QGIS Application - Bug report #6805
QGIS crashes updating non-spatial sqlite table

2012-12-01 02:29 PM - Rafael Varela

Status:	Closed		
Priority:	Normal		
Assignee:	Giuseppe Sucameli		
Category:	Python plugins		
Affected QGIS version:	1.8.0	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	fixed
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	15953

Description

changeAttributeValues() causes QGIS to crash when updating a non-spatial sqlite table. Adding new features works fine.

The problem occurs both running on Linux or Windows, and it can be reproduced with this script:

```
from qgis.core import *
import sqlite3

# Create simple SQLite table

conn = sqlite3.connect("/tmp/test.sqlite")
cursor = conn.cursor()

cursor.execute("CREATE TABLE tableName ('param' text, 'value' text)")
conn.commit()

cursor.execute("INSERT INTO tableName VALUES ('param1', 'value1')")
conn.commit()

cursor.execute("INSERT INTO tableName VALUES ('param22', 'value22')")
conn.commit()

conn.close()

# Add Layer to the interface (Works OK)

SQLiteLayer = QgsVectorLayer("/tmp/test.sqlite", "test", "ogr")

QgsMapLayerRegistry.instance().addMapLayers( [SQLiteLayer] )

# Add feature (Works OK)

paramindex = SQLiteLayer.dataProvider().fieldNameIndex("param")
valueindex = SQLiteLayer.dataProvider().fieldNameIndex("value")

newAttributes = {}
newAttributes[paramindex] = "newParam"
newAttributes[valueindex] = "newValue"

SQLiteLayer.startEditing()
```

```
newFeature = QgsFeature()
newFeature.setAttributeMap(newAttributes)
SQLiteLayer.dataProvider().addFeatures( [ newFeature ] )
SQLiteLayer.commitChanges()
del newFeature

# Update one feature (QGIS 1.8 crashes)

feature = QgsFeature()
SQLiteLayer.dataProvider().rewind()
SQLiteLayer.dataProvider().nextFeature(feature)

SQLiteLayer.startEditing()
SQLiteLayer.dataProvider().changeAttributeValues( {feature.id() : newAttributes} )
SQLiteLayer.commitChanges()
```

Associated revisions

Revision e81b0448 - 2012-12-02 07:52 PM - Giuseppe Sucameli

fix segfaults and memory leaks in sip files (fix #6805)

History

#1 - 2012-12-01 02:37 PM - Rafael Varela

Sorry, there's a mistake in the script.

Instead of

```
newAttributes = []
```

it should be

```
newAttributes = {}
```

#2 - 2012-12-01 03:01 PM - Giovanni Manghi

- Status changed from Open to Feedback

have you tested qgis master?

#3 - 2012-12-01 04:10 PM - Giuseppe Sucameli

- Status changed from Feedback to Closed

- Resolution set to invalid

Already fixed yesterday in commit:85faeb37a0.

#4 - 2012-12-01 04:14 PM - Giuseppe Sucameli

- Resolution deleted (invalid)

- Status changed from Closed to Feedback

I was wrong, similar problem, same provider, but not the same function.

#5 - 2012-12-02 02:02 AM - Martin Dobias

The crash is probably due to incorrect format of newAttributes. The values should be QVariant instances. (But it should not crash either.) What if you use:

```
newAttributes = { paramindex : QVariant("newparam"), valueindex : QVariant("newvalue") }
```

As a side note (not related to the crash), you don't need to use startEditing() and commitChanges() if you are modifying the provider directly (i.e. not using vector layer's edit buffer).

Also, you should always call provider's select() function before any actual nextFeature() calls. The rewind() method is useless here, too.

#6 - 2012-12-02 02:40 AM - Rafael Varela

Giuseppe:

Yes, my original script crashes master too. I've just installed the Windows build 70273b9 to test it.

Martin:

First of all, thank you very much for your comments. It clarifies some doubts I had about startEditing(), rewind() or select()

I changed the script to use Variant instances and now the update works OK.

Thanks again to you and Giuseppe for your support.

#7 - 2012-12-02 07:40 AM - Giuseppe Sucameli

Martin Dobias wrote:

> *The crash is probably due to incorrect format of newAttributes. The values should be QVariant instances. (But it should not crash either.)*

I've got crashes using the snipped above, the crash occurs in **convertions.sip** file.

Martin, I've seen that you didn't used sipConvertToMappedType for QMap<int, TYPE> since you got crashes (it was 2008), you replaced it with a snipped that manually converts a PyObject to QMap<int, TYPE>:

> *// using sipConvertToMappedType to convert directly to QMap<int, TYPE> doesn't work*

> *// and ends with a segfault*

In my Ubuntu 12.10, sip 4.13.3, using sipConvertToMappedType it works without any crash, probably it was fixed in somewhat sip version.
A #ifdef SIP_VERSION >= 0x041200 could help, we already know we get crashed using the actual code in SIP >= 4.12 (as it crashes on Win as well).

#8 - 2012-12-02 08:07 AM - Giuseppe Sucameli

Martin, I guess there's more than one problem in the current **conversions.sip** file...

Have a loot at lines 259-269:

```
    //TYPE *t = reinterpret_cast<TYPE *>(sipConvertToInstance(PyList_GET_ITEM(sipPy, i), sipClass_TYPE, sipTransferObj, SIP_NOT_NONE, &state, sipIsErr));
    QList<TYPE> * t = reinterpret_cast< QList<TYPE> * >(sipConvertToMappedType(PyList_GET_ITEM(sipPy, i), qlist_type, sipTransferObj, SIP_NOT_NONE, &state, sipIsErr));

    if (*sipIsErr)
    {
      sipReleaseInstance(t, sipClass_TYPE, state);
      delete ql;
      return 0;
    }
    ql->append(*t);
    sipReleaseInstance(t, sipClass_TYPE, state);
```

The TYPE* t variable was commented and replaced with QList<TYPE> * t, but the sipReleaseInstance is assuming to work on the old t variable...

I don't know if it makes sense to fix that and other similar problems or waiting for your merge...

#9 - 2012-12-02 08:12 AM - Giuseppe Sucameli

Giuseppe Sucameli wrote:

> *I've got crashes using the snipped above, the crash occurs in **convertions.sip** file.*

FYI, it crashes at line 627, sipReleaseInstance(tobj2, sipClass_TYPE, state);

I'm not a SIP guru, but probably the problem is the same I reported before, since tobj2 should be fa I suppose...

#10 - 2012-12-02 10:54 AM - Giuseppe Sucameli

- Status changed from Feedback to Closed

Fixed in changeset commit:"e81b0448890b6ec001736b5dff5c65aaf248bed0".

#11 - 2012-12-02 11:21 AM - Giuseppe Sucameli

- Resolution set to fixed

- Assignee set to Giuseppe Sucameli

Martin, I fixed the problems I found (memory leaks and segfaults) because I don't know if your branch will be merged soon (though I hope you do that).

I leaved your workaround there (I don't know which is the last SIP version that requires that hack) but the code I added uses the sipConvertToMappedType whether SIP >= 4.12.