Quassel IRC - Bug #1134

Quassel client crashes after generating preview for URL http://odbl.poole.ch/germany-20111208-20120111-poly.html

01/17/2012 02:01 PM - eliasp

Status:	Closed	**Start date:**	01/17/2012
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Quassel Client	**Estimated time:**	0.00 hour
Target version:			
Version:	0.7.2	**OS:**	Linux

Description

Application: quasselclient (v0.7.3 (dist-7db97a6))
KDE Platform Version: 4.7.97 (4.8 RC2 (4.7.97) (Compiled from sources)
Qt Version: 4.7.4
Operating System: Linux 3.1.6-gentoo x86_64
Distribution: "Gentoo Base System release 2.0.3"

-- Information about the crash:
Someone posted the URL http://odbl.poole.ch/germany-20111208-20120111-poly.html in an IRC channel which loads a very huge page containing OpenStreetMap statistics.

I hovered the link and saw the preview for some seconds, before I continued to move the cursor.

Around 5 seconds later, QuasselClient crashed.

The crash can be reproduced every time.

-- Backtrace:
Application: Quassel IRC (quasselclient), signal: Aborted
[Current thread is 1 (Thread 0x7f1b04ffd760 (LWP 30963))]

Thread 3 (Thread 0x7f1aeb941700 (LWP 30992)):
#0 pthread_cond_wait () at ../nptl/sysdeps/unix/sysv/linux/x86_64/pthread_cond_wait.S:162
#1 0x00007f1b02f69ee4 in scavengerThread (this=0x7f1b037caf00) at wtf/FastMalloc.cpp:2378
#2 WTF::TCMalloc_PageHeap::runScavengerThread (context=0x7f1b037caf00) at wtf/FastMalloc.cpp:1497
#3 0x00007f1affcf0a35 in start_thread (arg=0x7f1aeb941700) at pthread_create.c:301
#4 0x00007f1b006ff43d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:115

Thread 2 (Thread 0x7f1aeb040700 (LWP 30993)):
#0 0x00007f1b006f72fb in *__GI__poll (fds=<optimized out>, nfds=<optimized out>, timeout=<optimized out>) at ../sysdeps/unix/sysv/linux/poll.c:87
#1 0x00007f1afff48585 in g_main_context_poll (n_fds=1, fds=0x7f1aec003b80, timeout=<optimized out>, context=0x122b120, priority=<optimized out>) at gmain.c:3402
#2 g_main_context_iterate (context=0x122b120, block=1, dispatch=1, self=<optimized out>) at gmain.c:3084
#3 0x00007f1afff489a4 in g_main_context_iteration (context=0x122b120, may_block=1) at gmain.c:3152
#4 0x00007f1b04b2db74 in QEventDispatcherGlib::processEvents (this=0x17c2a90, flags=<optimized out>) at kernel/qeventdispatcher_glib.cpp:424
#5 0x00007f1b04b06268 in QEventLoop::processEvents (this=<optimized out>, flags=...) at kernel/qeventloop.cpp:149
#6 0x00007f1b04b0645f in QEventLoop::exec (this=0x7f1aeb03fe20, flags=...) at kernel/qeventloop.cpp:201
#7 0x00007f1b04a2f6a1 in QThread::exec (this=<optimized out>) at thread/qthread.cpp:498
#8 0x00007f1b04a31ae3 in QThreadPrivate::start (arg=0x15ae170) at thread/qthread_unix.cpp:331
#9 0x00007f1affcf0a35 in start_thread (arg=0x7f1aeb040700) at pthread_create.c:301
#10 0x00007f1b006ff43d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:115

Thread 1 (Thread 0x7f1b04ffd760 (LWP 30963)):
[KCrash Handler]
#6 0x00007f1b00662cd5 in ***__GI__raise (sig=6) at ../nptl/sysdeps/unix/sysv/linux/raise.c:64***
#7 ***0x00007f1b00663eef in *__GI_abort () at abort.c:92***
#8 **0x00007f1b0069b2ee in __libc_message (do_abort=2, fmt=0x7f1b0076e778 "**** glibc detected * **%s: %s: 0x%s** *\n") at ../sysdeps/unix/sysv/linux/libc_fatal.c:186

