

QGIS Application - Bug report #15345

Crashes when switching to some UTM CRSs with certain data

2016-07-26 12:51 PM - Johannes Kroeger

Status: Priority: Assignee: Category: Affected QGIS version: Operating System: Pull Request or Patch supplied: Crashes QGIS or corrupts data:	Closed High Projection Support 2.18.4 No No No Yes	Regression?: Easy fix?: Resolution: Copied to github as #:	No No 23277
Description This could probably be nailed down better but here it goes: Load the shapefile from http://www.naturalearthdata.com/http://www.naturalearthdata.com/download/10m/cultural/ne_10m_populated_places.zip (also works with the layer from their sqlite version) Switch OTF CRS to EPSG 25832 or 25833 (probably many others result in the same crash). QGIS will crash. I am on Archlinux, qgis built from master a short while ago at 7343b36. With gdb I got this backtrace: <pre>*** Error in `/usr/bin/qgis': double free or corruption (fasttop): 0x00007fff3c0010e0 *** ===== Backtrace: ===== /usr/lib/libc.so.6(+0x6ed4b)[0x7ffff43fad4b] /usr/lib/libc.so.6(+0x74546)[0x7ffff4400546] /usr/lib/libc.so.6(+0x74d1e)[0x7ffff4400d1e] /usr/lib/libqgis_core.so.2.99.0(_ZN11QgsSymbolV210stopRenderER16QgsRenderContext+0xbf)[0x7ffff61b6ccf] /usr/lib/libqgis_core.so.2.99.0(_ZN25QgsSingleSymbolRendererV210stopRenderER16QgsRenderContext+0x1a)[0x7ffff616f8aa][?]usr/lib/libc.so.6(+0x74546)[0x7ffff4400546]] /usr/lib/libqgis_core.so.2.99.0(+0x5f9b7e)[0x7ffff6504b7e] /usr/lib/libqgis_core.so.2.99.0(+0x5fb019)[0x7ffff6506019] /usr/lib/libqgis_core.so.2.99.0(_ZN25QgsMapRendererParallelJob17renderLayerStaticER14LayerRenderJob+0x67)[0x7ffff639b587][?]usr/lib/libc.so.6(+0x74546)[0x7ffff4400546] 87] /usr/lib/libqgis_core.so.2.99.0(+0x491ba6)[0x7ffff639cba6] /usr/lib/libqgis_core.so.2.99.0(+0x491f28)[0x7ffff639cf28] /usr/lib/libQtCore.so.4(_ZN12QtConcurrent16ThreadEngineBase3runEv+0x6d)[0x7ffff5a8030d] /usr/lib/libQtCore.so.4(+0x7f3fa)[0x7ffff5a823fa] /usr/lib/libQtCore.so.4(+0x8c12c)[0x7ffff5a8f12c] /usr/lib/libpthread.so.0(+0x7484)[0x7ffeda44484] /usr/lib/libc.so.6(clone+0x6d)[0x7ffff44736dd]</pre>			

Associated revisions

Revision fefa572e - 2017-05-07 11:53 PM - Nyall Dawson

Fix crash when transform errors occur while rendering

If a transform exception occurred while rendering a symbol then the QgsSymbolRenderContext cleanup code was never called, leading to a double delete and crash.

Fixes #16377, #15345, and numerous other crashes seen "in the wild"

Possibly refs #16385

Revision 452c8066 - 2017-05-12 12:15 AM - Nyal Dawson

Fix crash when transform errors occur while rendering

If a transform exception occurred while rendering a symbol then the QgsSymbolRenderContext cleanup code was never called, leading to a double delete and crash.

Fixes #16377, #15345, and numerous other crashes seen "in the wild"

Possibly refs #16385

(cherry-picked from fefa572)

History

#1 - 2016-07-26 12:55 PM - Johannes Kroeger

Huh! I played around some more. If I load the file, then first set OTF CRS to EPSG 3978, then to 25832, I will get the same backtrace.

