Quassel IRC - Bug #682

Core crashes on client connection

04/25/2009 11:28 AM - seezer

Status:	Resolved	**Start date:**	04/25/2009
Priority:	High	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Quassel Core	**Estimated time:**	0.00 hour
Target version:			
Version:	0.5-pre	**OS:**	Any

Description

Sometimes, right after pressing OK on the login credentials dialog, quasselcore crashes.
Only seems to occur on ssl encrypted client<->core connections.

This never happened to me with pre 0.4.0 cores but can't pinpoint any exact version.

Qt versions tested:
Qt 4.4.3 from debian lenny
Qt 4.5.0 built manually

Occured much less often to me since I upgraded to 4.5.0 but might be only coincidence.

Crashes look like:

Quassel IRC: 0.4.0 431ac220d932f46f298f7b43d0754d773a5f8ccc
Quassel IRC: 0.4.0 431ac220d932f46f298f7b43d0754d773a5f8ccc

1. 0 quasselcore 0x000000000059119a Quassel::logBacktrace(QString const&)
2. 1 quasselcore 0x0000000000574e22 Quassel::handleSignal(int)
3. 2 libc.so.6 0x00007f0eead9ff60 0x0000000000000000
4. 3 libz.so.1 0x00007f0eea95c671 0x0000000000000000
5. 4 libz.so.1 0x00007f0eea95d238 0x0000000000000000
6. 5 libz.so.1 0x00007f0eea95a5fc 0x0000000000000000
7. 6 libz.so.1 0x00007f0eea95928d deflate
8. 7 libcrypto.so.0.9.8 0x00007f0ee9b1f88e 0x0000000000000000
9. 8 libcrypto.so.0.9.8 0x00007f0ee9b1f4f2 COMP_compress_block
10. 9 libssl.so.0.9.8 0x00007f0ee9dbb30e ssl3_do_compress
11. 10 libssl.so.0.9.8 0x00007f0ee9dbb45c 0x0000000000000000
12. 11 libssl.so.0.9.8 0x00007f0ee9dbb950 ssl3_write_bytes
13. 12 libQtNetwork.so.4 0x00007f0eebed013f 0x0000000000000000
14. 13 libQtNetwork.so.4 0x00007f0eebecd72c 0x0000000000000000
15. 14 libQtNetwork.so.4 0x00007f0eebec6dbb QSslSocket::flush()
16. 15 libQtNetwork.so.4 0x00007f0eebec6e27 0x0000000000000000
17. 16 libQtNetwork.so.4 0x00007f0eebec706c QSslSocket::qt_metacall(QMetaObject::Call, int, void**)
18. 17 libQtCore.so.4 0x00007f0eec2e2827 QMetaCallEvent::placeMetaCall(QObject*)
19. 18 libQtCore.so.4 0x00007f0eec2e7545 QObject::event(QEvent*)
20. 19 libQtCore.so.4 0x00007f0eec2cd59a QCoreApplicationPrivate::notify_helper(QObject*, QEvent*)
21. 20 libQtCore.so.4 0x00007f0eec2d0b38 QCoreApplication::notify(QObject*, QEvent*)
22. 21 libQtCore.so.4 0x00007f0eec2cf72b QCoreApplication::notifyInternal(QObject*, QEvent*)
23. 22 libQtCore.so.4 0x00007f0eec2d41dd QCoreApplication::sendEvent(QObject*, QEvent*)
24. 23 libQtCore.so.4 0x00007f0eec2cfd00 QCoreApplicationPrivate::sendPostedEvents(QObject*, int, QThreadData*)
25. 24 libQtCore.so.4 0x00007f0eec30834c QEventDispatcherUNIX::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)
26. 25 libQtCore.so.4 0x00007f0eec2cbfcf QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)
27. 26 libQtCore.so.4 0x00007f0eec2cc1de QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>)
28. 27 libQtCore.so.4 0x00007f0eec1b3dee QThread::exec()
29. 28 quasselcore 0x00000000004bfcbd SessionThread::run()
30. 29 libQtCore.so.4 0x00007f0eec1b870f 0x0000000000000000
31. 30 libpthread.so.0 0x00007f0eea534fc7 0x0000000000000000
32. 31 libc.so.6 0x00007f0eeae3d5ad clone

Associated revisions

Revision e042ae69dbe4f42e9e4441f4b5832cfe5ca89067 - 06/28/2009 04:08 PM - Marcus Eggenberger

An attempt to fix #682 - core crash on client connect when using ssl.
As I'm unable to reproduce this bug, I'm just following a hunch here.
Please let me know if it helps. seezer: ping!

Revision e042ae69 - 06/28/2009 04:08 PM - Marcus Eggenberger

An attempt to fix #682 - core crash on client connect when using ssl.
As I'm unable to reproduce this bug, I'm just following a hunch here.
Please let me know if it helps. seezer: ping!