#9 0x00007f1b0069fd0e in malloc_printerr (action=3, str=0x7f1b0076e868 "munmap_chunk(): invalid pointer", ptr=<optimized out>) at malloc.c:6283
#10 0x00007f1b04b17857 in QObjectPrivate::deleteChildren (this=0x5643ad0) at kernel/qobject.cpp:1955
#11 0x00007f1b03f96a69 in QWidget::~QWidget (this=0x560e500, __in_chrg=<optimized out>) at kernel/qwidget.cpp:1651
#12 0x00007f1b02d04f7f in QWebView::~QWebView (this=0x560e500, __in_chrg=<optimized out>) at ../WebKit/qt/Api/qwebview.cpp:335
#13 0x00007f1b044afc56 in QGraphicsProxyWidget::~QGraphicsProxyWidget (this=<optimized out>, __in_chrg=<optimized out>) at graphicsview/qgraphicsproxywidget.cpp:554
#14 0x00007f1b044afc93 in QGraphicsProxyWidget::~QGraphicsProxyWidget (this=0x7f1aec02ef40, __in_chrg=<optimized out>) at graphicsview/qgraphicsproxywidget.cpp:556
#15 0x00007f1b0449e6d5 in QGraphicsItem::~QGraphicsItem (this=0x5630610, __in_chrg=<optimized out>) at graphicsview/qgraphicsitem.cpp:1488
#16 0x000000000050384a in WebPreviewItem::~WebPreviewItem (this=0x78f3, __in_chrg=<optimized out>) at /var/tmp/portage/net-irc/quassel-0.7.3/work/quassel-0.7.3/src/qtui/webpreviewitem.h:28
#17 0x00000000004db918 in ChatScene::webPreviewNextStep (this=0x39a03d0) at /var/tmp/portage/net-irc/quassel-0.7.3/work/quassel-0.7.3/src/qtui/chatscene.cpp:1105
#18 0x0000000000505a98 in ChatScene::qt_metacall (this=0x39a03d0, _c=QMetaObject::InvokeMetaMethod, _id=6, _a=0x7fff38eb67b0) at /var/tmp/portage/net-irc/quassel-0.7.3/work/quassel-0.7.3_build/src/qtui/moc_chatscene.cxx:165
#19 0x00007f1b04b193e0 in QMetaObject::activate (sender=0x39a0510, m=<optimized out>, local_signal_index=<optimized out>, argv=0x0) at kernel/qobject.cpp:3278
#20 0x00007f1b04b18c17 in QObject::event (this=0x39a0510, e=<optimized out>) at kernel/qobject.cpp:1181
#21 0x00007f1b03f521f8 in QApplicationPrivate::notify_helper (this=0x8bb3c0, receiver=0x39a0510, e=0x7fff38eb6ef0) at kernel/qapplication.cpp:4481
#22 0x00007f1b03f568b0 in QApplication::notify (this=<optimized out>, receiver=0x39a0510, e=0x7fff38eb6ef0) at kernel/qapplication.cpp:4360
#23 0x00007f1b015fa600 in KApplication::notify (this=0x7fff38eb91a0, receiver=0x39a0510, event=0x7fff38eb6ef0) at /var/tmp/portage/kde-base/kdelibs-4.7.97-r1/work/kdelibs-4.7.97/kdeui/kernel/kapplication.cpp:311
#24 0x00007f1b04b06ce0 in QCoreApplication::notifyInternal (this=0x7fff38eb91a0, receiver=0x39a0510, event=0x7fff38eb6ef0) at kernel/qcoreapplication.cpp:787
#25 0x00007f1b04b30269 in sendEvent (event=0x7fff38eb6ef0, receiver=<optimized out>) at kernel/qcoreapplication.h:215
#26 QTimerInfoList::activateTimers (this=0x8be0d0) at kernel/qeventdispatcher_unix.cpp:603
#27 0x00007f1b04b2d544 in timerSourceDispatch (source=<optimized out>) at kernel/qeventdispatcher_glib.cpp:184
#28 0x00007f1afff480a2 in g_main_dispatch (context=0x8bdc00) at gmain.c:2441
#29 g_main_context_dispatch (context=0x8bdc00) at gmain.c:3011
#30 0x00007f1afff487e8 in g_main_context_iterate (context=0x8bdc00, block=1, dispatch=1, self=<optimized out>) at gmain.c:3089
