QGIS Application - Bug report #14909
regression: QGIS crashes when closing docked attribute table

2016-05-26 07:37 PM - Mathieu Pellerin - nIRV

Status:	Closed		
Priority:	Severe/Regression		
Assignee:	Nathan Woodrow		
Category:	Attribute table		
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	22862

Description

Steps to reproduce:

1. Make sure that the attribute table opens as a floatable dock panel (it might require a QGIS restart)
2. Create a new project
3. Add a vector layer
4. Right-click on the layer, open the attribute table
5. The attribute table should be docked to the bottom part of the window
6. Click on the panel's [x] close button
7. **boom** crash.

The gdb's where output:

```
#0  0x00007ffff502c1e8 in QRegion::operator=(QRegion const&) ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#1  0x00007ffff50ab9b9 in ?? () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#2  0x00007ffff4ed1b59 in ?? () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#3  0x00007ffff4ed1cf4 in QWidgetPrivate::deleteExtra() ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#4  0x00007ffff4ed1f3d in QWidgetPrivate::~QWidgetPrivate() ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#5  0x00007ffff53565b7 in ?? () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#6  0x00007ffff5b5c98a in QObject::~QObject() ()
   from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#7  0x00007ffff4ede341 in QWidget::~QWidget() ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#8  0x00007ffff7620ce4 in QgsAttributeTableDialog::~QgsAttributeTableDialog()
    () from /home/webmaster/dev/cpp/QGIS/bm/output/lib/libqgis_app.so.2.15.0
#9  0x00007ffff7620d22 in QgsAttributeTableDialog::~QgsAttributeTableDialog()
    () from /home/webmaster/dev/cpp/QGIS/bm/output/lib/libqgis_app.so.2.15.0
#10 0x00007ffff5b5a2b1 in QObjectPrivate::deleteChildren() ()
   from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#11 0x00007ffff4ede2a2 in QWidget::~QWidget() ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#12 0x00007ffff79c0381 in QgsAttributeTableDock::~QgsAttributeTableDock() ()
   from /home/webmaster/dev/cpp/QGIS/bm/output/lib/libqgis_app.so.2.15.0
```

Related issues:

Duplicated by QGIS Application - Bug report # 15018: closing a docked attribu...	**Rejected**	**2016-06-13**

Associated revisions

Revision a05b2ad9 - 2016-06-14 09:40 AM - Matthias Kuhn

Fix crash when closing docked attribute table

Fix #14909
Fix #15018

git bisect is your friend

History

#1 - 2016-05-26 09:50 PM - Mathieu Pellerin - nIRV

Note: you might have to open and close the attribute table panel twice to trigger the crash. On my machine, it crashes either on first or second closure.

#2 - 2016-05-29 07:26 PM - Mathieu Pellerin - nIRV

- Resolution set to invalid
- Status changed from Open to Closed

~~If I disable TimeManager, crash is gone; closing.~~

#3 - 2016-06-02 08:51 PM - Mathieu Pellerin - nIRV

- Resolution deleted (invalid)
- Assignee set to Nathan Woodrow
- Status changed from Closed to Reopened

I was wrong, the crasher is still occuring even when timemanager (and other plugins) are disabled.

Nathan can reproduce the crasher.

#4 - 2016-06-03 01:32 AM - Mathieu Pellerin - nIRV

I've installed Qt's debug package, here's a more complete gdb output of the crasher:

```
#0  QWidgetBackingStore::resetWidget (this=0xb7d6b90, widget=0xb0ab750) at painting/qbackingstore_p.h:247
#1  QWidgetBackingStore::~QWidgetBackingStore (this=0xb7d6b90, __in_chrg=<optimized out>) at painting/qbackingstore.cpp:906
#2  0x00007ffff4d4ab59 in QWidgetBackingStoreTracker::destroy (this=0xb781ea0) at kernel/qwidget.cpp:225
#3  0x00007ffff4d4acf4 in QWidgetPrivate::deleteExtra (this=this@entry=0xc074020) at kernel/qwidget.cpp:1833
#4  0x00007ffff4d4af3d in QWidgetPrivate::~QWidgetPrivate (this=0xc074020, __in_chrg=<optimized out>) at kernel/qwidget.cpp:365
#5  0x00007ffff51cf5b7 in QDialogPrivate::~QDialogPrivate (this=0xc074020, __in_chrg=<optimized out>)
    at ../../include/QtGui/private/../../../src/gui/dialogs/qdialog_p.h:66
#6  QDialogPrivate::~QDialogPrivate (this=0xc074020, __in_chrg=<optimized out>) at
../../include/QtGui/private/../../../src/gui/dialogs/qdialog_p.h:66
#7  0x00007ffff59d598a in QScopedPointerDeleter<QObjectData>::cleanup (pointer=<optimized out>) at
../../include/QtCore/../../src/corelib/tools/qscopedpointer.h:62
#8  QScopedPointer<QObjectData, QScopedPointerDeleter<QObjectData> >::~QScopedPointer (this=0xc09e0d8, __in_chrg=<optimized out>)
    at ../../include/QtCore/../../src/corelib/tools/qscopedpointer.h:100
```

