Audacious - Bug #828

Info popup causes segmentation fault in Qt 5 UI

September 15, 2018 17:08 - A. Wilcox

Status:	Closed	**Start date:**	September 15, 2018
Priority:	Major	**Due date:**	
Assignee:		**% Done:**	100%
Category:	libaudqt	**Estimated time:**	0.00 hour
Target version:	3.10.1		
Affects version:	3.10		

Description

I'm the maintainer for Audacious at Adélie Linux, and I was attempting to bump Audacious from 3.9 to 3.10.

During the bump, I decided to test it out by playing a CD. Hovering over the track I wanted to listen to showed a tool tip (the InfoPopup widget); moving the mouse in any way after the widget is displayed immediately causes a segmentation fault. Further debugging led me to believe the 'delete' at the top of show_popup should probably be a deleteLater():

```
awilcox on gwyn [pts/12 Sat 15 11:39] audacious: LD_LIBRARY_PATH=lib:lib/audacious gdb bin/audacio
us
GNU gdb (GDB) 8.2
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "powerpc64-foxkit-linux-musl".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from bin/audacious...done.
(gdb) run
Starting program: /home/awilcox/audacious/bin/audacious
[New LWP 39627]
[New LWP 39628]
[New LWP 39629]
[New LWP 39630]
[LWP 39629 exited]
[New LWP 39634]
Qt: gdb: -nograb added to command-line options.
         Use the -dograb option to enforce grabbing.
[New LWP 39635]
[New LWP 39636]
[New LWP 39637]
[LWP 39637 exited]

Thread 1 "audacious" received signal SIGSEGV, Segmentation fault.
QList<QGraphicsView*>::QList (this=0x3fffffffdd48, l=...) at ../../include/QtCore/../../src/coreli
b/tools/qlist.h:807
807     ../../include/QtCore/../../src/corelib/tools/qlist.h: No such file or directory.
(gdb) bt
#0  0x00003fffee6ff2d4 in QList<QGraphicsView*>::QList(QList<QGraphicsView*> const&) (this=0x3ffff
fffdd48, l=...) at ../../include/QtCore/../../src/corelib/tools/qlist.h:807
#1  0x00003fffee71b33c in QGraphicsScene::views() const (this=<optimized out>) at graphicsview/qgr
aphicsscene.cpp:3280
#2  0x00003fffee2cb534 in mapToGlobalTransform(QWidget const*) (w=0x10047ca60) at kernel/qwidget.c
pp:12533
```

```
#3  0x00003fffee2cb75c in QWidget::mapFromGlobal(QPoint const&) const (this=<optimized out>, pos=.
..) at kernel/qwidget.cpp:12582
#4  0x00003fffee283c8c in QApplicationPrivate::dispatchEnterLeave(QWidget*, QWidget*, QPointF cons
t&) (enter=0x10047ca60, leave=<optimized out>, globalPosF=...) at kernel/qapplication.cpp:2351
#5  0x00003fffee284880 in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QW
idget*, QWidget**, QPointer<QWidget>&, bool) (receiver=0x10047ca60, event=
    0x3fffffffe340, alienWidget=0x0, nativeWidget=0x10047ca60, buttonDown=0x3fffee8d5460 <qt_butto
n_down>, lastMouseReceiver=..., spontaneous=<optimized out>) at kernel/qapplication.cpp:2684
#6  0x00003fffee30ccb8 in QWidgetWindow::handleMouseEvent(QMouseEvent*) (this=0x10033e2e0, event=0
x3fffffffe878) at kernel/qwidgetwindow.cpp:629