#31 0x00007f1afff489a4 in g_main_context_iteration (context=0x8bdc00, may_block=1) at gmain.c:3152
#32 0x00007f1b04b2db3c in QEventDispatcherGlib::processEvents (this=0x89ccf0, flags=<optimized out>) at kernel/qeventdispatcher_glib.cpp:422
#33 0x00007f1b03fe94c6 in QGuiEventDispatcherGlib::processEvents (this=<optimized out>, flags=<optimized out>) at kernel/qguieventdispatcher_glib.cpp:204
#34 0x00007f1b04b06268 in QEventLoop::processEvents (this=<optimized out>, flags=...) at kernel/qeventloop.cpp:149
#35 0x00007f1b04b0645f in QEventLoop::exec (this=0x7fff38eb7180, flags=...) at kernel/qeventloop.cpp:201
#36 0x00007f1b0439d30a in QDialog::exec (this=0x7fff38eb7200) at dialogs/qdialog.cpp:552
#37 0x00007f1b043bab7e in QMessageBoxPrivate::showOldMessageBox (parent=<optimized out>, icon=<optimized out>, title=<optimized out>, text=<optimized out>, button0=16384, button1=65536, button2=0) at dialogs/qmessagebox.cpp:1923
#38 0x00007f1b043bad89 in showNewMessageBox (parent=<optimized out>, icon=<optimized out>, title=<optimized out>, text=<optimized out>, buttons=..., defaultButton=QMessageBox::No) at dialogs/qmessagebox.cpp:1518
#39 0x00007f1b043bae65 in QMessageBox::information (parent=<optimized out>, title=<optimized out>, text=<optimized out>, buttons=<optimized out>, defaultButton=<optimized out>) at dialogs/qmessagebox.cpp:1573
#40 0x00007f1b02cff4c9 in information (button1=QMessageBox::No, button0=QMessageBox::Yes, text=..., title=..., parent=0x560e500) at ../../../../include/QtGui/../../src/gui/dialogs/qmessagebox.h:230
#41 QWebPage::shouldInterruptJavaScript (this=<optimized out>) at ../WebKit/qt/Api/qwebpage.cpp:2151
#42 0x00007f1b02cff8da in QWebPage::qt_metacall (this=0x1ef94f0, _c=QMetaObject::InvokeMetaMethod, _id=23, _a=0x7fff38eb74f0) at .moc/release-shared/moc_qwebpage.cpp:288
#43 0x00007f1b04b0ea27 in QMetaMethod::invoke (this=0x7fff38eb7970, object=0x1ef94f0, connectionType=Qt::DirectConnection, returnValue=..., val0=..., val1=..., val2=..., val3=..., val4=..., val5=..., val6=..., val7=..., val8=..., val9=...) at kernel/qmetaobject.cpp:1597
#44 0x00007f1b04b0f5df in QMetaObject::invokeMethod (obj=0x1ef94f0, member=<optimized out>, type=Qt::DirectConnection, ret=..., val0=..., val1=..., val2=..., val3=..., val4=..., val5=..., val6=..., val7=..., val8=..., val9=...) at kernel/qmetaobject.cpp:1151
#45 0x00007f1b02cde410 in WebCore::ChromeClientQt::shouldInterruptJavaScript (this=<optimized out>) at ../WebKit/qt/WebCoreSupport/ChromeClientQt.cpp:328
#46 0x00007f1b02b3df64 in WebCore::Chrome::shouldInterruptJavaScript (this=0x7f1ae5bed390) at page/Chrome.cpp:317
#47 0x00007f1b02f5bf49 in JSC::TimeoutChecker::didTimeOut (this=0x7f1aeb0a0218, exec=0x7f1ae9bb2220) at runtime/TimeoutChecker.cpp:146
#48 0x00007f1b02ec93b8 in JSC::cti_timeout_check (args=0x7fff38eb7c40) at jit/JITStubs.cpp:1098
#49 0x00007f1ac7889e58 in ?? ()
#50 0x00007f1b04e77478 in ?? ()