#9 QObject::~QObject (this=0xc09e0d0, __in_chrg=<optimized out>) at kernel/qobject.cpp:844
#10 0x00007ffff4d57341 in QWidget::~QWidget (this=0xc09e0d0, __in_chrg=<optimized out>) at kernel/qwidget.cpp:1554
#11 0x00007ffff75dbabe in QgsAttributeTableDialog::~QgsAttributeTableDialog (this=0xc09e0d0, __in_chrg=<optimized out>) at ../src/app/qgsattributetabledialog.cpp:278
#12 0x00007ffff75dbafc in QgsAttributeTableDialog::~QgsAttributeTableDialog (this=0xc09e0d0, __in_chrg=<optimized out>) at ../src/app/qgsattributetabledialog.cpp:282
#13 0x00007ffff59d32b1 in QObjectPrivate::deleteChildren (this=this@entry=0xb97ce50) at kernel/qobject.cpp:1935
#14 0x00007ffff4d572a2 in QWidget::~QWidget (this=0xb7c0770, __in_chrg=<optimized out>) at kernel/qwidget.cpp:1679
#15 0x00007ffff798ee17 in QgsAttributeTableDock::~QgsAttributeTableDock (this=0xb7c0770, __in_chrg=<optimized out>)
    at src/app/../../../src/app/qgsattributetabledialog.h:238
#16 0x00007ffff798ee4c in QgsAttributeTableDock::~QgsAttributeTableDock (this=0xb7c0770, __in_chrg=<optimized out>)
    at src/app/../../../src/app/qgsattributetabledialog.h:238
#17 0x00007ffff59d4dd8 in QObject::event (this=this@entry=0xb7c0770, e=e@entry=0xb7f2050) at kernel/qobject.cpp:1203
#18 0x00007ffff4d57d3c in QWidget::event (this=this@entry=0xb7c0770, event=event@entry=0xb7f2050) at kernel/qwidget.cpp:8859
#19 0x00007ffff510e343 in QDockWidget::event (this=0xb7c0770, event=0xb7f2050) at widgets/qdockwidget.cpp:1492
#20 0x00007ffff4d00fdc in QApplicationPrivate::notify_helper (this=this@entry=0x8f7c30, receiver=receiver@entry=0xb7c0770, e=e@entry=0xb7f2050)
    at kernel/qapplication.cpp:4570
#21 0x00007ffff4d07f16 in QApplication::notify (this=0x7fffffffdad0, receiver=0xb7c0770, e=0xb7f2050) at kernel/qapplication.cpp:4356
#22 0x00007ffff604fe4d in QgsApplication::notify (this=0x7fffffffdad0, receiver=0xb7c0770, event=0xb7f2050) at ../src/core/qgsapplication.cpp:281
#23 0x00007ffff59ba90d in QCoreApplication::notifyInternal (this=0x7fffffffdad0, receiver=receiver@entry=0xb7c0770, event=event@entry=0xb7f2050)
    at kernel/qcoreapplication.cpp:955
#24 0x00007ffff59be3c6 in QCoreApplication::sendEvent (event=0xb7f2050, receiver=0xb7c0770) at ../../include/QtCore/../../src/corelib/kernel/qcoreapplication.h:231
#25 QCoreApplicationPrivate::sendPostedEvents (receiver=receiver@entry=0x0, event_type=event_type@entry=0, data=0x8d2a80) at kernel/qcoreapplication.cpp:1579
#26 0x00007ffff59be6a3 in QCoreApplication::sendPostedEvents (receiver=receiver@entry=0x0, event_type=event_type@entry=0) at kernel/qcoreapplication.cpp:1472
#27 0x00007ffff59eb13e in QCoreApplication::sendPostedEvents () at ../../include/QtCore/../../src/corelib/kernel/qcoreapplication.h:236
#28 postEventSourceDispatch (s=0x8df550) at kernel/qeventdispatcher_glib.cpp:300
#29 0x00007fffed4191a7 in g_main_context_dispatch () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#30 0x00007fffed419400 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#31 0x00007fffed4194ac in g_main_context_iteration () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#32 0x00007ffff59eb2ae in QEventDispatcherGlib::processEvents (this=0x853a10, flags=...) at kernel/qeventdispatcher_glib.cpp:450
#33 0x00007ffff4dae616 in QGuiEventDispatcherGlib::processEvents (this=<optimized out>, flags=...) at kernel/qguieventdispatcher_glib.cpp:204
---Type <return> to continue, or q <return> to quit---
#34 0x00007ffff59b918f in QEventLoop::processEvents (this=this@entry=0x7fffffffd150, flags=...) at kernel/qeventloop.cpp:149
#35 0x00007ffff59b94f5 in QEventLoop::exec (this=this@entry=0x7fffffffd150, flags=...) at kernel/qeventloop.cpp:204
#36 0x00007ffff59bf4b9 in QCoreApplication::exec () at kernel/qcoreapplication.cpp:1227
#37 0x0000000000409bfd in main (argc=1, argv=0x7fffffffddb8) at ../src/app/main.cpp:1257

