Quassel IRC - Bug #232

Parting a newly joined channel crashes the client.

07/30/2008 02:19 PM - ZRegis

Status:	Resolved	**Start date:**	
Priority:	High	**Due date:**	
Assignee:	EgS	**% Done:**	0%
Category:	Quassel Client	**Estimated time:**	0.00 hour
Target version:	0.3.0		
Version:	0.13.1	**OS:**	Any

Description

The problem was not occurring before the 25/07/07 git version
and probably caused by bug fixes on the 27/07

Additional information:

The channel is leaved correctly.
then the error occured.

Associated revisions

Revision ff7c0776d68d9749b07f54a3e26c342dfb12f081 - 08/09/2008 04:38 PM - Marcus Eggenberger

fixing segfaults on part if the part results in an empty category (BR #232)

Revision ff7c0776 - 08/09/2008 04:38 PM - Marcus Eggenberger

fixing segfaults on part if the part results in an empty category (BR #232)

History

#1 - 08/05/2008 08:16 PM - Weaselweb

I've generated a backtrace from visual studio (german version), but i've some problems with pdb's, so there are no detailed information about Qtlibs:
QtCored4.dll!671a7269()
[Unten angegebene Rahmen sind möglicherweise nicht korrekt und/oder fehlen, keine Symbole geladen für QtCored4.dll]

quasselclient.exe!AbstractTreeItem::dataChanged(int _t1=0) Zeile 89 + 0x19 Bytes C++

quasselclient.exe!UserCategoryItem::removeUser(IrcUser * ircUser=0x04e183c0) Zeile 603 C++
quasselclient.exe!ChannelBufferItem::removeUserFromCategory(IrcUser * ircUser=0x04e183c0) Zeile 505 + 0xc Bytes C++
quasselclient.exe!ChannelBufferItem::part(IrcUser * ircUser=0x04e183c0) Zeile 491 C++
quasselclient.exe!ChannelBufferItem::qt_metacall(QMetaObject::Call _c=InvokeMetaMethod, int _id=1, void * * _a=0x011fd16c) Zeile 358 + 0x11 Bytes C++
QtCored4.dll!671a6c0e()
QtCored4.dll!671a71f0()
quasselclient.exe!IrcChannel::ircUserParted(IrcUser * _t1=0x04e183c0) Zeile 279 + 0x17 Bytes C++
quasselclient.exe!IrcChannel::part(IrcUser * ircuser=0x04e183c0) Zeile 191 C++
quasselclient.exe!IrcUser::partChannel(IrcChannel * channel=0x054dc8d0) Zeile 234 C++
quasselclient.exe!IrcUser::partChannel(const QString & channelname={...}) Zeile 247 C++
quasselclient.exe!IrcUser::qt_metacall(QMetaObject::Call _c=InvokeMetaMethod, int _id=36, void * * _a=0x011fd414) Zeile 189 + 0xf Bytes C++
quasselclient.exe!SignalProxy::invokeSlot(QObject * receiver=0x04e183c0, int methodId=48, const QList<QVariant> & params={...}, QVariant & returnValue={...}) Zeile 891 + 0x19 Bytes C++
quasselclient.exe!SignalProxy::handleSync(QIODevice * sender=0x017c3fb8, QList<QVariant> params={...}) Zeile 760 + 0x18 Bytes C++
quasselclient.exe!SignalProxy::receivePeerSignal(QIODevice * sender=0x017c3fb8, const QVariant & packedFunc={...}) Zeile 711 C++
quasselclient.exe!SignalProxy::dataAvailable() Zeile 911 + 0x10 Bytes C++
quasselclient.exe!SignalProxy::qt_metacall(QMetaObject::Call _c=InvokeMetaMethod, int _id=5, void * * _a=0x011fd85c) Zeile 94 + 0x8 Bytes C++
QtCored4.dll!671a6c0e()
[snip]

HTH

#2 - 08/05/2008 10:15 PM - Weaselweb

So, here is another one with correct (and full) debugging information in Qt (Hint: Change -Zi to -Z7 in QMAKE_CFLAGS_DEBUG inside qmake.conf)