Revision e049ffc61b5e260a49d73102a74c3821af827e77 - 07/12/2009 03:16 PM - Marcus Eggenberger

Fixes #682 - Core crashes on client connection
Big thanks to seezer for debuging and researching!

Revision e049ffc6 - 07/12/2009 03:16 PM - Marcus Eggenberger

Fixes #682 - Core crashes on client connection
Big thanks to seezer for debuging and researching!

Revision 00fcb4ab7fd1a2af1c81d9cab13ee23fb7d7b73c - 07/12/2009 03:19 PM - Marcus Eggenberger

Fixes #682 - Core crashes on client connection
Big thanks to seezer for debuging and researching!

Revision 00fcb4ab - 07/12/2009 03:19 PM - Marcus Eggenberger

Fixes #682 - Core crashes on client connection
Big thanks to seezer for debuging and researching!

History

#1 - 04/25/2009 11:32 AM - Cybertinus

Also have the same problem with Quassel Core on Gentoo.
I've tried it with Qt 4.4 and 4.5.0 (haven't had a chrash with 4.5.1, but that is around for 2 days or so ;)) and both chrashed. I used the Qt versions Gentoo provided.
I just enabled the debug USE-flag on Gentoo. When it chrashes again I will attach that chrashlog.

#2 - 04/26/2009 03:48 PM - seezer

It's always one of two "different" crashlogs.
This is the other one:

Quassel IRC: 0.4.0 431ac220d932f46f298f7b43d0754d773a5f8ccc

1. 0 quasselcore 0x000000000059119a Quassel::logBacktrace(QString const&)
2. 1 quasselcore 0x0000000000574e22 Quassel::handleSignal(int)
3. 2 libc.so.6 0x00007f3cb9663f60 0x0000000000000000
4. 3 libz.so.1 0x00007f3cb9220be9 0x0000000000000000
5. 4 libz.so.1 0x00007f3cb9221052 0x0000000000000000
6. 5 libz.so.1 0x00007f3cb921e5fc 0x0000000000000000
7. 6 libz.so.1 0x00007f3cb921d28d deflate
8. 7 libcrypto.so.0.9.8 0x00007f3cb83e388e 0x0000000000000000
9. 8 libcrypto.so.0.9.8 0x00007f3cb83e34f2 COMP_compress_block
10. 9 libssl.so.0.9.8 0x00007f3cb867f30e ssl3_do_compress
11. 10 libssl.so.0.9.8 0x00007f3cb867f45c 0x0000000000000000
12. 11 libssl.so.0.9.8 0x00007f3cb867f950 ssl3_write_bytes
13. 12 libQtNetwork.so.4 0x00007f3cba79413f 0x0000000000000000
14. 13 libQtNetwork.so.4 0x00007f3cba79172c 0x0000000000000000
15. 14 libQtNetwork.so.4 0x00007f3cba78adbb QSslSocket::flush()
16. 15 libQtNetwork.so.4 0x00007f3cba78ae27 0x0000000000000000
17. 16 libQtNetwork.so.4 0x00007f3cba78b06c QSslSocket::qt_metacall(QMetaObject::Call, int, void**)
18. 17 libQtCore.so.4 0x00007f3cbaba6827 QMetaCallEvent::placeMetaCall(QObject*)
19. 18 libQtCore.so.4 0x00007f3cbabab545 QObject::event(QEvent*)
20. 19 libQtCore.so.4 0x00007f3cbab9159a QCoreApplicationPrivate::notify_helper(QObject*, QEvent*)
21. 20 libQtCore.so.4 0x00007f3cbab94b38 QCoreApplication::notify(QObject*, QEvent*)
22. 21 libQtCore.so.4 0x00007f3cbab9372b QCoreApplication::notifyInternal(QObject*, QEvent*)
23. 22 libQtCore.so.4 0x00007f3cbab981dd QCoreApplication::sendEvent(QObject*, QEvent*)
24. 23 libQtCore.so.4 0x00007f3cbab93d00 QCoreApplicationPrivate::sendPostedEvents(QObject*, int, QThreadData*)
25. 24 libQtCore.so.4 0x00007f3cbabcc34c QEventDispatcherUNIX::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)
26. 25 libQtCore.so.4 0x00007f3cbab8ffcf QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)
27. 26 libQtCore.so.4 0x00007f3cbab901de QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>)