#5 - 2016-06-12 09:00 PM - Mathieu Pellerin - nIRV

- Category changed from Attribute table to Map Canvas

Still crashing; updated gdb trace:

#0 QRegion::operator= (this=0xb2abf98, r=...) at painting/qregion.cpp:3935

#1 0x00007ffff4e8e9b9 in QWidgetBackingStore::resetWidget (this=0xb795dc0, widget=0xad9d4a0) at painting/qbackingstore_p.h:250
#2 QWidgetBackingStore::~QWidgetBackingStore (this=0xb795dc0, __in_chrg=<optimized out>) at painting/qbackingstore.cpp:906
#3 0x00007ffff4cb4b59 in QWidgetBackingStoreTracker::destroy (this=0xbcd4b10) at kernel/qwidget.cpp:225
#4 0x00007ffff4cb4cf4 in QWidgetPrivate::deleteExtra (this=this@entry=0xb189a00) at kernel/qwidget.cpp:1833
#5 0x00007ffff4cb4f3d in QWidgetPrivate::~QWidgetPrivate (this=0xb189a00, __in_chrg=<optimized out>) at kernel/qwidget.cpp:365
#6 0x00007ffff51395b7 in QDialogPrivate::~QDialogPrivate (this=0xb189a00, __in_chrg=<optimized out>) at
../../include/QtGui/private/../../../src/gui/dialogs/qdialog_p.h:66
#7 QDialogPrivate::~QDialogPrivate (this=0xb189a00, __in_chrg=<optimized out>) at
../../include/QtGui/private/../../../src/gui/dialogs/qdialog_p.h:66
#8 0x00007ffff593f98a in QScopedPointerDeleter<QObjectData>::cleanup (pointer=<optimized out>) at
../../include/QtCore/../../src/corelib/tools/qscopedpointer.h:62
#9 QScopedPointer<QObjectData, QScopedPointerDeleter<QObjectData> >::~QScopedPointer (this=0xb1cdee8, __in_chrg=<optimized out>)
    at ../../include/QtCore/../../src/corelib/tools/qscopedpointer.h:100
#10 QObject::~QObject (this=0xb1cdee0, __in_chrg=<optimized out>) at kernel/qobject.cpp:844
#11 0x00007ffff4cc1341 in QWidget::~QWidget (this=0xb1cdee0, __in_chrg=<optimized out>) at kernel/qwidget.cpp:1554
#12 0x00007ffff75d7e3e in QgsAttributeTableDialog::~QgsAttributeTableDialog (this=0xb1cdee0, __in_chrg=<optimized out>) at
../src/app/qgsattributetabledialog.cpp:277
#13 0x00007ffff75d7e7c in QgsAttributeTableDialog::~QgsAttributeTableDialog (this=0xb1cdee0, __in_chrg=<optimized out>) at
../src/app/qgsattributetabledialog.cpp:281
#14 0x00007ffff593d2b1 in QObjectPrivate::deleteChildren (this=this@entry=0xbdd17d0) at kernel/qobject.cpp:1935
#15 0x00007ffff4cc12a2 in QWidget::~QWidget (this=0xba322a0, __in_chrg=<optimized out>) at kernel/qwidget.cpp:1679
#16 0x00007ffff75e4702 in QgsDockWidget::~QgsDockWidget (this=0xba322a0, __in_chrg=<optimized out>) at
../src/app/../gui/qgsdockwidget.h:28
#17 0x00007ffff798c003 in QgsAttributeTableDock::~QgsAttributeTableDock (this=0xba322a0, __in_chrg=<optimized out>) at
src/app/../../../src/app/qgsattributetabledialog.h:238
#18 0x00007ffff798c038 in QgsAttributeTableDock::~QgsAttributeTableDock (this=0xba322a0, __in_chrg=<optimized out>) at
