

# QGIS Application - Bug report #16377

## Crash when zooming a reprojected PostGIS layer

2017-03-25 01:50 AM - Paolo Cavallini

<b>Status:</b> Closed <b>Priority:</b> High <b>Assignee:</b> <b>Category:</b> Projection Support <b>Affected QGIS version:</b> 2.18.4 <b>Operating System:</b> Debian <b>Pull Request or Patch supplied:</b> No <b>Crashes QGIS or corrupts data:</b> Yes	<b>Regression?:</b> Yes <b>Easy fix?:</b> No <b>Resolution:</b> <b>Copied to github as #:</b> 24287
<b>Description</b>  A PostGIS layer with a wrong extent (-inf, -inf - -10.56548, 9.94114, EPSG:4326) reliably causes QGIS to crash when zooming in deeper than 1:50.000, if reprojected to EPSG:3857. No crash if not reprojected. bt says:  <pre> #0 __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:58 #1 0x00007fffd8e140a in __GI_abort () at abort.c:89 #2 0x00007fffd91dbd0 in __libc_message (do_abort=do_abort@entry=2,     fmt=fmt@entry=0x7ffeda12c30 "**** Error in `%s': %s: 0x%s ***\n")     at ../sysdeps/posix/libc_fatal.c:175 #3 0x00007fffd923f96 in malloc_printerr (action=3,     str=0x7ffeda12d88 "double free or corruption (fasttop)", ptr=&lt;optimized out&gt;,     ar_ptr=&lt;optimized out&gt;) at malloc.c:5046 #4 0x00007fffd92478e in _int_free (av=0x7fff20000020, p=0x7fff2000bab0, have_lock=0) at malloc.c:3902 #5 0x00007ffff503809e in QgsSymbolV2RenderContext::~QgsSymbolV2RenderContext (this=0x7fff2001bdf0,     __in_chrg=&lt;optimized out&gt;) at /usr/local/src/qgis/QGIS/src/core/symbology-ng/qgssymbolv2.cpp:1049 #6 0x00007ffff50349a3 in QgsSymbolV2::stopRender (this=0x555555fd2af0, context=...)     at /usr/local/src/qgis/QGIS/src/core/symbology-ng/qgssymbolv2.cpp:469 #7 0x00007ffff4ff6dca in QgsSingleSymbolRendererV2::stopRender (this=0x55555632d4070, context=...)     at /usr/local/src/qgis/QGIS/src/core/symbology-ng/qgssinglesymbolrendererv2.cpp:127 #8 0x00007ffff536bc00 in QgsVectorLayerRenderer::stopRenderV2 (this=0x555556185ab0, selRenderer=0x0)     at /usr/local/src/qgis/QGIS/src/core/qgsvectorlayerrenderer.cpp:524 #9 0x00007ffff536aa66 in QgsVectorLayerRenderer::drawRendererv2 (this=0x555556185ab0, fit=...)     at /usr/local/src/qgis/QGIS/src/core/qgsvectorlayerrenderer.cpp:363 #10 0x00007ffff5369f2e in QgsVectorLayerRenderer::render (this=0x555556185ab0)     at /usr/local/src/qgis/QGIS/src/core/qgsvectorlayerrenderer.cpp:256 #11 0x00007ffff520fb77 in QgsMapRendererParallelJob::renderLayerStatic (job=...)     at /usr/local/src/qgis/QGIS/src/core/qgsmaprenderparalleljob.cpp:261 #12 0x00007ffff5210e8a in QtConcurrent::FunctionWrapper1&lt;void, LayerRenderJob&amp;&gt;::operator() (     this=0x555556311a8f8, u=...) at /usr/include/qt4/QtCore/qtconcurrentfunctionwrappers.h:86 #13 0x00007ffff5210bed in QtConcurrent::MapKernel&lt;QList&lt;LayerRenderJob&gt;::iterator, QtConcurrent::FunctionWrapper1&lt;void,     LayerRenderJob&amp;&gt; &gt;::runIteration (this=0x555556311a8c0, it=...)     at /usr/include/qt4/QtCore/qtconcurrentmapkernel.h:73 #14 0x00007ffff5210c77 in QtConcurrent::MapKernel&lt;QList&lt;LayerRenderJob&gt;::iterator, QtConcurrent::FunctionWrapper1&lt;void,     LayerRenderJob&amp;&gt; &gt;::runIterations (this=0x555556311a8c0, sequenceBeginIterator=...,     beginIndex=0, endIndex=1) at /usr/include/qt4/QtCore/qtconcurrentmapkernel.h:82 #15 0x00007ffff52110c9 in QtConcurrent::IterateKernel&lt;QList&lt;LayerRenderJob&gt;::iterator, void&gt;::forThreadFunction     (this=0x555556311a8c0) at /usr/include/qt4/QtCore/qtconcurrentiteratekernel.h:263 #16 0x00007ffff5210df4 in QtConcurrent::IterateKernel&lt;QList&lt;LayerRenderJob&gt;::iterator, void&gt;::threadFunction </pre>	

```
(this=0x55556311a8c0) at /usr/include/qt4/QtCore/qtconcurrenttiterkernel.h:225
#17 0x00007ffff467bd5d in QtConcurrent::ThreadEngineBase::run() ()
    from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#18 0x00007ffff467ddba in ?? () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#19 0x00007ffff468adaa in ?? () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#20 0x00007ffefcafc424 in start_thread (arg=0x7fff2aac1700) at pthread_create.c:333
#21 0x00007ffed9959bf in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:105
```