#51 0x00007f1ac78326c0 in ?? ()
#52 0x00007f1ae6ef4758 in ?? ()
#53 0x00007f1ae6ef4778 in ?? ()
#54 0x00007f1ac788c26e in ?? ()
#55 0x0000000200000008 in ?? ()
#56 0x7fffffff00000003 in ?? ()
#57 0x00007f1ae5dc9d90 in ?? ()
#58 0x00007f1ae5b06d80 in ?? ()
#59 0x00007f1ae9b41eb0 in ?? ()
#60 0x00007f1aeb0531d0 in ?? ()
#61 0x00007f1ae9bb2220 in ?? ()
#62 0x00007f1aeb0a02a0 in ?? ()
#63 0x00007f1b037cad90 in ?? () from /usr/lib64/qt4/libQtWebKit.so.4
#64 0x00007f1aeb09ea00 in ?? ()
#65 0x00007f1aeb0531b8 in ?? ()
#66 0x00007f1aeb0531d0 in ?? ()
#67 0x00007f1b037cad90 in ?? () from /usr/lib64/qt4/libQtWebKit.so.4
#68 0x0000000005644a88 in ?? ()
#69 0x00007f1ae9bb2058 in ?? ()
#70 0x00007f1ae9bb2000 in ?? ()
#71 0x00007f1b02eb56ec in execute (exception=0x7f1aeb0a02a0, globalData=0x7f1aeb09ea00, callFrame=0x0, registerFile=0x7f1ac788c0f2, this=<optimized out>) at jit/JITCode.h:77
#72 JSC::Interpreter::execute (this=0x7f1ac788c0da, functionExecutable=<optimized out>, callFrame=0x7f1ae9bb2220, function=0x7f1ae5fc2c80, thisObj=<optimized out>, args=<optimized out>, scopeChain=0x7f1ae9281ed0, exception=0x7f1aeb0a02a0) at interpreter/Interpreter.cpp:687
#73 0x00007f1b02efe24a in JSC::JSFunction::call (this=0x7f1ae5fc2c80, exec=0x5644a88, thisValue=..., args=...) at runtime/JSFunction.cpp:122
#74 0x00007f1b02ed9438 in JSC::call (exec=<optimized out>, functionObject=<optimized out>, callType=<optimized out>, callData=<optimized out>, thisValue=<optimized out>, args=<optimized out>) at runtime/CallData.cpp:39
#75 0x00007f1b028aaf65 in WebCore::JSEventListener::handleEvent (this=0x7f1ae69a0180, scriptExecutionContext=<optimized out>, event=0x7f1ac7a84780) at bindings/js/JSEventListener.cpp:115
#76 0x00007f1b029810f3 in WebCore::EventTarget::fireEventListeners (this=0x7f1ae6a12c00, event=0x7f1ac7a84780, d=0x7f1ae5ac98c0, entry=...) at dom/EventTarget.cpp:315
#77 0x00007f1b0298121b in WebCore::EventTarget::fireEventListeners (this=0x7f1ae6a12c00, event=0x7f1ac7a84780) at dom/EventTarget.cpp:276
#78 0x00007f1b0298f7f2 in WebCore::Node::dispatchGenericEvent (this=0x7f1ae6a12c00, prpEvent=<optimized out>) at dom/Node.cpp:2644
#79 0x00007f1b0298fcab in WebCore::Node::dispatchEvent (this=0x7f1ae6a12c00, prpEvent=<optimized out>) at dom/Node.cpp:2567
#80 0x00007f1b02961094 in WebCore::Document::finishedParsing (this=0x7f1ae6a12c00) at dom/Document.cpp:4288
#81 0x00007f1b02a97380 in WebCore::HTMLTokenizer::end (this=0x7f1ae68da800) at html/HTMLTokenizer.cpp:1878
#82 0x00007f1b02a9744b in WebCore::HTMLTokenizer::finish (this=0x7f1ae68da800) at html/HTMLTokenizer.cpp:1918
#83 0x00007f1b02af743a in WebCore::FrameLoader::endIfNotLoadingMainResource (this=0x7f1ae5bd8860) at loader/FrameLoader.cpp:971
#84 0x00007f1b02af8c71 in WebCore::FrameLoader::finishedLoading (this=0x7f1ae5bd8860) at loader/FrameLoader.cpp:2770
#85 0x00007f1b02b179fb in WebCore::MainResourceLoader::didFinishLoading (this=0x7f1ae6859d80) at loader/MainResourceLoader.cpp:424
#86 0x00007f1b02cc7f3b in WebCore::QNetworkReplyHandler::finish (this=0x4e89070) at platform/network/qt/QNetworkReplyHandler.cpp:261
#87 0x00007f1b02cc87d3 in WebCore::QNetworkReplyHandler::qt_metacall (this=0x4e89070, _c=QMetaObject::InvokeMetaMethod, _id=<optimized out>, _a=0x7fff38eb8550) at .moc/release-shared/moc_QNetworkReplyHandler.cpp:84
#88 0x00007f1b04b193e0 in QMetaObject::activate (sender=0x562c080, m=<optimized out>, local_signal_index=<optimized out>, argv=0x0) at kernel/qobject.cpp:3278
#89 0x00007f1b03adaf25 in QNetworkReplyImplPrivate::finished (this=0x4c9d4b0) at access/qnetworkreplyimpl.cpp:687
#90 0x00007f1b03ac7db8 in QNetworkAccessHttpBackend::replyFinished (this=0x560bc30) at access/qnetworkaccesshttpbackend.cpp:768
#91 0x00007f1b03ad940f in QNetworkReplyImplPrivate::handleNotifications (this=0x4c9d4b0) at access/qnetworkreplyimpl.cpp:390
#92 0x00007f1b03ad9446 in QNetworkReplyImpl::event (this=<optimized out>, e=<optimized out>) at access/qnetworkreplyimpl.cpp:899
#93 0x00007f1b03f521f8 in QApplicationPrivate::notify_helper (this=0x8bb3c0, receiver=0x562c080, e=0x564aa00) at kernel/qapplication.cpp:4481
#94 0x00007f1b03f568b0 in QApplication::notify (this=<optimized out>, receiver=0x562c080, e=0x564aa00) at kernel/qapplication.cpp:4360
#95 0x00007f1b015fa600 in KApplication::notify (this=0x7fff38eb91a0, receiver=0x562c080, event=0x564aa00) at /var/tmp/portage/kde-base/kdelibs-4.7.97-r1/work/kdelibs-4.7.97/kdeui/kernel/kapplication.cpp:311
#96 0x00007f1b04b06ce0 in QCoreApplication::notifyInternal (this=0x7fff38eb91a0, receiver=0x562c080, event=0x564aa00) at