QtCored4.dll!QMetaObject::activate(QObject * sender=0x055cdcc0, const QMetaObject * m=0x007e13b8, int from_local_signal_index=0, int

to_local_signal_index=1, void * * argv=0x011fced0) Zeile 3093 + 0x8 Bytes C++

quasselclient.exe!AbstractTreeItem::dataChanged(int *t1=0) Zeile 89 + 0x19 Bytes C++*
*quasselclient.exe!UserCategoryItem::removeUser(IrcUser * ircUser=0x04d22f50) Zeile 603 C++*
*quasselclient.exe!ChannelBufferItem::removeUserFromCategory(IrcUser * ircUser=0x04d22f50) Zeile 505 + 0xc Bytes C++*
*quasselclient.exe!ChannelBufferItem::part(IrcUser * ircUser=0x04d22f50) Zeile 491 C++*
*quasselclient.exe!ChannelBufferItem::qt_metacall(QMetaObject::Call _c=InvokeMetaMethod, int _id=1, void * * _a=0x011fd068) Zeile 358 + 0x11 Bytes C++*
*QtCored4.dll!QMetaObject::activate(QObject * sender=0x055de100, int from_signal_index=21, int to_signal_index=21, void * * argv=0x011fd068) Zeile 3007 + 0x2b Bytes C++*
*QtCored4.dll!QMetaObject::activate(QObject * sender=0x055de100, const QMetaObject * m=0x007ada44, int local_signal_index=9, void * * argv=0x011fd068) Zeile 3077 + 0x15 Bytes C++*
*quasselclient.exe!IrcChannel::ircUserParted(IrcUser * _t1=0x04d22f50) Zeile 279 + 0x17 Bytes C++*
*quasselclient.exe!IrcChannel::part(IrcUser * ircuser=0x04d22f50) Zeile 191 C++*
*quasselclient.exe!IrcUser::partChannel(IrcChannel * channel=0x055de100) Zeile 234 C++*
quasselclient.exe!IrcUser::partChannel(const QString & channelname={...}) Zeile 247 C++
*quasselclient.exe!IrcUser::qt_metacall(QMetaObject::Call _c=InvokeMetaMethod, int _id=36, void * * _a=0x011fd310) Zeile 189 + 0xf Bytes C++*
*quasselclient.exe!SignalProxy::invokeSlot(QObject * receiver=0x04d22f50, int methodId=48, const QList<QVariant> & params={...}, QVariant & returnValue={...}) Zeile 891 + 0x19 Bytes C++*
*quasselclient.exe!SignalProxy::handleSync(QIODevice * sender=0x041335e8, QList<QVariant> params={...}) Zeile 760 + 0x18 Bytes C++*
*quasselclient.exe!SignalProxy::receivePeerSignal(QIODevice * sender=0x041335e8, const QVariant & packedFunc={...}) Zeile 711 C++*
quasselclient.exe!SignalProxy::dataAvailable() Zeile 911 + 0x10 Bytes C++
*quasselclient.exe!SignalProxy::qt_metacall(QMetaObject::Call _c=InvokeMetaMethod, int _id=5, void * * _a=0x011fd758) Zeile 94 + 0x8 Bytes C++*
*QtCored4.dll!QMetaObject::activate(QObject * sender=0x041335e8, int from_signal_index=4, int to_signal_index=4, void * * argv=0x00000000) Zeile 3007 + 0x2b Bytes C++*
*QtCored4.dll!QMetaObject::activate(QObject * sender=0x041335e8, const QMetaObject * m=0x6729fd98, int local_signal_index=0, void * * argv=0x00000000) Zeile 3077 + 0x15 Bytes C++*
QtCored4.dll!QIODevice::readyRead() Zeile 83 + 0x12 Bytes C++
QtNetworkd4.dll!QSslSocketPrivate::_q_readyReadSlot() Zeile 2010 C++
*QtNetworkd4.dll!QSslSocket::qt_metacall(QMetaObject::Call _c=InvokeMetaMethod, int _id=15, void * * _a=0x011fd85c) Zeile 113 + 0xf Bytes C++*
*QtCored4.dll!QMetaObject::activate(QObject * sender=0x04135c00, int from_signal_index=4, int to_signal_index=4, void * * argv=0x00000000) Zeile 3007 + 0x2b Bytes C++*