---

## Associated revisions

### Revision fefa572e - 2017-05-07 11:53 PM - 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

### 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 - 2017-03-27 04:07 AM - Giovanni Manghi

- Status changed from Open to Feedback

it was tagged as regression because this caused no crash in a previous qgis release?

I would be interested in the data to allow me try replicate the crash also on other systems.

### #2 - 2017-04-29 04:56 AM - Giovanni Manghi

can we have a copy/dump of data? thanks.

**#3 - 2017-04-29 05:58 AM - Paolo Cavallini**

- *Crashes QGIS or corrupts data changed from No to Yes*

It was classified as severe because it causes a crash.

Now looking for the data.

**#4 - 2017-04-29 06:01 AM - Paolo Cavallini**

- *File test2\_zoom.zip added*

- *Status changed from Feedback to Open*

Importing the attached shp to PostGIS via drag&drop on DB Manager resulted in a layer with the wrong bounding box, which triggers the crash.

**#5 - 2017-04-29 11:35 AM - Giovanni Manghi**

Paolo Cavallini wrote:

*It was classified as severe because it causes a crash.  
Now looking for the data.*

severe is used for regressions, high for causing crashes (or other high priority issues) that are not necessarily regressions. Is this a known regression?

Thanks for the data.

**#6 - 2017-04-29 11:54 AM - Giovanni Manghi**

- *Status changed from Open to Feedback*

Tried on 2.18.7 on Linux/Ubuntu 16.04 and Windows several ways to import including d&d in db manager. No method resulted in invalid extent for the layer, and once loaded no one crashed qgis after zooming in below 1:50000.

**#7 - 2017-04-29 12:06 PM - Paolo Cavallini**

If the extent is valid, I do not expect a crash.

We had extensive discussion on the ML, possibly it has been fixed in the meantime without closing the ticket?

Thanks for checking.

**#8 - 2017-04-30 05:06 PM - Giovanni Manghi**

- *Regression? set to Yes*

**#9 - 2017-04-30 05:09 PM - Giovanni Manghi**

- *Priority changed from Severe/Regression to High*

**#10 - 2017-05-01 01:10 AM - Giovanni Manghi**

- *Easy fix? set to No*

#11 - 2017-05-12 12:00 AM - Nyal Dawson

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

Applied in changeset commit:qgis|fefa572e9f8a5559e029dd9a369e5a8a1921de00b.

Files

test2_zoom.zip	84 KB	2017-04-29	Paolo Cavallini
----------------	-------	------------	-----------------