kernel/qcoreapplication.cpp:787
#97 0x00007f1b04b098e7 in sendEvent (event=0x564aa00, receiver=0x562c080) at kernel/qcoreapplication.h:215
#98 QCoreApplicationPrivate::sendPostedEvents (receiver=0x0, event_type=0, data=0x89d510) at kernel/qcoreapplication.cpp:1428
#99 0x00007f1b04b2da16 in sendPostedEvents () at kernel/qcoreapplication.h:220
#100 postEventSourceDispatch (s=<optimized out>) at kernel/qeventdispatcher_glib.cpp:277
#101 0x00007f1afff480a2 in g_main_dispatch (context=0x8bdc00) at gmain.c:2441
#102 g_main_context_dispatch (context=0x8bdc00) at gmain.c:3011
#103 0x00007f1afff487e8 in g_main_context_iterate (context=0x8bdc00, block=1, dispatch=1, self=<optimized out>) at gmain.c:3089
#104 0x00007f1afff489a4 in g_main_context_iteration (context=0x8bdc00, may_block=1) at gmain.c:3152
#105 0x00007f1b04b2db3c in QEventDispatcherGlib::processEvents (this=0x89ccf0, flags=<optimized out>) at kernel/qeventdispatcher_glib.cpp:422
#106 0x00007f1b03fe94c6 in QGuiEventDispatcherGlib::processEvents (this=<optimized out>, flags=<optimized out>) at kernel/qguieventdispatcher_glib.cpp:204
#107 0x00007f1b04b06268 in QEventLoop::processEvents (this=<optimized out>, flags=...) at kernel/qeventloop.cpp:149
#108 0x00007f1b04b0645f in QEventLoop::exec (this=0x7fff38eb8f70, flags=...) at kernel/qeventloop.cpp:201
#109 0x00007f1b04b09b59 in QCoreApplication::exec () at kernel/qcoreapplication.cpp:1064
#110 0x0000000000437d1a in main (argc=1, argv=<optimized out>) at /var/tmp/portage/net-irc/quassel-0.7.3/work/quassel-0.7.3/src/common/main.cpp:139

Related issues:

Is duplicate of Quassel IRC - Bug #1089: Preview of website with WebGL makes ...	**Resolved**	**08/02/2011**

History

#1 - 01/21/2012 08:48 PM - johu

- Status changed from New to Closed

Please search for open bugs next time.