28. 27 libQtCore.so.4 0x00007f3cbaa77dee QThread::exec()
29. 28 quasselcore 0x00000000004bfcbd SessionThread::run()
30. 29 libQtCore.so.4 0x00007f3cbaa7c70f 0x0000000000000000
31. 30 libpthread.so.0 0x00007f3cb8df8fc7 0x0000000000000000
32. 31 libc.so.6 0x00007f3cb97015ad clone
33. 0 quasselcore 0x000000000059119a Quassel::logBacktrace(QString const&)
34. 1 quasselcore 0x0000000000574e22 Quassel::handleSignal(int)
35. 2 libc.so.6 0x00007f3cb9663f60 0x0000000000000000
36. 3 libz.so.1 0x00007f3cb9220671 0x0000000000000000
37. 4 libz.so.1 0x00007f3cb9221238 0x0000000000000000
38. 5 libz.so.1 0x00007f3cb921e5fc 0x0000000000000000
39. 6 libz.so.1 0x00007f3cb921d28d deflate
40. 7 libcrypto.so.0.9.8 0x00007f3cb83e388e 0x0000000000000000
41. 8 libcrypto.so.0.9.8 0x00007f3cb83e34f2 COMP_compress_block
42. 9 libssl.so.0.9.8 0x00007f3cb867f30e ssl3_do_compress
43. 10 libssl.so.0.9.8 0x00007f3cb867f45c 0x0000000000000000
44. 11 libssl.so.0.9.8 0x00007f3cb867f950 ssl3_write_bytes
45. 12 libQtNetwork.so.4 0x00007f3cba79413f 0x0000000000000000
46. 13 libQtNetwork.so.4 0x00007f3cba79172c 0x0000000000000000
47. 14 libQtNetwork.so.4 0x00007f3cba788600 0x0000000000000000
48. 15 libQtNetwork.so.4 0x00007f3cba78b035 QSslSocket::qt_metacall(QMetaObject::Call, int, void**)
49. 16 libQtCore.so.4 0x00007f3cbabade5c QMetaObject::activate(QObject*, int, int, void**)
50. 17 libQtCore.so.4 0x00007f3cbabaf4f5 QMetaObject::activate(QObject*, QMetaObject const*, int, void**)
51. 18 libQtCore.so.4 0x00007f3cbabf5258 QIODevice::readyRead()
52. 19 libQtNetwork.so.4 0x00007f3cba76effd 0x0000000000000000
53. 20 libQtNetwork.so.4 0x00007f3cba77275b 0x0000000000000000
54. 21 libQtNetwork.so.4 0x00007f3cba759463 0x0000000000000000
55. 22 libQtNetwork.so.4 0x00007f3cba75aed5 0x0000000000000000
56. 23 libQtCore.so.4 0x00007f3cbab9159a QCoreApplicationPrivate::notify_helper(QObject*, QEvent*)
57. 24 libQtCore.so.4 0x00007f3cbab94b38 QCoreApplication::notify(QObject*, QEvent*)
58. 25 libQtCore.so.4 0x00007f3cbab9372b QCoreApplication::notifyInternal(QObject*, QEvent*)
59. 26 libQtCore.so.4 0x00007f3cbab981dd QCoreApplication::sendEvent(QObject*, QEvent*)
60. 27 libQtCore.so.4 0x00007f3cbabc9ad7 QEventDispatcherUNIX::activateSocketNotifiers()
61. 28 libQtCore.so.4 0x00007f3cbabcc2fb QEventDispatcherUNIXPrivate::doSelect(QFlags<QEventLoop::ProcessEventsFlag>, timeval*)
62. 29 libQtCore.so.4 0x00007f3cbabcc476 QEventDispatcherUNIX::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)
63. 30 libQtCore.so.4 0x00007f3cbab8ffcf QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)
64. 31 libQtCore.so.4 0x00007f3cbab901de QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>)
65. 32 libQtCore.so.4 0x00007f3cbab94135 QCoreApplication::exec()
66. 33 quasselcore 0x0000000000472976 main
67. 34 libc.so.6 0x00007f3cb96501a6 __libc_start_main
68. 35 quasselcore 0x0000000000470d49 std::ios_base::Init::~Init()

#3 - 05/09/2009 11:15 AM - tobyS

Another crash log, created with all qt packages, quassel and openssl compiled with "-debug" use flag (Gentoo):