#7  0x00003fffee30ff68 in QWidgetWindow::event(QEvent*) (this=0x10033e2e0, event=0x3fffffffe878) a
t kernel/qwidgetwindow.cpp:250
#8  0x00003fffee27a2f4 in QApplicationPrivate::notify_helper(QObject*, QEvent*) (this=<optimized o
ut>, receiver=0x10033e2e0, e=0x3fffffffe878) at kernel/qapplication.cpp:3722
#9  0x00003fffee285ba0 in QApplication::notify(QObject*, QEvent*) (this=0x10008ff00, receiver=0x10
033e2e0, e=0x3fffffffe878) at kernel/qapplication.cpp:3094
#10 0x00003ffff7580010 in QCoreApplication::notifyInternal2(QObject*, QEvent*) (receiver=0x10033e2
e0, event=0x3fffffffe878) at kernel/qcoreapplication.cpp:1024
#11 0x00003fffedbfcb58 in QCoreApplication::sendSpontaneousEvent(QObject*, QEvent*) (event=0x3ffff
fffe868, receiver=0x10033e2e0) at ../../include/QtCore/../../src/corelib/kernel/qcoreapplication.h
:236
#12 0x00003fffedbfcb58 in QGuiApplicationPrivate::processMouseEvent(QWindowSystemInterfacePrivate:
:MouseEvent*) (e=0x1004b10c0) at kernel/qguiapplication.cpp:1952
#13 0x00003fffedbfef60 in QGuiApplicationPrivate::processWindowSystemEvent(QWindowSystemInterfaceP
rivate::WindowSystemEvent*) (e=<optimized out>) at kernel/qguiapplication.cpp:1733
#14 0x00003fffedbbfd64 in QWindowSystemInterface::sendWindowSystemEvents(QFlags<QEventLoop::Proces
sEventsFlag>) (flags=...) at kernel/qwindowsysteminterface.cpp:946
#15 0x00003fffed1b2314 in userEventSourceDispatch(GSource*, GSourceFunc, gpointer) (source=<optimi
zed out>) at qeventdispatcher_glib.cpp:77
#16 0x00003ffff7b24220 in g_main_context_dispatch () at /usr/lib/libglib-2.0.so.0
#17 0x00003ffff7b24568 in  () at /usr/lib/libglib-2.0.so.0
#18 0x00003ffff7b2469c in g_main_context_iteration () at /usr/lib/libglib-2.0.so.0
#19 0x00003ffff76035b4 in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag
>) (this=0x3ffff7b3a4a0 <g_poll>, flags=...) at kernel/qeventdispatcher_glib.cpp:423
#20 0x00003fffed1b25f0 in QPAEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFl
ag>) (this=<optimized out>, flags=...) at qeventdispatcher_glib.cpp:122
#21 0x00003ffff757ca14 in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) (this=<
optimized out>, flags=...) at kernel/qeventloop.cpp:134
#22 0x00003ffff757d1f0 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) (this=0x3fffffff
ede8, flags=...) at kernel/qeventloop.cpp:212
#23 0x00003ffff758afa8 in QCoreApplication::exec() () at kernel/qcoreapplication.cpp:1297
#24 0x00003fffedbf1118 in QGuiApplication::exec() () at kernel/qguiapplication.cpp:1679
#25 0x00003fffee27a100 in QApplication::exec() () at kernel/qapplication.cpp:2910
#26 0x00003fffeda5d718 in audqt::run() () at audqt.cc:90
#27 0x00003fffed3d0dc8 in QtUI::run() (this=<optimized out>) at qtui.cc:63
#28 0x00003ffff7ebca6c in interface_run() () at interface.cc:163
#29 0x00003ffff7edb61c in aud_run() () at runtime.cc:323
#30 0x000000010000b3e4 in main(int, char**) (argc=<optimized out>, argv=<optimized out>) at main.c
c:395
```

