# QGIS Application - Bug report #4912
# Segfault on exit-with-save

2012-01-30 05:43 AM - Sandro Santilli

| | | | |
|---|---|---|---|
| **Status:** | Closed | | |
| **Priority:** | High | | |
| **Assignee:** | | | |
| **Category:** | | | |
| **Affected QGIS version:** | 1.7.3 | **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 #:** | 14719 |

**Description**

When closing the main window and answering YES to "do you want to save?" I get a segfault, loosing all work done.

Debug lines:

```
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsvectorlayer.cpp: 182: (~QgsVectorLayer) entered.
Debug: /usr/src/qgis/qgis-1.7/src/providers/postgres/qgspostgresprovider.cpp: 198: (~QgsPostgresProvider) deconstructing.
Debug: /usr/src/qgis/qgis-1.7/src/app/legend/qgslegend.cpp: 239: (removeLayer) called.
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 830: (updateFullExtent) called.
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 887: (updateFullExtent) Full extent: Empty
Debug: /usr/src/qgis/qgis-1.7/src/gui/qgsmapoverviewcanvas.cpp: 174: (drawExtentRect) panning: extent to widget:
[-2147483648,-2147483648] [1x1]
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsvectorlayer.cpp: 182: (~QgsVectorLayer) entered.
Debug: /usr/src/qgis/qgis-1.7/src/providers/postgres/qgspostgresprovider.cpp: 198: (~QgsPostgresProvider) deconstructing.
Debug: /usr/src/qgis/qgis-1.7/src/providers/grass/qgsgrass.cpp: 583: (closeMapset) entered.
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 830: (updateFullExtent) called.
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 887: (updateFullExtent) Full extent: Empty
Debug: /usr/src/qgis/qgis-1.7/src/gui/qgsmapoverviewcanvas.cpp: 174: (drawExtentRect) panning: extent to widget:
[-2147483648,-2147483648] [1x1]
Debug: /usr/src/qgis/qgis-1.7/src/providers/grass/qgsgrass.cpp: 583: (closeMapset) entered.
Segmentation fault (core dumped)
```

Backtrace:

```
Core was generated by `qgis'.
Program terminated with signal 11, Segmentation fault.
#0  0x00007fc46d6ea76c in malloc_consolidate (av=0x7fc46d9f1e40) at malloc.c:5144
5144    malloc.c: No such file or directory.
        in malloc.c
(gdb) bt
#0  0x00007fc46d6ea76c in malloc_consolidate (av=0x7fc46d9f1e40) at malloc.c:5144
#1  0x00007fc46d6ed460 in _int_free (av=0x7fc46d9f1e40, p=0x2ddbc20) at malloc.c:5017
#2  0x00007fc46d6f0e83 in *__GI___libc_free (mem=<value optimized out>) at malloc.c:3738
#3  0x00007fc46eb922c9 in CPLCleanupTLSList (papTLSList=0x2dd57b0) at cpl_multiproc.cpp:184
#4  0x00007fc46eb525ea in ~GDALDriverManager (this=0x35813b0, __in_chrg=<value optimized out>) at
gdaldrivermanager.cpp:234
#5  0x00007fc46eb51cae in GDALDestroy () at gdaldllmain.cpp:67
#6  0x00007fc46e8a625f in __do_global_dtors_aux () from /usr/local/lib/libgdal.so
#7  0x0000000000000000 in ?? ()
```

This is with gdal 1.9.0

Unfortunately the simplest way I found to reproduce involves having a PostGIS topology setup.
To reproduce:

1. Load POSTGIS/topology/test/load_topology.sql into a database to create a "city_data" topology
2. Start db_manager, select your "city_data" schema and hit Topology Viewer
3. Close the qgis window
4. Answer "yes" to the "want to save?" question

Actually I think you get the segfault even if you answer "no"...

### History

#### #1 - 2012-01-30 05:45 AM - Giovanni Manghi

*- Priority changed from Normal to 6*

As it affects 1.7.3 I think the priority should be max.

#### #2 - 2012-01-30 05:47 AM - Sandro Santilli

I'm not sure it is a qgis or gdal issue. Gioman: can you reproduce ?

#### #3 - 2012-01-30 06:03 AM - Sandro Santilli

I've updated GDAL to current SVN trunk and as a result I get the segfault as soon as I close the GUI window, even before getting the save window.