2009-05-09 11:09:24 Debug: Quassel IRC: "0.4.1" "b5798a1041d83a7118b7e9b7cffd4d5307a72d0e"
2009-05-09 11:09:24 Debug: Quassel IRC: "0.4.1" "b5798a1041d83a7118b7e9b7cffd4d5307a72d0e"
2009-05-09 11:09:24 Debug: # 0 quasselcore 0x08141cd3 Quassel::logBacktrace(QString const&)
2009-05-09 11:09:24 Debug: # 0 quasselcore 0x08141cd3 Quassel::logBacktrace(QString const&)
2009-05-09 11:09:24 Debug: # 1 quasselcore 0x08123a44 Quassel::handleSignal(int)
2009-05-09 11:09:24 Debug: # 1 quasselcore 0x08123a44 Quassel::handleSignal(int)
2009-05-09 11:09:24 Debug: # 2 0xffffe420 __kernel_sigreturn
2009-05-09 11:09:24 Debug: # 2 0xffffe420 __kernel_sigreturn
2009-05-09 11:09:24 Debug: # 3 libz.so.1 0xb789b3fa 0x00000000
2009-05-09 11:09:24 Debug: # 3 libz.so.1 0xb789b3fa 0x00000000
2009-05-09 11:09:24 Debug: # 4 libz.so.1 0xb789bbfc 0x00000000
2009-05-09 11:09:24 Debug: # 4 libz.so.1 0xb789bc41 0x00000000
2009-05-09 11:09:24 Debug: # 5 libz.so.1 0xb78994d6 0x00000000
2009-05-09 11:09:24 Debug: # 5 libz.so.1 0xb78994d6 0x00000000
2009-05-09 11:09:24 Debug: # 6 libz.so.1 0xb7898627 deflate
2009-05-09 11:09:24 Debug: # 6 libz.so.1 0xb7898627 deflate
2009-05-09 11:09:24 Debug: # 7 libcrypto.so.0.9.8 0xb75125de 0x00000000
2009-05-09 11:09:24 Debug: # 7 libcrypto.so.0.9.8 0xb75125de 0x00000000
2009-05-09 11:09:24 Debug: # 8 libcrypto.so.0.9.8 0xb751157e COMP_compress_block
2009-05-09 11:09:24 Debug: # 8 libcrypto.so.0.9.8 0xb751157e COMP_compress_block
2009-05-09 11:09:24 Debug: # 9 libssl.so.0.9.8 0xb7576d2b ssl3_do_compress
2009-05-09 11:09:24 Debug: # 9 libssl.so.0.9.8 0xb7576d2b ssl3_do_compress
2009-05-09 11:09:24 Debug: # 10 libssl.so.0.9.8 0xb7576e5f 0x00000000
2009-05-09 11:09:24 Debug: # 10 libssl.so.0.9.8 0xb7576e5f 0x00000000
2009-05-09 11:09:24 Debug: # 11 libssl.so.0.9.8 0xb7577280 ssl3_write_bytes
2009-05-09 11:09:24 Debug: # 11 libssl.so.0.9.8 0xb7577280 ssl3_write_bytes
2009-05-09 11:09:24 Debug: # 12 libssl.so.0.9.8 0xb75744b2 ssl3_write
2009-05-09 11:09:24 Debug: # 12 libssl.so.0.9.8 0xb75744b2 ssl3_write
2009-05-09 11:09:24 Debug: # 13 libssl.so.0.9.8 0xb75861f9 SSL_write

