f8b6149f1c9 in QObject::event (this=0x2e18240, e=<value optimized out>) at kernel/qobject.cpp:1190
#23 0x00007f8b608489f4 in QApplicationPrivate::notify_helper (this=0x2746240, receiver=0x2e18240, e=0x7fffe9ed5530) at kernel/qapplication.cpp:4462
#24 0x00007f8b6084d3ba in QApplication::notify (this=<value optimized out>, receiver=0x2e18240, e=0x7fffe9ed5530) at kernel/qapplication.cpp:4341
#25 0x00007f8b5cee2866 in KApplication::notify (this=0x7fffe9ed6eb0, receiver=0x2e18240, event=0x7fffe9ed5530) at ../../kdeui/kernel/kapplication.cpp:311
#26 0x00007f8b6148b49c in QCoreApplication::notifyInternal (this=0x7fffe9ed6eb0, receiver=0x2e18240, event=0x7fffe9ed5530) at kernel/qcoreapplication.cpp:731
#27 0x00007f8b614b8f12 in sendEvent (this=0x274fc30) at ../../include/QtCore/../../src/corelib/kernel/qcoreapplication.h:215
#28 QTimerInfoList::activateTimers (this=0x274fc30) at kernel/qeventdispatcher_unix.cpp:604
#29 0x00007f8b614b5d18 in timerSourceDispatch (source=<value optimized out>) at kernel/qeventdispatcher_glib.cpp:184
#30 idleTimerSourceDispatch (source=<value optimized out>) at kernel/qeventdispatcher_glib.cpp:231
#31 0x00007f8b5aa1fbcd in g_main_context_dispatch () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#32 0x00007f8b5aa203a8 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#33 0x00007f8b5aa20639 in g_main_context_iteration () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#34 0x00007f8b614b63ef in QEventDispatcherGlib::processEvents (this=0x26f4350, flags=<value optimized out>) at kernel/qeventdispatcher_glib.cpp:422
#35 0x00007f8b608f24de in QGuiEventDispatcherGlib::processEvents (this=<value optimized out>, flags=<value optimized out>) at kernel/qguieventdispatcher_glib.cpp:204
#36 0x00007f8b6148a882 in QEventLoop::processEvents (this=<value optimized out>, flags=...) at kernel/qeventloop.cpp:149
#37 0x00007f8b6148aabc in QEventLoop::exec (this=0x7fffe9ed57a0, flags=...) at kernel/qeventloop.cpp:201
#38 0x00007f8b60d09fd6 in QDialog::exec (this=0x7fffe9ed5820) at dialogs/qdialog.cpp:552
#39 0x00007f8b60d2a4a2 in showNewMessageBox (parent=<value optimized out>, icon=<value optimized out>, title=<value optimized out>, text=<value optimized out>, buttons=..., defaultButton=QMessageBox::NoButton) at dialogs/qmessagebox.cpp:1531
#40 0x00007f8b60d2a5ff in QMessageBox::information (parent=<value optimized out>, title=<value optimized out>, text=<value optimized out>, buttons=<value optimized out>, defaultButton=<value optimized out>) at dialogs/qmessagebox.cpp:1560
#41 0x00007f8b5ef0c4e1 in QWebPage::javaScriptAlert(QWebFrame, QString constx%x) () from /usr/lib/libQtWebKit.so.4
#42 0x00007f8b5eee7e0f in ?? () from /usr/lib/libQtWebKit.so.4
#43 0x00007f8b5ed25eb0 in ?? () from /usr/lib/libQtWebKit.so.4
#44 0x00007f8b5e8134ef in ?? () from /usr/lib/libQtWebKit.so.4
#45 0x00007f8b617e31b4 in ?? ()
#46 0x00007f8b36f36110 in ?? ()
#47 0x0000000000000001 in ?? ()
#48 0x0000000000000000 in ?? ()
```

Related issues:

Has duplicate Quassel IRC - Bug #1134: Quassel client crashes after generatin...	**Closed**	**01/17/2012**

Associated revisions

Revision 54a5d32d35101d5fbcb2687665d52415ca3a6aca - 01/20/2012 07:27 PM - kode54

Disables JavaScript, which fixes #1089 and other issues related to modal dialogs inside the preview crashing when the preview is destroyed.

Revision 54a5d32d - 01/20/2012 07:27 PM - kode54

Disables JavaScript, which fixes #1089 and other issues related to modal dialogs inside the preview crashing when the preview is destroyed.

Revision ebbf83b1e06bde94deaab15f5d4f10f29cf1fab2 - 01/21/2012 08:09 PM - kode54

Disables JavaScript, which fixes #1089 and other issues related to modal dialogs inside the preview crashing when the preview is destroyed.

Revision ebbf83b1 - 01/21/2012 08:09 PM - kode54

Disables JavaScript, which fixes #1089 and other issues related to modal dialogs inside the preview crashing when the preview is destroyed.

History

#1 - 01/21/2012 08:09 PM - kode54

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset 54a5d32d35101d5fbcb2687665d52415ca3a6aca.

#2 - 01/21/2012 08:39 PM - johu

- Target version set to 0.7.4