Quassel IRC - Bug #1508

quasselcore crashes after a few minutes in libpcre2

01/03/2019 07:19 PM - mgorny

Status:	New	**Start date:**	01/03/2019
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Version:	0.13.0	**OS:**	Any

Description

A few minutes after starting, quasselcore suddenly crashes. Backtrace follows:

```
#0  0xf6c05679 in jit_machine_stack_exec () from /usr/lib/libpcre2-16.so.0
#1  0xf6c308ff in pcre2_jit_match_16 () from /usr/lib/libpcre2-16.so.0
#2  0xf6c328ab in pcre2_match_16 () from /usr/lib/libpcre2-16.so.0
#3  0xf77e8bb4 in safe_pcre2_match_16(pcre2_real_code_16 const*, unsigned short const*, int, int,
int, pcre2_real_match_data_16*, pcre2_real_match_context_16*) () from /usr/lib/libQt5Core.so.5
#4  0xf77ecc6a in QRegularExpressionPrivate::doMatch(QString const&, int, int, int, QRegularExpres
sion::MatchType, QFlags<QRegularExpression::MatchOption>, QRegularExpressionPrivate::CheckSubjectS
tringOption, QRegularExpressionMatchPrivate const*) const () from /usr/lib/libQt5Core.so.5
#5  0xf77ed1a1 in QRegularExpression::match(QString const&, int, QRegularExpression::MatchType, QF
lags<QRegularExpression::MatchOption>) const ()
   from /usr/lib/libQt5Core.so.5
#6  0xf7c848b8 in ExpressionMatch::match (this=0xf4b59964, string=..., matchEmpty=false)
    at /home/mgorny/git/quassel/src/common/expressionmatch.cpp:68
#7  0xf7cc4eb8 in NickHighlightMatcher::match (this=0xf5a047d8, string=..., netId=..., currentNick
=..., identityNicks=...)
    at /home/mgorny/git/quassel/src/common/nickhighlightmatcher.cpp:43
#8  0xf7c8a6e3 in HighlightRuleManager::match (this=0xf5a047c0, netId=..., msgContents=..., msgSen
der=..., msgType=Message::Plain, msgFlags=...,
    bufferName=..., currentNick=..., identityNicks=...) at /home/mgorny/git/quassel/src/common/hig
hlightrulemanager.cpp:195
#9  0xf7e21f6b in CoreHighlightRuleManager::match (this=0xf5a047c0, msg=..., currentNick=..., iden
tityNicks=...)
    at /home/mgorny/git/quassel/src/core/corehighlightrulemanager.cpp:49
#10 0xf7e48302 in CoreSession::recvMessageFromServer (this=0xf5a04730, networkId=..., type=Message
::Plain, bufferType=BufferInfo::ChannelBuffer,
    target=..., text_=..., sender=..., flags=...) at /home/mgorny/git/quassel/src/core/coresession
.cpp:324
#11 0xf7e48714 in CoreSession::processMessageEvent (this=0xf5a04730, event=0xf4761a80) at /home/mg
orny/git/quassel/src/core/coresession.cpp:349
#12 0xf7f18e85 in CoreSession::qt_static_metacall (_o=0xf5a04730, _c=QMetaObject::InvokeMetaMethod
, _id=43, _a=0xf6374df4)
    at /home/mgorny/git/quassel/build/src/core/quassel_core_autogen/EWIEGA46WW/moc_coresession.cpp
:319
#13 0xf7f19afd in CoreSession::qt_metacall (this=0xf5a04730, _c=QMetaObject::InvokeMetaMethod, _id
=43, _a=0xf6374df4)
    at /home/mgorny/git/quassel/build/src/core/quassel_core_autogen/EWIEGA46WW/moc_coresession.cpp
:609
#14 0xf7c7ff3c in EventManager::dispatchEvent (this=0xf5a4d5e0, event=0xf4761a80) at /home/mgorny/
git/quassel/src/common/eventmanager.cpp:289
#15 0xf7c7f95c in EventManager::processEvent (this=0xf5a4d5e0, event=0xf4761a80) at /home/mgorny/g
it/quassel/src/common/eventmanager.cpp:221
#16 0xf7c7f843 in EventManager::postEvent (this=0xf5a4d5e0, event=0xf4761a80) at /home/mgorny/git/