2009-05-09 11:09:24 Debug: # 13 libssl.so.0.9.8 0xb75861f9 SSL_write
2009-05-09 11:09:24 Debug: # 14 libQtNetwork.so.4 0xb7cefd22 0x00000000
2009-05-09 11:09:24 Debug: # 14 libQtNetwork.so.4 0xb7cefd22 0x00000000
2009-05-09 11:09:24 Debug: # 15 libQtNetwork.so.4 0xb7ced27f 0x00000000
2009-05-09 11:09:24 Debug: # 15 libQtNetwork.so.4 0xb7ced27f 0x00000000
2009-05-09 11:09:24 Debug: # 16 libQtNetwork.so.4 0xb7ce65c8 QSslSocket::flush()
2009-05-09 11:09:24 Debug: # 16 libQtNetwork.so.4 0xb7ce5f98 0x00000000
2009-05-09 11:09:24 Debug: # 17 libQtNetwork.so.4 0xb7ce6608 0x00000000
2009-05-09 11:09:24 Debug: # 17 libQtNetwork.so.4 0xb7ce9006 QSslSocket::qt_metacall(QMetaObject::Call, int, void**)
2009-05-09 11:09:24 Debug: # 18 libQtNetwork.so.4 0xb7ce8fd6 QSslSocket::qt_metacall(QMetaObject::Call, int, void**)
2009-05-09 11:09:24 Debug: # 18 libQtCore.so.4 0xb7e5db8e QMetaObject::activate(QObject*, int, int, void**)
2009-05-09 11:09:24 Debug: # 19 libQtCore.so.4 0xb7e58ca9 QMetaCallEvent::placeMetaCall(QObject*)
2009-05-09 11:09:24 Debug: # 19 libQtCore.so.4 0xb7e5e104 QMetaObject::activate(QObject*, QMetaObject const*, int, void**)
2009-05-09 11:09:24 Debug: # 20 libQtCore.so.4 0xb7e59f57 QObject::event(QEvent*)
2009-05-09 11:09:24 Debug: # 20 libQtCore.so.4 0xb7e93623 QIODevice::readyRead()
2009-05-09 11:09:24 Debug: # 21 libQtCore.so.4 0xb7e4b4a3 QCoreApplicationPrivate::notify_helper(QObject*, QEvent*)
2009-05-09 11:09:24 Debug: # 21 libQtNetwork.so.4 0xb7cd150d 0x00000000
2009-05-09 11:09:24 Debug: # 22 libQtCore.so.4 0xb7e4b513 QCoreApplication::notify(QObject*, QEvent*)
2009-05-09 11:09:24 Debug: # 22 libQtNetwork.so.4 0xb7cd4de1 0x00000000
2009-05-09 11:09:24 Debug: # 23 libQtCore.so.4 0xb7e4b09a QCoreApplication::notifyInternal(QObject*, QEvent*)
2009-05-09 11:09:24 Debug: # 23 libQtNetwork.so.4 0xb7cc107b 0x00000000
2009-05-09 11:09:24 Debug: # 24 libQtCore.so.4 0xb7e4bfb6 QCoreApplicationPrivate::sendPostedEvents(QObject*, int, QThreadData*)
2009-05-09 11:09:24 Debug: # 24 libQtNetwork.so.4 0xb7cc2d5f 0x00000000
2009-05-09 11:09:24 Debug: # 25 libQtCore.so.4 0xb7e4c1ad QCoreApplication::sendPostedEvents(QObject*, int)
2009-05-09 11:09:24 Debug: # 25 libQtCore.so.4 0xb7e4b4a3 QCoreApplicationPrivate::notify_helper(QObject*, QEvent*)
2009-05-09 11:09:24 Debug: # 26 libQtCore.so.4 0xb7e715dd 0x00000000
2009-05-09 11:09:24 Debug: # 26 libQtCore.so.4 0xb7e4b513 QCoreApplication::notify(QObject*, QEvent*)
2009-05-09 11:09:24 Debug: # 27 libglib-2.0.so.0 0xb77eaf1b g_main_context_dispatch
2009-05-09 11:09:24 Debug: # 27 libQtCore.so.4 0xb7e4b09a QCoreApplication::notifyInternal(QObject*, QEvent*)
2009-05-09 11:09:24 Debug: # 28 libglib-2.0.so.0 0xb77ee41f 0x00000000
2009-05-09 11:09:24 Debug: # 29 libglib-2.0.so.0 0xb77ee997 g_main_context_iteration
2009-05-09 11:09:24 Debug: # 28 libQtCore.so.4 0xb7e71a4d 0x00000000
2009-05-09 11:09:24 Debug: # 30 libQtCore.so.4 0xb7e71b98 QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)
2009-05-09 11:09:24 Debug: # 29 libglib-2.0.so.0 0xb77eaf1b g_main_context_dispatch
2009-05-09 11:09:24 Debug: # 31 libQtCore.so.4 0xb7e4a36d QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)
2009-05-09 11:09:24 Debug: # 30 libglib-2.0.so.0 0xb77ee41f 0x00000000
2009-05-09 11:09:24 Debug: # 32 libQtCore.so.4 0xb7e4a51a QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>)
2009-05-09 11:09:24 Debug: # 31 libglib-2.0.so.0 0xb77ee997 g_main_context_iteration
2009-05-09 11:09:24 Debug: # 33 libQtCore.so.4 0xb7d6c301 QThread::exec()
2009-05-09 11:09:24 Debug: # 32 libQtCore.so.4 0xb7e71b98 QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)
2009-05-09 11:09:24 Debug: # 34 quasselcore 0x0808ca58 SessionThread::run()
2009-05-09 11:09:24 Debug: # 33 libQtCore.so.4 0xb7e4a36d QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)
2009-05-09 11:09:24 Debug: # 35 libQtCore.so.4 0xb7d6f00d 0x00000000
2009-05-09 11:09:24 Debug: # 34 libQtCore.so.4 0xb7e4a51a QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>)
2009-05-09 11:09:24 Debug: # 36 libpthread.so.0 0xb77a019b 0x00000000
2009-05-09 11:09:24 Debug: # 35 libQtCore.so.4 0xb7e4c26a QCoreApplication::exec()
2009-05-09 11:09:24 Debug: # 37 libc.so.6 0xb797286e clone
2009-05-09 11:09:24 Debug: # 36 quasselcore 0x080764ac main
2009-05-09 11:09:24 Debug: # 37 libc.so.6 0xb78c160c __libc_start_main
2009-05-09 11:09:24 Debug: # 38 quasselcore 0x08075c41 QObject::event(QEvent*)

#4 - 07/11/2009 03:08 PM - seezer

Ok, I have a little update on that.
Thought fix e042ae69dbe4f42e9e4441f4b5832cfe5ca89067 didn't help.
I even tried it with a blocking version of socket->flush() but that didn't fix it either.
But it helped getting the crash into the main thread which then got me the attention of thiago ;)

He told me where our problem is:
moveToThread is actually called via a signal of the socket to be moved

In detail:
QSslSocketBackendPrivate::transmit causes QIODevice::readyRead etc.
If transmit hasn't finished until the thread is moved, two threads use the same socket.