Changing line 179 of infopopup-qt.cc from "delete s_infopopup;" to "if (s_infopopup) s_infopopup->deleteLater();" helped in some way, but still ended in a crash:

```
awilcox on gwyn [pts/12 Sat 15 11:50] audacious: LD_LIBRARY_PATH=lib:lib/audacious gdb bin/audacio
us
GNU gdb (GDB) 8.2
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "powerpc64-foxkit-linux-musl".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
```

```
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from bin/audacious...done.
(gdb) run
Starting program: /home/awilcox/audacious/bin/audacious
[New LWP 40361]
[New LWP 40362]
[New LWP 40363]
[New LWP 40364]
[LWP 40363 exited]
[New LWP 40373]
Qt: gdb: -nograb added to command-line options.
         Use the -dograb option to enforce grabbing.
[New LWP 40390]
[New LWP 40391]
QCoreApplication::postEvent: Unexpected null receiver
[New LWP 40393]
[LWP 40393 exited]
QCoreApplication::postEvent: Unexpected null receiver
[New LWP 40394]
[LWP 40394 exited]

Thread 1 "audacious" received signal SIGSEGV, Segmentation fault.
QCoreApplication::notifyInternal2 (receiver=0x1004b20a0, event=0x3fffffffdfa0) at kernel/qcoreappl
ication.cpp:1021
1021    kernel/qcoreapplication.cpp: No such file or directory.
(gdb) bt
#0  0x00003ffff757ffac in QCoreApplication::notifyInternal2(QObject*, QEvent*) (receiver=0x1004b20
a0, event=0x3fffffffdfa0) at kernel/qcoreapplication.cpp:1021
#1  0x00003fffee283df8 in QCoreApplication::sendEvent(QObject*, QEvent*) (event=0x3fffffffdf90, re
ceiver=0x1004b20a0) at ../../include/QtCore/../../src/corelib/kernel/qcoreapplication.h:233
#2  0x00003fffee283df8 in QApplicationPrivate::dispatchEnterLeave(QWidget*, QWidget*, QPointF cons
t&) (enter=0x1004b20a0, leave=<optimized out>, globalPosF=...) at kernel/qapplication.cpp:2357
#3  0x00003fffee284880 in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QW
idget*, QWidget**, QPointer<QWidget>&, bool) (receiver=0x1004b20a0, event=
    0x3fffffffe340, alienWidget=0x0, nativeWidget=0x1004b20a0, buttonDown=0x3fffee8d5460 <qt_butto
n_down>, lastMouseReceiver=..., spontaneous=<optimized out>) at kernel/qapplication.cpp:2684
#4  0x00003fffee30ccb8 in QWidgetWindow::handleMouseEvent(QMouseEvent*) (this=0x100480c40, event=0
x3fffffffe878) at kernel/qwidgetwindow.cpp:629
#5  0x00003fffee30ff68 in QWidgetWindow::event(QEvent*) (this=0x100480c40, event=0x3fffffffe878) a
t kernel/qwidgetwindow.cpp:250
#6  0x00003fffee27a2f4 in QApplicationPrivate::notify_helper(QObject*, QEvent*) (this=<optimized o
ut>, receiver=0x100480c40, e=0x3fffffffe878) at kernel/qapplication.cpp:3722
#7  0x00003fffee285ba0 in QApplication::notify(QObject*, QEvent*) (this=0x10008ff00, receiver=0x10
0480c40, e=0x3fffffffe878) at kernel/qapplication.cpp:3094
#8  0x00003ffff7580010 in QCoreApplication::notifyInternal2(QObject*, QEvent*) (receiver=0x100480c
40, event=0x3fffffffe878) at kernel/qcoreapplication.cpp:1024
#9  0x00003fffedbfcb58 in QCoreApplication::sendSpontaneousEvent(QObject*, QEvent*) (event=0x3ffff
fffe868, receiver=0x100480c40) at ../../include/QtCore/../../src/corelib/kernel/qcoreapplication.h
:236
#10 0x00003fffedbfcb58 in QGuiApplicationPrivate::processMouseEvent(QWindowSystemInterfacePrivate:
:MouseEvent*) (e=0x100480ee0) at kernel/qguiapplication.cpp:1952
#11 0x00003fffedbfef60 in QGuiApplicationPrivate::processWindowSystemEvent(QWindowSystemInterfaceP
rivate::WindowSystemEvent*) (e=<optimized out>) at kernel/qguiapplication.cpp:1733
#12 0x00003fffedbbfd64 in QWindowSystemInterface::sendWindowSystemEvents(QFlags<QEventLoop::Proces
sEventsFlag>) (flags=...) at kernel/qwindowsysteminterface.cpp:946
#13 0x00003fffed1b2314 in userEventSourceDispatch(GSource*, GSourceFunc, gpointer) (source=<optimi
zed out>) at qeventdispatcher_glib.cpp:77
#14 0x00003ffff7b24220 in g_main_context_dispatch () at /usr/lib/libglib-2.0.so.0
#15 0x00003ffff7b24568 in  () at /usr/lib/libglib-2.0.so.0
#16 0x00003ffff7b2469c in g_main_context_iteration () at /usr/lib/libglib-2.0.so.0
#17 0x00003ffff76035b4 in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag
>) (this=0x3ffff7b3a4a0 <g_poll>, flags=...) at kernel/qeventdispatcher_glib.cpp:423
```

```
#18 0x00003fffed1b25f0 in QPAEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFl
ag>) (this=<optimized out>, flags=...) at qeventdispatcher_glib.cpp:122
#19 0x00003ffff757ca14 in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) (this=<
optimized out>, flags=...) at kernel/qeventloop.cpp:134
#20 0x00003ffff757d1f0 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) (this=0x3fffffff
ede8, flags=...) at kernel/qeventloop.cpp:212
#21 0x00003ffff758afa8 in QCoreApplication::exec() () at kernel/qcoreapplication.cpp:1297
#22 0x00003fffedbf1118 in QGuiApplication::exec() () at kernel/qguiapplication.cpp:1679
#23 0x00003fffee27a100 in QApplication::exec() () at kernel/qapplication.cpp:2910
#24 0x00003fffeda5d718 in audqt::run() () at audqt.cc:90
#25 0x00003fffed3d0dc8 in QtUI::run() (this=<optimized out>) at qtui.cc:63
#26 0x00003ffff7ebca6c in interface_run() () at interface.cc:163
#27 0x00003ffff7edb61c in aud_run() () at runtime.cc:323
#28 0x0000000010000b3e4 in main(int, char**) (argc=<optimized out>, argv=<optimized out>) at main.c
c:395
```