#### #4 - 2012-01-30 06:20 AM - Sandro Santilli

Got some valgrind saying too (but qgis is stripped, looks like)

```
==21518== Invalid read of size 4
==21518==    at 0x26CB6783: PyObject_Free (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26C9D04A: ??? (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26CAFFBA: ??? (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26C7FCB2: ??? (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26CAE4E6: ??? (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26CB0E16: PyDict_SetItem (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26CB2E8C: _PyModule_Clear (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26CB2EC7: ??? (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26CB01F6: PyDict_DelItem (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26D11FA1: PyEval_EvalFrameEx (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26D15927: PyEval_EvalFrameEx (in /usr/lib/libpython2.6.so.1.0)
==21518==    by 0x26D15927: PyEval_EvalFrameEx (in /usr/lib/libpython2.6.so.1.0)
==21518==  Address 0x2afd9020 is 48 bytes inside a block of size 128 free'd
==21518==    at 0x4C26DCF: operator delete(void*) (vg_replace_malloc.c:387)
```

==21518== by 0x6AD25B2: ??? (in /usr/lib/libQtCore.so.4.6.2)
==21518== by 0x6ACB44E: ??? (in /usr/lib/libQtCore.so.4.6.2)
==21518== by 0x6AD082B: ??? (in /usr/lib/libQtCore.so.4.6.2)
==21518== by 0x6AD091D: ??? (in /usr/lib/libQtCore.so.4.6.2)
==21518== by 0x6AC3258: QSettings::~QSettings() (in /usr/lib/libQtCore.so.4.6.2)
==21518== by 0x273C9A27: ??? (in /usr/lib/pyshared/python2.6/PyQt4/QtCore.so)
==21518== by 0x273B3608: ??? (in /usr/lib/pyshared/python2.6/PyQt4/QtCore.so)
==21518== by 0x270D77F8: ??? (in /usr/lib/pyshared/python2.6/sip.so)
==21518== by 0x26CCD634: ??? (in /usr/lib/libpython2.6.so.1.0)
==21518== by 0x26C9B472: ??? (in /usr/lib/libpython2.6.so.1.0)
==21518== by 0x26D169C6: PyEval_EvalCodeEx (in /usr/lib/libpython2.6.so.1.0)

And

==21518== Invalid read of size 4
==21518== at 0x5354FC: QBasicAtomicInt::deref() (qatomic_x86_64.h:133)
==21518== by 0x55D384A: QList<QgsSearchTreeNode*>::~QList() (qlist.h:620)
==21518== by 0x9E1262F: __cxa_finalize (cxa_finalize.c:56)
==21518== by 0x54C9F15: ??? (in /usr/local/lib/libqgis_core.so.1.7.3)
==21518== by 0x59C06B0: ??? (in /usr/local/lib/libqgis_core.so.1.7.3)
==21518== by 0x9E12261: exit (exit.c:78)
==21518== by 0x9DF7C53: (below main) (libc-start.c:258)
==21518== Address 0x1f152470 is 0 bytes inside a block of size 56 free'd
==21518== at 0x4C270BD: free (vg_replace_malloc.c:366)
==21518== by 0x630F837: QList<QgsRasterCalcNode*>::free(QListData::Data*) (qlist.h:649)
==21518== by 0x630F8B9: QList<QgsRasterCalcNode*>::~QList() (qlist.h:621)
==21518== by 0x9E1262F: __cxa_finalize (cxa_finalize.c:56)
==21518== by 0x62BDD45: ??? (in /usr/local/lib/libqgis_analysis.so.1.7.3)
==21518== by 0x630F900: ??? (in /usr/local/lib/libqgis_analysis.so.1.7.3)
==21518== by 0x9E12261: exit (exit.c:78)
==21518== by 0x9DF7C53: (below main) (libc-start.c:258)

Dunno how raster calc is involved in this...

#### #5 - 2012-01-30 06:22 AM - Sandro Santilli

I've just tried MASTER and it is *also* affected.

#### #6 - 2012-01-30 06:25 AM - Sandro Santilli

*- File city_data.qgs added*

I'm attaching the qgis project you can use to try at reproducing the error.
It assumes you have a postgis database called "strk" in which you loaded load_topology.sql.
It serves the purpose of taking db_manager out of the picture.

#### #7 - 2012-01-30 06:30 AM - Paolo Cavallini

Here it works smoothly.