Background:
thiago explained to me that QSslSocket needs 4 transmit operations:
from the unencrypted buffer into the SSL engine, from the SSL engine into the socket
from the socket into the SSL engine, from the SSL engine into the decrypted buffer

The backtrace showing the behaviour:

```
Breakpoint 1, SessionThread::addRemoteClientToSession (this=0x1ff6430, socket=0x7fe494318a30) at /home/quassel
/quasselsource/src/core/sessionthread.cpp:90
```

```
90        socket->moveToThread(session()->thread());

(gdb) bt                                                                    0x7fe494318a30

#0  SessionThread::addRemoteClientToSession (this=0x1ff6430, socket=0x7fe494318a30) at /home/quassel/quasselso
urce/src/core/sessionthread.cpp:90
#1  0x00000000004c0592 in SessionThread::addClientToSession (this=0x1ff6430, peer=0x7fe494318a30) at /home/qua
ssel/quasselsource/src/core/sessionthread.cpp:75
#2  0x00000000004c0692 in SessionThread::addClient (this=0x1ff6430, peer=0x7fe494318a30) at /home/quassel/quas
selsource/src/core/sessionthread.cpp:66
#3  0x0000000000477e4e in Core::setupClientSession (this=0x1fc9da0, socket=0x7fe494318a30, uid={<SignedId> = {
id = 1}, <No data fields>})
    at /home/quassel/quasselsource/src/core/core.cpp:693

#4  0x00000000004817e8 in Core::processClientMessage (this=0x1fc9da0, socket=0x7fe494318a30, msg=@0x7fffebc106
50) at /home/quassel/quasselsource/src/core/core.cpp:620
#5  0x000000000048190e in Core::clientHasData (this=0x1fc9da0) at /home/quassel/quasselsource/src/core/core.cp
p:488
#6  0x00000000004e7ba4 in Core::qt_metacall (this=0x1fc9da0, _c=QMetaObject::InvokeMetaMethod, _id=12, _a=0x7f
ffebc10840)
    at /home/quassel/quasselsource/build/src/core/moc_core.cxx:117

#7  0x00007fe49ee28b44 in QMetaObject::activate (sender=0x7fe494318a30, from_signal_index=4, to_signal_index=4
, argv=0x0) at kernel/qobject.cpp:3104
#8  0x00007fe49ee2a285 in QMetaObject::activate (sender=0x7fe494318a30, m=0x85f700, local_signal_index=0, argv
=0x0) at kernel/qobject.cpp:3178
#9  0x00007fe49ee6ffb0 in QIODevice::readyRead (this=0x7fe494318a30) at .moc/debug-shared/moc_qiodevice.cpp:85

#10 0x00007fe49ea0a81c in QSslSocketBackendPrivate::transmit (this=0x7fe4945c9140) at ssl/qsslsocket_openssl.c
pp:668
#11 0x00007fe49ea01110 in QSslSocketPrivate::_q_readyReadSlot (this=0x7fe4945c9140) at ssl/qsslsocket.cpp:2010

#12 0x00007fe49ea03b83 in QSslSocket::qt_metacall (this=0x7fe494318a30, _c=QMetaObject::InvokeMetaMethod, _id=
15, _a=0x7fffebc11b50) at .moc/debug-shared/moc_qsslsocket.cpp:114
#13 0x00007fe49ee28b44 in QMetaObject::activate (sender=0x7fe494557fa0, from_signal_index=4, to_signal_index=4
, argv=0x0) at kernel/qobject.cpp:3104
#14 0x00007fe49ee2a285 in QMetaObject::activate (sender=0x7fe494557fa0, m=0x85f700, local_signal_index=0, argv
=0x0) at kernel/qobject.cpp:3178
#15 0x00007fe49ee6ffb0 in QIODevice::readyRead (this=0x7fe494557fa0) at .moc/debug-shared/moc_qiodevice.cpp:85

#16 0x00007fe49e9e7b89 in QAbstractSocketPrivate::canReadNotification (this=0x7fe4945c8b90) at socket/qabstrac
tsocket.cpp:604
#17 0x00007fe49e9eb2f5 in QAbstractSocketPrivate::readNotification (this=0x7fe4945c8b90) at ../../include/QtNe
twork/private/../../../src/network/socket/qabstractsocket_p.h:77
#18 0x00007fe49e9d1feb in QAbstractSocketEngine::readNotification (this=0x7fe4944532f0) at socket/qabstractsoc
ketengine.cpp:154
#19 0x00007fe49e9d3a5d in QReadNotifier::event (this=0x7fe4944da550, e=0x7fffebc11e40) at socket/qnativesocket
engine.cpp:1036
#20 0x00007fe49ee0c34a in QCoreApplicationPrivate::notify_helper (this=0x1fac1f0, receiver=0x7fe4944da550, eve
nt=0x7fffebc11e40) at kernel/qcoreapplication.cpp:746
#21 0x00007fe49ee0f848 in QCoreApplication::notify (this=0x7fffebc123d0, receiver=0x7fe4944da550, event=0x7fff
ebc11e40) at kernel/qcoreapplication.cpp:692
#22 0x00007fe49ee0e43b in QCoreApplication::notifyInternal (this=0x7fffebc123d0, receiver=0x7fe4944da550, even
t=0x7fffebc11e40) at kernel/qcoreapplication.cpp:610
#23 0x00007fe49ee12eed in QCoreApplication::sendEvent (receiver=0x7fe4944da550, event=0x7fffebc11e40) at ../..
/include/QtCore/../../src/corelib/kernel/qcoreapplication.h:213
#24 0x00007fe49ee44893 in QEventDispatcherUNIX::activateSocketNotifiers (this=0x1fabad0) at kernel/qeventdispa
tcher_unix.cpp:862
#25 0x00007fe49ee470b7 in QEventDispatcherUNIXPrivate::doSelect (this=0x1fad750, flags={i = -339664736}, timeo
ut=0x7fffebc12070) at kernel/qeventdispatcher_unix.cpp:250
#26 0x00007fe49ee47232 in QEventDispatcherUNIX::processEvents (this=0x1fabad0, flags={i = -339664624}) at kern
el/qeventdispatcher_unix.cpp:904
#27 0x00007fe49ee0ad5f in QEventLoop::processEvents (this=0x7fffebc121f0, flags={i = -339664512}) at kernel/qe
ventloop.cpp:149
#28 0x00007fe49ee0af83 in QEventLoop::exec (this=0x7fffebc121f0, flags={i = -339664384}) at kernel/qeventloop.
cpp:201
#29 0x00007fe49ee0ee45 in QCoreApplication::exec () at kernel/qcoreapplication.cpp:888

#30 0x0000000000472d36 in main (argc=9, argv=0x7fffebc12848) at /home/quassel/quasselsource/src/common/main.cp
p:144
```

