QGIS Application - Bug report #14909
regression: QGIS crashes when closing docked attribute table
2016-05-26 07:37 PM - Mathieu Pellerin - nIRV

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Severe/Regression</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Nathan Woodrow</td>
</tr>
<tr>
<td>Category:</td>
<td>Attribute table</td>
</tr>
<tr>
<td>Affected QGIS version:</td>
<td>master</td>
</tr>
<tr>
<td>Regression?:</td>
<td>No</td>
</tr>
<tr>
<td>Easy fix?:</td>
<td>No</td>
</tr>
<tr>
<td>Pull Request or Patch supplied:</td>
<td>No</td>
</tr>
<tr>
<td>Crashes QGIS or corrupt data:</td>
<td>Yes</td>
</tr>
<tr>
<td>Copied to github as #:</td>
<td>22862</td>
</tr>
</tbody>
</table>

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:

```bash
#0  0x00007fff502c1e8 in QRegion::operator=(QRegion const&) ()
    from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#1  0x00007fff50abbb9 in ?? () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#2  0x00007fff54ed1b59 in ?? () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#3  0x00007fff54ed1cf4 in QWidgetPrivate::deleteExtra() ()
    from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#4  0x00007fff54ed1f3d in QWidgetPrivate::~QWidgetPrivate() ()
    from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#5  0x00007fff53565b7 in ?? () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#6  0x00007fff555b59a in QObject::QObject() ()
    from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#7  0x00007fff54ede841 in QWidget::QWidget() ()
    from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#8  0x00007fff7620ce4 in QgsAttributeTableDialog::QgsAttributeTableDialog() ()
    from /home/webmaster/dev/cpp/QGIS/bm/output/lib/libqgis_app.so.2.15.0
#9  0x00007fff7620d22 in QgsAttributeTableDialog::QgsAttributeTableDialog() ()
    from /home/webmaster/dev/cpp/QGIS/bm/output/lib/libqgis_app.so.2.15.0
#10 0x00007fff565a2b1 in QObjectPrivate::deleteChildren() ()
    from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#11 0x00007fff4ede2a2 in QWidget::QWidget() ()
    from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#12 0x00007fff79c0381 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 attribute table... Rejected 2016-06-13
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=0xc074020) at kernel/qwidget.cpp:1833
#4  0x00007ffff4d4af3d in QWidgetPrivate::~QWidgetPrivate (this=0xc074020, __in_chrg=<optimized out>) at kernel/qwidget.cpp:365
#5  0x00007fffff51f5b7 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  0x00007ff59d5f98a in QS scopedPointerDeleter<QObjectData>::cleanup (pointer=<optimized out>) at ../../include/QtCore/../../../src/corelib/tools/qscopedpointer.h:62
#8  QS scopedPointer<QObjectData, QS scopedPointerDeleter<QObjectData> >::~QS scopedPointer (this=0xc09e0d8, __in_chrg=<optimized out>) at ../../include/QtCore/../../../src/corelib/tools/qscopedpointer.h:100
```

2021-09-06
#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
I've investigated this and identified more precisely the cause of the crash.

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

```cpp
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:“a05b2ad9a1ace292e77db8541240c0c8bc2a096”.

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