Looking at the Qt 5 code, it seems like this line might crash if an event was fired on a thread that didn't own the event's target. It doesn't **look** like such a thing happens in libaudqt, but I don't have the time right now to look at all of the qtui plugin to be sure it doesn't happen there.

I am more than happy to try out different patches or aide in further debugging in any way I can.

History

#1 - September 15, 2018 17:14 - A. Wilcox

I should add some details, I apologise for not including them:

- Qt 5.9.6 LTS
- Audacious 3.10 release, though the above stack traces were done with git master with --prefix=$HOME/audacious
- musl libc 1.1.20
- Linux kernel 4.14.56

#2 - September 18, 2018 15:16 - John Lindgren

I can't reproduce this, and I don't see anything wrong with the code. Can you reproduce this on a mainstream or glibc-based distribution such as Ubuntu?

#3 - September 18, 2018 17:29 - A. Wilcox

- File valgrind.txt added

Here's a valgrind trace from Debian, showing the same exact crash. I no longer believe it is a threading issue; it is **definitely** a use-after-free/delete issue.

#4 - September 18, 2018 23:41 - John Lindgren

I'm still confused as to why I'm not able to reproduce this, but it seems Dolphin had a similar crash recently and their fix was to use deleteLater() as you suggested:

https://bugs.kde.org/show_bug.cgi?id=217449#c3

There is a second "delete s_infopopup;" in infopopup_hide(), at infopopup-qt.cc line 209. If you change that one to deleteLater() as well, does it help? And if not, can you capture a new Valgrind log with both "delete"s changed to "deleteLater"s?

Thanks!

#5 - September 20, 2018 17:38 - A. Wilcox

I can verify that changing that second delete to deleteLater solves the issue. I've opened a PR at https://github.com/audacious-media-player/audacious/pull/32 to fix this. Thank you.

#6 - September 20, 2018 17:53 - John Lindgren

- % Done changed from 0 to 100

- Target version set to 3.10.1

- Status changed from New to Closed

- Category set to libaudqt

Thank you for testing and for the pull request! Fixed:
https://github.com/audacious-media-player/audacious/commit/1d34f6799b8f5910fc6863ae96afd5ab035e830f

Files

valgrind.txt	339 KB	September 18, 2018	A. Wilcox