*QtCored4.dll!QMetaObject::activate(QObject * sender=0x04135c00, const QMetaObject * m=0x6729fd98, int local_signal_index=0, void * * argv=0x00000000) Zeile 3077 + 0x15 Bytes C++*
QtCored4.dll!QIODevice::readyRead() Zeile 83 + 0x12 Bytes C++
QtNetworkd4.dll!QAbstractSocketPrivate::canReadNotification() Zeile 575 C++
QtNetworkd4.dll!QAbstractSocketPrivate::readNotification() Zeile 79 + 0x15 Bytes C++
QtNetworkd4.dll!QAbstractSocketEngine::readNotification() Zeile 143 C++
*QtNetworkd4.dll!QReadNotifier::event(QEvent * e=0x011fdcd8) Zeile 975 C++*
*QtGuid4.dll!QApplicationPrivate::notify_helper(QObject * receiver=0x041088d8, QEvent * e=0x011fdcd8) Zeile 3800 + 0x11 Bytes C++*
*QtGuid4.dll!QApplication::notify(QObject * receiver=0x041088d8, QEvent * e=0x011fdcd8) Zeile 3392 + 0x10 Bytes C++*
*QtCored4.dll!QCoreApplication::notifyInternal(QObject * receiver=0x041088d8, QEvent * event=0x011fdcd8) Zeile 591 + 0x15 Bytes C++*
*QtCored4.dll!QCoreApplication::sendEvent(QObject * receiver=0x041088d8, QEvent * event=0x011fdcd8) Zeile 215 + 0x39 Bytes C++*
QtCored4.dll!qt_internal_proc(HWND_* hwnd=0x00330294, unsigned int message=1024, unsigned int wp=656, long lp=1) Zeile 464 + 0xf Bytes
C++
user32.dll!7e368734()
[Unten angegebene Rahmen sind möglicherweise nicht korrekt und/oder fehlen, keine Symbole geladen für user32.dll]
user32.dll!7e368816()
user32.dll!7e3689cd()
user32.dll!7e368a10()
QtCored4.dll!QEventDispatcherWin32::processEvents(QFlags<enum QEventLoop::ProcessEventsFlag> flags={...}) Zeile 743 + 0x21 Bytes C++
QtGuid4.dll!QGuiEventDispatcherWin32::processEvents(QFlags<enum QEventLoop::ProcessEventsFlag> flags={...}) Zeile 1090 + 0x15 Bytes C++
QtCored4.dll!QEventLoop::processEvents(QFlags<enum QEventLoop::ProcessEventsFlag> flags={...}) Zeile 150 C++
QtCored4.dll!QEventLoop::exec(QFlags<enum QEventLoop::ProcessEventsFlag> flags={...}) Zeile 200 + 0x1c Bytes C++
QtCored4.dll!QCoreApplication::exec() Zeile 849 + 0x15 Bytes C++
QtGuid4.dll!QApplication::exec() Zeile 3331 C++
quasselclient.exe!main(int argc=1, char * * argv=0x003e6490) Zeile 163 + 0x8 Bytes C++
quasselclient.exe!WinMain(HINSTANCE__ * instance=0x00400000, HINSTANCE__ * prevInstance=0x00000000, char * *_formal=0x00052367, int cmdShow=1) Zeile 140 + 0x12 Bytes C++*
*quasselclient.exe!*_tmainCRTStartup() Zeile 578 + 0x35 Bytes C
quasselclient.exe!WinMainCRTStartup() Zeile 403 C
kernel32.dll!7c817067()

#3 - 08/08/2008 02:21 PM - EgS

Thanks for all the traces. I finally managed to reproduce the issue myself.

This crash only happens when you part a channel that you just joined in the current session (aka: no reconnect to core after that join)

I'm on it.

#4 - 08/08/2008 02:24 PM - EgS

I just edited the Topic of the bug to better reflect the actual issue and deleted some notes that weren't helping this issue.

#5 - 08/09/2008 04:48 PM - EgS

this should be fixed in current git. please let me know if there are still crashes related to part