#### #8 - 2012-01-30 06:48 AM - Sandro Santilli

Paolo: which gdal version are you using ?

#### #9 - 2012-01-30 06:52 AM - Paolo Cavallini

1.7.3-6+b3, official package from Debian unstable

#### #10 - 2012-01-30 07:02 AM - Sandro Santilli

Then I guess it is a gdal issue ?
I filed this one : http://trac.osgeo.org/gdal/ticket/4476

#### #11 - 2012-01-30 08:00 AM - Sandro Santilli

*- File city_data_segfault.qgs added*

Attaching first simplification of the project file. May have to do with rule-based rendering.

#### #12 - 2012-01-30 08:41 AM - Sandro Santilli

There's surely something wrong in the tear-down process of qgis.

This is what comes out on clicking the "close-window" widget, note the calls to "updateFullExtent":

```
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 830: (updateFullExtent) called.
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 887: (updateFullExtent) Full extent: Empty
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 830: (updateFullExtent) called.
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 887: (updateFullExtent) Full extent: Empty
Debug: /usr/src/qgis/qgis-1.7/src/gui/qgsmapoverviewcanvas.cpp: 174: (drawExtentRect) panning: extent to widget: [-2147483648,-2147483648]
[1x1]
Debug: /usr/src/qgis/qgis-1.7/src/gui/qgsmapcanvas.cpp: 320: (setLayerSet) Layers have changed, refreshing
Debug: /usr/src/qgis/qgis-1.7/src/app/legend/qgslegend.cpp: 239: (removeLayer) called.
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 830: (updateFullExtent) called.
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 887: (updateFullExtent) Full extent: Empty
Debug: /usr/src/qgis/qgis-1.7/src/gui/qgsmapoverviewcanvas.cpp: 174: (drawExtentRect) panning: extent to widget: [-2147483648,-2147483648]
[1x1]
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsvectorlayer.cpp: 182: (~QgsVectorLayer) entered.
Debug: /usr/src/qgis/qgis-1.7/src/providers/postgres/qgspostgresprovider.cpp: 198: (~QgsPostgresProvider) deconstructing.
Debug: /usr/src/qgis/qgis-1.7/src/providers/grass/qgsgrass.cpp: 583: (closeMapset) entered.
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 830: (updateFullExtent) called.
Debug: /usr/src/qgis/qgis-1.7/src/core/qgsmaprenderer.cpp: 887: (updateFullExtent) Full extent: Empty
Debug: /usr/src/qgis/qgis-1.7/src/gui/qgsmapoverviewcanvas.cpp: 174: (drawExtentRect) panning: extent to widget: [-2147483648,-2147483648]
[1x1]
Debug: /usr/src/qgis/qgis-1.7/src/providers/grass/qgsgrass.cpp: 583: (closeMapset) entered.
Segmentation fault (core dumped)
```

I build with: -DQGISDEBUG=1 -D CMAKE_BUILD_TYPE=Debug

#### #13 - 2012-01-30 11:24 AM - Martin Dobias

Does it segfault even if you disable all plugins?

#### #14 - 2012-01-30 11:45 PM - Sandro Santilli

Yes, it does happen w/out any plugin enabled.

#### #15 - 2012-02-10 11:08 PM - Paolo Cavallini

*- Priority changed from 6 to High*

#### #16 - 2012-02-15 03:32 AM - Giovanni Manghi

Sandro Santilli wrote:

> *I'm not sure it is a qgis or gdal issue. Gioman: can you reproduce ?*

no, I can't replicate the issue.

#### #17 - 2012-04-16 03:56 AM - Giovanni Manghi

*- Status changed from Open to Feedback*

Can you please give it a try with qgis master? thanks.

#### #18 - 2012-04-16 04:03 AM - Sandro Santilli

I can't reproduce with master (58f754b) - I guess it was fixed..

#### #19 - 2012-04-16 06:32 AM - Paolo Cavallini

*- Target version changed from Version 1.7.4 to Version 1.8.0*

#### #20 - 2012-05-30 03:36 AM - Giovanni Manghi

*- Status changed from Feedback to Closed*

*- Resolution set to fixed*

### Files

| | | | |
|---|---|---|---|
| city_data.qgs | 61.4 KB | 2012-01-30 | Sandro Santilli |
| city_data_segfault.qgs | 20.7 KB | 2012-01-30 | Sandro Santilli |