quassel/src/common/eventmanager.cpp:203
#17 0xf7e44095 in QtPrivate::FunctorCall<QtPrivate::IndexesList<0>, QtPrivate::List<Event*>, void,
 void (EventManager::*)(Event*)>::call (f=
    (void (EventManager::*)(EventManager * const, Event *)) 0xf7c7f762 <EventManager::postEvent(Ev
ent*)>, o=0xf5a4d5e0, arg=0xf6375044)
    at /usr/include/qt5/QtCore/qobjectdefs_impl.h:136
#18 0xf7e438e5 in QtPrivate::FunctionPointer<void (EventManager::*)(Event*)>::call<QtPrivate::List
```

```
<Event*>, void> (f=
    (void (EventManager::*)(EventManager * const, Event *)) 0xf7c7f762 <EventManager::postEvent(Ev
ent*)>, o=0xf5a4d5e0, arg=0xf6375044)
    at /usr/include/qt5/QtCore/qobjectdefs_impl.h:169
#19 0xf7e42da5 in QtPrivate::QSlotObject<void (EventManager::*)(Event*), QtPrivate::List<Event*>,
 void>::impl (which=1, this_=0xf5a5b9a0,
    r=0xf5a4d5e0, a=0xf6375044, ret=0x0) at /usr/include/qt5/QtCore/qobject_impl.h:120
#20 0xf795d3cd in QMetaObject::activate(QObject*, int, int, void**) () from /usr/lib/libQt5Core.so
.5
#21 0xf795d957 in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/li
b/libQt5Core.so.5
#22 0xf7f1c3bc in CtcpParser::newEvent (this=0xf5a4d910, _t1=0xf4761a80)
    at /home/mgorny/git/quassel/build/src/core/quassel_core_autogen/EWIEGA46WW/moc_ctcpparser.cpp:
159
#23 0xf7e90611 in CtcpParser::displayMsg (this=0xf5a4d910, event=0xf4752330, msgType=Message::Plai
n, msg=..., sender=..., target=...,
    msgFlags=...) at /home/mgorny/git/quassel/src/core/ctcpparser.cpp:66
#24 0xf7e9158c in CtcpParser::parseSimple (this=0xf5a4d910, e=0xf4752330, messagetype=Message::Pla
in, dequotedMessage=...,
    ctcptype=CtcpEvent::Query, flags=...) at /home/mgorny/git/quassel/src/core/ctcpparser.cpp:199
#25 0xf7e912b0 in CtcpParser::parse (this=0xf5a4d910, e=0xf4752330, messagetype=Message::Plain)
    at /home/mgorny/git/quassel/src/core/ctcpparser.cpp:190
#26 0xf7e90e8f in CtcpParser::processIrcEventRawPrivmsg (this=0xf5a4d910, event=0xf4752330)
    at /home/mgorny/git/quassel/src/core/ctcpparser.cpp:149
#27 0xf7f1c177 in CtcpParser::qt_static_metacall (_o=0xf5a4d910, _c=QMetaObject::InvokeMetaMethod,
 _id=3, _a=0xf6375344)
    at /home/mgorny/git/quassel/build/src/core/quassel_core_autogen/EWIEGA46WW/moc_ctcpparser.cpp:
103
#28 0xf7f1c32b in CtcpParser::qt_metacall (this=0xf5a4d910, _c=QMetaObject::InvokeMetaMethod, _id=
3, _a=0xf6375344)
    at /home/mgorny/git/quassel/build/src/core/quassel_core_autogen/EWIEGA46WW/moc_ctcpparser.cpp:
145
#29 0xf7c7ff3c in EventManager::dispatchEvent (this=0xf5a4d5e0, event=0xf4752330) at /home/mgorny/
git/quassel/src/common/eventmanager.cpp:289
#30 0xf7c7f95c in EventManager::processEvent (this=0xf5a4d5e0, event=0xf4752330) at /home/mgorny/g
it/quassel/src/common/eventmanager.cpp:221
#31 0xf7c7f843 in EventManager::postEvent (this=0xf5a4d5e0, event=0xf4752330) at /home/mgorny/git/
quassel/src/common/eventmanager.cpp:203
#32 0xf7e44095 in QtPrivate::FunctorCall<QtPrivate::IndexesList<0>, QtPrivate::List<Event*>, void,
 void (EventManager::*)(Event*)>::call (f=
    (void (EventManager::*)(EventManager * const, Event *)) 0xf7c7f762 <EventManager::postEvent(Ev
ent*)>, o=0xf5a4d5e0, arg=0xf6375594)
    at /usr/include/qt5/QtCore/qobjectdefs_impl.h:136