src/app/../../../src/app/qgsattributetabledialog.h:238
#19 0x00007ffff593edd8 in QObject::event (this=this@entry=0xba322a0, e=e@entry=0xba984e0) at kernel/qobject.cpp:1203
#20 0x00007ffff4cc1d3c in QWidget::event (this=this@entry=0xba322a0, event=event@entry=0xba984e0) at kernel/qwidget.cpp:8859
#21 0x00007ffff5078343 in QDockWidget::event (this=0xba322a0, event=0xba984e0) at widgets/qdockwidget.cpp:1492
#22 0x00007ffff4c6afdc in QApplicationPrivate::notify_helper (this=this@entry=0x8fbc60, receiver=receiver@entry=0xba322a0,
e=e@entry=0xba984e0) at kernel/qapplication.cpp:4570
#23 0x00007ffff4c71f16 in QApplication::notify (this=0x7fffffffdad0, receiver=0xba322a0, e=0xba984e0) at kernel/qapplication.cpp:4356
#24 0x00007ffff6006e89 in QgsApplication::notify (this=0x7fffffffdad0, receiver=0xba322a0, event=0xba984e0) at
../src/core/qgsapplication.cpp:281
#25 0x00007ffff592490d in QCoreApplication::notifyInternal (this=0x7fffffffdad0, receiver=receiver@entry=0xba322a0,
event=event@entry=0xba984e0) at kernel/qcoreapplication.cpp:955
#26 0x00007ffff59283c6 in QCoreApplication::sendEvent (event=0xba984e0, receiver=0xba322a0) at
../../include/QtCore/../../src/corelib/kernel/qcoreapplication.h:231
#27 QCoreApplicationPrivate::sendPostedEvents (receiver=receiver@entry=0x0, event_type=event_type@entry=0, data=0x8d6a80) at
kernel/qcoreapplication.cpp:1579
#28 0x00007ffff59286a3 in QCoreApplication::sendPostedEvents (receiver=receiver@entry=0x0, event_type=event_type@entry=0) at
kernel/qcoreapplication.cpp:1472
#29 0x00007ffff595513e in QCoreApplication::sendPostedEvents () at ../../include/QtCore/../../src/corelib/kernel/qcoreapplication.h:236
#30 postEventSourceDispatch (s=0x8e3580) at kernel/qeventdispatcher_glib.cpp:300
#31 0x00007fffed3801a7 in g_main_context_dispatch () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#32 0x00007fffed380400 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#33 0x00007fffed3804ac in g_main_context_iteration () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#34 0x00007ffff59552ae in QEventDispatcherGlib::processEvents (this=0x858d80, flags=...) at kernel/qeventdispatcher_glib.cpp:450
#35 0x00007ffff4d18616 in QGuiEventDispatcherGlib::processEvents (this=<optimized out>, flags=...) at kernel/qguieventdispatcher_glib.cpp:204
#36 0x00007ffff592318f in QEventLoop::processEvents (this=this@entry=0x7fffffffd150, flags=...) at kernel/qeventloop.cpp:149
#37 0x00007ffff59234f5 in QEventLoop::exec (this=this@entry=0x7fffffffd150, flags=...) at kernel/qeventloop.cpp:204
#38 0x00007ffff59294b9 in QCoreApplication::exec () at kernel/qcoreapplication.cpp:1227

#39 0x0000000000409cdd in main (argc=1, argv=0x7fffffffddb8) at ../src/app/main.cpp:1257

</pre?