If I go 3978 -> 25833 however, I get this:

```
Thread 1 "qgis" received signal SIGSEGV, Segmentation fault.  
0x00007ffff440d76c in __memset_sse2 () from /usr/lib/libc.so.6
```

#2 - 2016-07-26 02:22 PM - Nyal Dawson

- Status changed from Open to Feedback

I can't reproduce (on ubuntu 16.04). Can you share a project?

#3 - 2016-07-27 06:11 AM - Johannes Kroeger

No project needed, it seems not to rely on anything (tried with a clean state, no .qgis2, no .config/QGIS/QGIS2.conf). I also reproduced it on another Archlinux system, there I used c9d6269.

#4 - 2016-07-27 09:56 AM - Johannes Kroeger

I just realised that above was not an actual gdb backtrace. Here is one from 2.16 built via <https://aur.archlinux.org/cgit/aur.git/tree/PKGBUILD?h=qgis>

```
#0 0x00007ffff43ca295 in raise () from /usr/lib/libc.so.6
#1 0x00007ffff43cb6da in abort () from /usr/lib/libc.so.6
#2 0x00007ffff4405d50 in __libc_message () from /usr/lib/libc.so.6
#3 0x00007ffff440b546 in malloc_printerr () from /usr/lib/libc.so.6
#4 0x00007ffff440bd1e in _int_free () from /usr/lib/libc.so.6
#5 0x00007ffff61c207f in QgsSymbolV2::stopRender(QgsRenderContext&) () from /usr/lib/libqgis_core.so.2.16.0
#6 0x00007ffff617af5a in QgsSingleSymbolRendererV2::stopRender(QgsRenderContext&) () from /usr/lib/libqgis_core.so.2.16.0
#7 0x00007ffff650b30e in QgsVectorLayerRenderer::drawRendererV2(QgsFeatureIterator&) () from /usr/lib/libqgis_core.so.2.16.0
#8 0x00007ffff650c8f5 in QgsVectorLayerRenderer::render() () from /usr/lib/libqgis_core.so.2.16.0
#9 0x00007ffff63a4b37 in QgsMapRendererParallelJob::renderLayerStatic(LayerRenderJob&) () from /usr/lib/libqgis_core.so.2.16.0
#10 0x00007ffff63a6156 in QtConcurrent::MapKernel<QList<LayerRenderJob>::iterator, QtConcurrent::FunctionWrapper1<void, LayerRenderJob&> >::runIterations(QList<LayerRenderJob>::iterator, int, int, void*)
    () from /usr/lib/libqgis_core.so.2.16.0
#11 0x00007ffff63a64d8 in QtConcurrent::IterateKernel<QList<LayerRenderJob>::iterator, void>::threadFunction() () from /usr/lib/libqgis_core.so.2.16.0
#12 0x00007ffff5a8b30d in QtConcurrent::ThreadEngineBase::run() () from /usr/lib/libQtCore.so.4
#13 0x00007ffff5a8d3fa in ?? () from /usr/lib/libQtCore.so.4
#14 0x00007ffff5a9a12c in ?? () from /usr/lib/libQtCore.so.4
#15 0x00007fffed4f484 in start_thread () from /usr/lib/libpthread.so.0
#16 0x00007ffff447e6dd in clone () from /usr/lib/libc.so.6
```

#5 - 2016-07-27 10:02 AM - Giovanni Manghi

- Priority changed from Normal to High
- Crashes QGIS or corrupts data changed from No to Yes
- Status changed from Feedback to Open
- Category set to Projection Support

Hi Nyal,

here (Ubuntu 16.04) it crashes too.

#6 - 2017-03-07 08:22 AM - Giovanni Manghi

- Affected QGIS version changed from master to 2.18.4
- Target version set to Version 2.18

#7 - 2017-05-01 01:02 AM - Giovanni Manghi

- Easy fix? set to No
- Regression? set to No

#8 - 2017-05-12 12:00 AM - Nyal Dawson

- Status changed from Open to Closed
- % Done changed from 0 to 100

Applied in changeset commit:qgis|fefa572e9f8a559e029dd9a369e5a8a1921de00b.