#33 0xf7e438e5 in QtPrivate::FunctionPointer<void (EventManager::*)(Event*)>::call<QtPrivate::List
<Event*>, void> (f=
    (void (EventManager::*)(EventManager * const, Event *)) 0xf7c7f762 <EventManager::postEvent(Ev
ent*)>, o=0xf5a4d5e0, arg=0xf6375594)
    at /usr/include/qt5/QtCore/qobjectdefs_impl.h:169
#34 0xf7e42da5 in QtPrivate::QSlotObject<void (EventManager::*)(Event*), QtPrivate::List<Event*>,
 void>::impl (which=1, this_=0xf5a5bbb0,
    r=0xf5a4d5e0, a=0xf6375594, ret=0x0) at /usr/include/qt5/QtCore/qobject_impl.h:120
#35 0xf795d3cd in QMetaObject::activate(QObject*, int, int, void**) () from /usr/lib/libQt5Core.so
.5
#36 0xf795d957 in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/li
b/libQt5Core.so.5
#37 0xf7f1d42a in IrcParser::newEvent (this=0xf5a5bae0, _t1=0xf4752330)
    at /home/mgorny/git/quassel/build/src/core/quassel_core_autogen/EWIEGA46WW/moc_ircparser.cpp:1
39
#38 0xf7ea90ee in IrcParser::processNetworkIncoming (this=0xf5a5bae0, e=0xf474ffa0) at /home/mgorn
y/git/quassel/src/core/ircparser.cpp:411
#39 0xf7f1d202 in IrcParser::qt_static_metacall (_o=0xf5a5bae0, _c=QMetaObject::InvokeMetaMethod,
 _id=1, _a=0xf6375834)
    at /home/mgorny/git/quassel/build/src/core/quassel_core_autogen/EWIEGA46WW/moc_ircparser.cpp:8
4
#40 0xf7f1d399 in IrcParser::qt_metacall (this=0xf5a5bae0, _c=QMetaObject::InvokeMetaMethod, _id=1
, _a=0xf6375834)
    at /home/mgorny/git/quassel/build/src/core/quassel_core_autogen/EWIEGA46WW/moc_ircparser.cpp:1
```

```
25
#41 0xf7c7ff3c in EventManager::dispatchEvent (this=0xf5a4d5e0, event=0xf474ffa0) at /home/mgorny/
git/quassel/src/common/eventmanager.cpp:289
#42 0xf7c7f95c in EventManager::processEvent (this=0xf5a4d5e0, event=0xf474ffa0) at /home/mgorny/g
it/quassel/src/common/eventmanager.cpp:221
#43 0xf7c7f843 in EventManager::postEvent (this=0xf5a4d5e0, event=0xf474ffa0) at /home/mgorny/git/
quassel/src/common/eventmanager.cpp:203
#44 0xf7e44095 in QtPrivate::FunctorCall<QtPrivate::IndexesList<0>, QtPrivate::List<Event*>, void,
 void (EventManager::*)(Event*)>::call (f=
    (void (EventManager::*)(EventManager * const, Event *)) 0xf7c7f762 <EventManager::postEvent(Ev
ent*)>, o=0xf5a4d5e0, arg=0xf6375a84)
    at /usr/include/qt5/QtCore/qobjectdefs_impl.h:136
#45 0xf7e438e5 in QtPrivate::FunctionPointer<void (EventManager::*)(Event*)>::call<QtPrivate::List
<Event*>, void> (f=
    (void (EventManager::*)(EventManager * const, Event *)) 0xf7c7f762 <EventManager::postEvent(Ev
ent*)>, o=0xf5a4d5e0, arg=0xf6375a84)
    at /usr/include/qt5/QtCore/qobjectdefs_impl.h:169
#46 0xf7e42da5 in QtPrivate::QSlotObject<void (EventManager::*)(Event*), QtPrivate::List<Event*>,
void>::impl (which=1, this_=0xf5a709a0,
    r=0xf5a4d5e0, a=0xf6375a84, ret=0x0) at /usr/include/qt5/QtCore/qobject_impl.h:120
#47 0xf795d3cd in QMetaObject::activate(QObject*, int, int, void**) () from /usr/lib/libQt5Core.so
.5
#48 0xf795d957 in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/li
b/libQt5Core.so.5
#49 0xf7f1815a in CoreNetwork::newEvent (this=0xf5a04400, _t1=0xf474ffa0)
    at /home/mgorny/git/quassel/build/src/core/quassel_core_autogen/EWIEGA46WW/moc_corenetwork.cpp
:779