And another backtrace of a crash showing two threads using the same socket:
Note the "strm" or "s" variable in deflate(|_slow):

```
Thread 8 (Thread 0x41ed5950 (LWP 1091)):
```

```
#0  deflate_slow (s=0x7f41982f3de0, flush=2) at deflate.c:1669
#1  0x00007f41a82cc28d in deflate (strm=0x7f41982df3c0, flush=2) at deflate.c:822
#2  0x00007f41a76e388e in ?? () from /usr/lib/libcrypto.so.0.9.8
#3  0x00007f41a76e34f2 in COMP_compress_block () from /usr/lib/libcrypto.so.0.9.8
#4  0x00007f41a739330e in ssl3_do_compress () from /usr/lib/libssl.so.0.9.8
#5  0x00007f41a739345c in ?? () from /usr/lib/libssl.so.0.9.8
#6  0x00007f41a7393950 in ssl3_write_bytes () from /usr/lib/libssl.so.0.9.8
#7  0x00007f41a9815e6d in QSslSocketBackendPrivate::transmit (this=0x7f41982b5410) at ssl/qsslsocket_openssl.c
pp:566
#8  0x00007f41a980d601 in QSslSocket::flush (this=<value optimized out>) at ssl/qsslsocket.cpp:693

#9  0x00007f41a98111b2 in QSslSocket::qt_metacall (this=0x7f41982994d0, _c=QMetaObject::InvokeMetaMethod, _id=
<value optimized out>, _a=0x7f419836f640)
    at .moc/release-shared/moc_qsslsocket.cpp:116

#10 0x00007f41a9bd4f58 in QObject::event (this=0x7f41982994d0, e=0x7f4198259230) at kernel/qobject.cpp:1102

#11 0x00007f41a9bc5aec in QCoreApplication::notifyInternal (this=0x7fff327c11d0, receiver=0x7f41982994d0, even
t=0x7f4198259230) at kernel/qcoreapplication.cpp:610
#12 0x00007f41a9bc6672 in QCoreApplicationPrivate::sendPostedEvents (receiver=0x0, event_type=0, data=0x172624
0)
    at ../../include/QtCore/../../src/corelib/kernel/qcoreapplication.h:213

#13 0x00007f41a9beffc0 in QEventDispatcherUNIX::processEvents (this=0x1720750, flags={i = 1106071600}) at kern
el/qeventdispatcher_unix.cpp:876
#14 0x00007f41a9bc45a2 in QEventLoop::processEvents (this=<value optimized out>, flags={i = 1106071648}) at ke
rnel/qeventloop.cpp:149
#15 0x00007f41a9bc4974 in QEventLoop::exec (this=0x41ed50a0, flags={i = 1106071728}) at kernel/qeventloop.cpp:
201
#16 0x00007f41a9adbd58 in QThread::exec (this=<value optimized out>) at thread/qthread.cpp:487

#17 0x00000000004c03b9 in SessionThread::run (this=0x1720a70) at /home/quassel/quasselsource/src/core/sessiont
hread.cpp:105
#18 0x00007f41a9adea15 in QThreadPrivate::start (arg=0x1720a70) at thread/qthread_unix.cpp:188

#19 0x00007f41a7ea7fc7 in start_thread () from /lib/libpthread.so.0

#20 0x00007f41a87b05ad in clone () from /lib/libc.so.6

#21 0x0000000000000000 in ?? ()
[...]
Thread 1 (Thread 0x7f41aa0bd6f0 (LWP 1085)):
#0  deflate_slow (s=0x7f41982f3de0, flush=2) at deflate.c:1669
#1  0x00007f41a82cc28d in deflate (strm=0x7f41982df3c0, flush=2) at deflate.c:822
#2  0x00007f41a76e388e in ?? () from /usr/lib/libcrypto.so.0.9.8