#6 - 2016-06-13 12:52 AM - Mathieu Pellerin - nIRV

- Category changed from Map Canvas to Attribute table

#7 - 2016-06-13 07:53 AM - Even Rouault

I've investigated this and identified more precisely the cause of the crash.

?

The Valgrind log shows it is a double free issue :

```
==27531== Invalid read of size 8
==27531==    at 0x88BB0AD: QWidgetBackingStore::~QWidgetBackingStore() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x86F2918: QWidgetBackingStoreTracker::destroy() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x86F2A61: QWidgetPrivate::deleteExtra() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x86F2C7C: QWidgetPrivate::~QWidgetPrivate() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x8B4C48A: QDialogPrivate::~QDialogPrivate() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x8158EBB: QObject::~QObject() (in /home/even/install-qt-4.8.5/lib/libQtCore.so.4.8.5)
==27531==    by 0x86F4D6F: QWidget::~QWidget() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x50408B7: QgsAttributeTableDialog::~QgsAttributeTableDialog() (qgsattributetabledialog.cpp:277)
==27531==    by 0x5040941: QgsAttributeTableDialog::~QgsAttributeTableDialog() (qgsattributetabledialog.cpp:281)
==27531==    by 0x8155001: QObjectPrivate::deleteChildren() (in /home/even/install-qt-4.8.5/lib/libQtCore.so.4.8.5)
==27531==    by 0x86F4CD3: QWidget::~QWidget() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x504D511: QgsDockWidget::~QgsDockWidget() (in
/home/even/qgis-git/Quantum-GIS.clean/build/output/lib/libqgis_app.so.2.15.0)
==27531==  Address 0x930e8488 is 8 bytes inside a block of size 40 free'd
==27531==    at 0x4C283A4: operator delete(void*) (vg_replace_malloc.c:480)
==27531==    by 0x8155001: QObjectPrivate::deleteChildren() (in /home/even/install-qt-4.8.5/lib/libQtCore.so.4.8.5)
==27531==    by 0x86F4CD3: QWidget::~QWidget() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x8B25BAD: QAbstractScrollAreaScrollBarContainer::~QAbstractScrollAreaScrollBarContainer() (in
/home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x8155001: QObjectPrivate::deleteChildren() (in /home/even/install-qt-4.8.5/lib/libQtCore.so.4.8.5)
==27531==    by 0x86F4CD3: QWidget::~QWidget() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x60EFC3F: QgsAttributeTableView::~QgsAttributeTableView() (in
/home/even/qgis-git/Quantum-GIS.clean/build/output/lib/libqgis_gui.so.2.15.0)
==27531==    by 0x60EFC7B: QgsAttributeTableView::~QgsAttributeTableView() (qgsattributetableview.h:44)
==27531==    by 0x8155001: QObjectPrivate::deleteChildren() (in /home/even/install-qt-4.8.5/lib/libQtCore.so.4.8.5)
==27531==    by 0x86F4CD3: QWidget::~QWidget() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x8AFCDC8: QSplitter::~QSplitter() (in /home/even/install-qt-4.8.5/lib/libQtGui.so.4.8.5)
==27531==    by 0x8155001: QObjectPrivate::deleteChildren() (in /home/even/install-qt-4.8.5/lib/libQtCore.so.4.8.5)
```

Digging more, I've identified that the following code in QgsAttributeTableView::setModel() is the cause :

```
mActionWidget = createActionWidget( 0 );
mActionWidget->setVisible( false );
updateActionImage( mActionWidget );
```

If the widget is not created, or updateActionImage() not called, then there's no crash.

Alternatively, if you keep that code but change QgsAttributeTableView::createActionWidget() so that the toolButton = new QToolButton(this) and container = new QWidget(this) use nullptr instead of this as a parent, there's no crash (but the painting of the icon is corrupted).

So there's an ownership issue with the backing store of this widget...

#8 - 2016-06-13 09:33 PM - Mathieu Pellerin - nIRV

- File crash.mp4 added

I noticed a larger OGR dataset will do a better job at replicating the crash quicker (i.e., you won't need to open -> close -> open -> close -> etc. for long).

See attached video.

#9 - 2016-06-14 12:40 AM - Anonymous

- Status changed from Reopened to Closed

Fixed in changeset commit:"a05b2ad9a1ace292e77dbe8541240c0c8bc2a096".

Files

crash.mp4	1.85 MB	2016-06-13	Mathieu Pellerin - nIRV