#50 0xf7e32b58 in CoreNetwork::onSocketHasData (this=0xf5a04400) at /home/mgorny/git/quassel/src/c
ore/corenetwork.cpp:521
#51 0xf7e43cb2 in QtPrivate::FunctorCall<QtPrivate::IndexesList<>, QtPrivate::List<>, void, void (
CoreNetwork::*)()>::call(void (CoreNetwork::*)(), CoreNetwork*, void**) (f=(void (CoreNetwork::*)(
CoreNetwork * const)) 0xf7e329f4 <CoreNetwork::onSocketHasData()>, o=0xf5a04400, arg=0xf6375c18)
    at /usr/include/qt5/QtCore/qobjectdefs_impl.h:136
#52 0xf7e43731 in QtPrivate::FunctionPointer<void (CoreNetwork::*)()>::call<QtPrivate::List<>, voi
d>(void (CoreNetwork::*)(), CoreNetwork*, void**) (f=(void (CoreNetwork::*)(CoreNetwork * const))
0xf7e329f4 <CoreNetwork::onSocketHasData()>, o=0xf5a04400, arg=0xf6375c18)
    at /usr/include/qt5/QtCore/qobjectdefs_impl.h:169
#53 0xf7e4267d in QtPrivate::QSlotObject<void (CoreNetwork::*)(), QtPrivate::List<>, void>::impl(i
nt, QtPrivate::QSlotObjectBase*, QObject*, void**, bool*) (which=1, this_=0xf5a6c790, r=0xf5a04400
, a=0xf6375c18, ret=0x0) at /usr/include/qt5/QtCore/qobject_impl.h:120
#54 0xf795d3cd in QMetaObject::activate(QObject*, int, int, void**) () from /usr/lib/libQt5Core.so
.5
#55 0xf795d957 in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/li
b/libQt5Core.so.5
#56 0xf783abfa in QIODevice::readyRead() () from /usr/lib/libQt5Core.so.5
#57 0xf6e0cfad in QSslSocketBackendPrivate::transmit() () from /usr/lib/libQt5Network.so.5
#58 0xf6deaf25 in QSslSocketPrivate::_q_flushReadBuffer() [clone .part.8] () from /usr/lib/libQt5N
etwork.so.5
#59 0xf6df4f4b in QSslSocket::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) () from
 /usr/lib/libQt5Network.so.5
#60 0xf795d0a6 in QMetaObject::activate(QObject*, int, int, void**) () from /usr/lib/libQt5Core.so
.5
#61 0xf795d957 in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/li
b/libQt5Core.so.5
#62 0xf783abfa in QIODevice::readyRead() () from /usr/lib/libQt5Core.so.5
#63 0xf6db4177 in QAbstractSocketPrivate::emitReadyRead(int) () from /usr/lib/libQt5Network.so.5
#64 0xf6db4278 in QAbstractSocketPrivate::canReadNotification() () from /usr/lib/libQt5Network.so.
5
#65 0xf6dca7fb in QReadNotifier::event(QEvent*) () from /usr/lib/libQt5Network.so.5
#66 0xf79292d6 in doNotify(QObject*, QEvent*) () from /usr/lib/libQt5Core.so.5
#67 0xf7929423 in QCoreApplication::notifyInternal2(QObject*, QEvent*) () from /usr/lib/libQt5Core
.so.5
#68 0xf7990f09 in socketNotifierSourceDispatch(_GSource*, int (*)(void*), void*) () from /usr/lib/
libQt5Core.so.5
#69 0xf6af735f in g_main_context_dispatch () from /usr/lib/libglib-2.0.so.0
#70 0xf6af7638 in g_main_context_iterate.isra () from /usr/lib/libglib-2.0.so.0
#71 0xf6af7741 in g_main_context_iteration () from /usr/lib/libglib-2.0.so.0
```

```
#72 0xf799002d in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () fr
om /usr/lib/libQt5Core.so.5
#73 0xf7927530 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQt5C
ore.so.5
#74 0xf773799f in QThread::exec() () from /usr/lib/libQt5Core.so.5
#75 0xf7737a84 in QThread::run() () from /usr/lib/libQt5Core.so.5
#76 0xf773dc0a in QThreadPrivate::start(void*) () from /usr/lib/libQt5Core.so.5
#77 0xf6c6cb57 in start_thread () from /lib/libpthread.so.0
#78 0xf738a5d6 in clone () from /lib/libc.so.6
```