#3  0x00007f41a76e34f2 in COMP_compress_block () from /usr/lib/libcrypto.so.0.9.8
#4  0x00007f41a739330e in ssl3_do_compress () from /usr/lib/libssl.so.0.9.8
#5  0x00007f41a739345c in ?? () from /usr/lib/libssl.so.0.9.8
#6  0x00007f41a7393950 in ssl3_write_bytes () from /usr/lib/libssl.so.0.9.8
#7  0x00007f41a9815e6d in QSslSocketBackendPrivate::transmit (this=0x7f41982b5410) at ssl/qsslsocket_openssl.c
pp:566
#8  0x00007f41a98111e2 in QSslSocket::qt_metacall (this=0x7f41982994d0, _c=QMetaObject::InvokeMetaMethod, _id=
<value optimized out>, _a=0x7fff327c0cd0)
    at .moc/release-shared/moc_qsslsocket.cpp:114

#9  0x00007f41a9bd9972 in QMetaObject::activate (sender=0x7f41982abee0, from_signal_index=<value optimized out
>, to_signal_index=4, argv=0x1470) at kernel/qobject.cpp:3104
#10 0x00007f41a97f784f in QAbstractSocketPrivate::canReadNotification (this=0x7f41982abf20) at socket/qabstrac
tsocket.cpp:604
#11 0x00007f41a97e65f1 in QReadNotifier::event (this=<value optimized out>, e=0x7f41985cf4a0) at socket/qnativ
esocketengine.cpp:1036
#12 0x00007f41a9bc5aec in QCoreApplication::notifyInternal (this=0x7fff327c11d0, receiver=0x7f41982b0790, even
t=0x7fff327c0db0) at kernel/qcoreapplication.cpp:610
#13 0x00007f41a9bee3ca in QEventDispatcherUNIX::activateSocketNotifiers (this=<value optimized out>) at ../../
include/QtCore/../../src/corelib/kernel/qcoreapplication.h:213
#14 0x00007f41a9beeb46 in QEventDispatcherUNIXPrivate::doSelect (this=0x16cb760, flags={i = 846991168}, timeou
t=0x7fff327c0f30) at kernel/qeventdispatcher_unix.cpp:250
#15 0x00007f41a9bf002d in QEventDispatcherUNIX::processEvents (this=0x16cb740, flags={i = 846991232}) at kerne
l/qeventdispatcher_unix.cpp:904
#16 0x00007f41a9bc45a2 in QEventLoop::processEvents (this=<value optimized out>, flags={i = 846991280}) at ker
nel/qeventloop.cpp:149
#17 0x00007f41a9bc4974 in QEventLoop::exec (this=0x7fff327c0ff0, flags={i = 846991360}) at kernel/qeventloop.c
pp:201
#18 0x00007f41a9bc6916 in QCoreApplication::exec () at kernel/qcoreapplication.cpp:888
```

```
#19 0x0000000000472d36 in main (argc=9, argv=0x7fff327c1648) at /home/quassel/quasselsource/src/common/main.cpp:144
```

So we have to make sure that we're outside of the signal-called function calls and that should do the trick.
Who got the best idea how to do that? :)

#5 - 07/11/2009 03:10 PM - seezer

- Status changed from New to Confirmed

- Priority changed from Normal to High

- Version changed from 0.4.0 to 0.5-pre

- OS changed from Linux to Any

#6 - 07/12/2009 03:21 PM - EgS

- Status changed from Confirmed to Resolved

- % Done changed from 0 to 100

Applied in changeset e049ffc61b5e260a49d73102a74c3821af827e77.