I would love to help debugging this but Qt types seem awfully obscure to debug :-(.

History

#1 - 01/22/2019 08:53 PM - Darkstar

This seems to be related to highlight matching rules. You can narrow it down by removing your highlight rules one by one until it no longer crashes. The rule you removed is the problematic one

#2 - 01/26/2019 05:33 AM - digitalcircuit

- Priority changed from Normal to High

Darkstar is correct - this is related to highlight matching. However, this actually stems from nickname highlight matching, not a specific highlight rule.

Would you look at the nicknames in use on your Quassel core, and either share them if not sensitive, or if sensitive, try them until you find whichever one causes the crash? It might have unusual characters in it, e.g. "\" or "[]"…

This crash appears to be in Qt's code (or one below), so it might be a Qt bug to file. It'd still be useful to find out what causes it, in case we can fix or workaround this.

#3 - 01/26/2019 09:15 AM - mgorny

I don't have any custom highlight matching rules. I've just disabled local highlights for all nicknames to check if that changes anything.

Also, I've noticed a weird thing trying to debug this. If I rebuild libpcre2 with '-O0 -ggdb', I can't reproduce the crash anymore. '-O2' causes it to crash again.

#4 - 01/26/2019 10:28 AM - mgorny

And it just crashed randomly again (and it highlighted me on my nick too). I've just disabled remote highlights for further investigation.

#5 - 01/26/2019 10:40 PM - mgorny

Upon investigating further, I've noticed that tests inside libpcre crash as well on this particular system, while they pass on my other systems. At the same time, they pass when JIT is disabled in libpcre2. Therefore, it is entirely possible that it's a problem with libpcre2 and not quassel.

#6 - 01/29/2019 02:08 AM - digitalcircuit

Thank you for digging deeper into this issue! I've brought this up with Sput in Freenode/#quassel as well.

If it turns out this is a system library issue, it's not great, but at least we know where to focus troubleshooting effort. I've noted issue #1507 as well.

Additional context on why it's an issue now:
Quassel 0.13 switched over to QRegularExpression in place of QRegExp when building against Qt 5, providing significant performance improvements. QRegularExpression makes use of the libpcre2 JIT engine, while QRegExp does not.