

QGIS Application - Bug report #15575

regression: zooming in on a canvas with a diagram-enabled polygon layer kills QGIS

2016-09-17 03:55 AM - Mathieu Pellerin - nIRV

Status:	Closed	
Priority:	Severe/Regression	
Assignee:		
Category:	Diagrams	
Affected QGIS version:	master	Regression?: No
Operating System:		Easy fix?: No
Pull Request or Patch supplied:	No	Resolution:
Crashes QGIS or corrupts data:	Yes	Copied to github as #: 23499
Description		
Under QGIS master (2.99), zooming in on a canvas with a pie diagram-enabled polygon layer instantly crash QGIS. Here's a preliminary gdb where output (I don't have a debug build at-hand on this machine): <pre>#0 __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:58 #1 0x00007ffff41403ea in __GI_abort () at abort.c:89 #2 0x00007ffff477858d in __gnu_cxx::__verbose_terminate_handler() () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6 #3 0x00007ffff4776336 in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6 #4 0x00007ffff4776381 in std::terminate() () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6 #5 0x00007ffff4776eff in __cxa_pure_virtual () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6 #6 0x00007ffff4ad4327 in GEOSGeom_clone_r () from /usr/lib/x86_64-linux-gnu/libgeos_c.so.1 #7 0x00007ffff6135f0d in QgsVectorLayerDiagramProvider::registerDiagram(QgsFeature&, QgsRenderContext&, QgsGeometry*) () from /home/webmaster/dev/cpp/QGIS/bm-qt5/output/lib/libqgis_core.so.2.99.0 #8 0x00007ffff6135a8b in QgsVectorLayerDiagramProvider::registerFeature(QgsFeature&, QgsRenderContext&, QgsGeometry*) () from /home/webmaster/dev/cpp/QGIS/bm-qt5/output/lib/libqgis_core.so.2.99.0 #9 0x00007ffff6158252 in QgsVectorLayerRenderer::drawRenderer(QgsFeatureIterator&) () from /home/webmaster/dev/cpp/QGIS/bm-qt5/output/lib/libqgis_core.so.2.99.0 #10 0x00007ffff6157804 in QgsVectorLayerRenderer::render() () from /home/webmaster/dev/cpp/QGIS/bm-qt5/output/lib/libqgis_core.so.2.99.0 #11 0x00007ffff6003898 in QgsMapRendererParallelJob::renderLayerStatic(LayerRenderJob&) () from /home/webmaster/dev/cpp/QGIS/bm-qt5/output/lib/libqgis_core.so.2.99.0 #12 0x00007ffff60047ea in QtConcurrent::FunctionWrapper1<void, LayerRenderJob&>::operator()(LayerRenderJob&) () from /home/webmaster/dev/cpp/QGIS/bm-qt5/output/lib/libqgis_core.so.2.99.0 #13 0x00007ffff6004529 in QtConcurrent::MapKernel<QList<LayerRenderJob>::iterator, QtConcurrent::FunctionWrapper1<void, LayerRenderJob&> >::runIteration(QList<LayerRenderJob>::iterator, int, void*) () from /home/webmaster/dev/cpp/QGIS/bm-qt5/output/lib/libqgis_core.so.2.99.0</pre> I'm running on a Qt5 build, although I have not tested against a Qt4 build to see whether that's related to the crash.		

Associated revisions

Revision 9264be89 - 2016-09-19 03:13 PM - Mathieu Pellerin - nIRV

fix diagram crash (fixes #15575) (#3504)

History

#1 - 2016-09-17 05:26 AM - Mathieu Pellerin - nIRV

Here's a debug build gdb output:

```
#0 __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:58
#1 0x00007ffff3fd23ea in __GI_abort () at abort.c:89
#2 0x00007ffff460a58d in __gnu_cxx::__verbose_terminate_handler() () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#3 0x00007ffff4608336 in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#4 0x00007ffff4608381 in std::terminate() () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#5 0x00007ffff4608eff in __cxa_pure_virtual () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#6 0x00007ffff959327 in GEOSGeom_clone_r () from /usr/lib/x86_64-linux-gnu/libgeos_c.so.1
#7 0x00007ffff6005677 in QgsVectorLayerDiagramProvider::registerDiagram (this=0x55555c599680, feat=..., context=...,
obstacleGeometry=0x0)
    at /home/webmaster/dev/cpp/QGIS/src/core/qgsvectorlayerdiagramprovider.cpp:248
#8 0x00007ffff60051f5 in QgsVectorLayerDiagramProvider::registerFeature (this=0x55555c599680, feature=..., context=...,
obstacleGeometry=0x0)
    at /home/webmaster/dev/cpp/QGIS/src/core/qgsvectorlayerdiagramprovider.cpp:192
#9 0x00007ffff602931f in QgsVectorLayerRenderer::drawRenderer (this=0x55555643ef30, fit=...) at
/home/webmaster/dev/cpp/QGIS/src/core/qgsvectorlayerrenderer.cpp:364
#10 0x00007ffff60286be in QgsVectorLayerRenderer::render (this=0x55555643ef30) at
/home/webmaster/dev/cpp/QGIS/src/core/qgsvectorlayerrenderer.cpp:260
#11 0x00007ffff5eb0fe in QgsMapRendererParallelJob::renderLayerStatic (job=...) at
/home/webmaster/dev/cpp/QGIS/src/core/qgsmaprenderparalleljob.cpp:232
#12 0x00007ffff5ec05e6 in QtConcurrent::FunctionWrapper1<void, LayerRenderJob&>::operator() (this=0x55555c0d3fc8, u=...)
    at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentfunctionwrappers.h:77
#13 0x00007ffff5ec0325 in QtConcurrent::MapKernel<QList<LayerRenderJob>::iterator, QtConcurrent::FunctionWrapper1<void,
LayerRenderJob&> >::runIteration (
    this=0x55555c0d3f90, it=...) at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentmapkernel.h:63
#14 0x00007ffff5ec03be in QtConcurrent::MapKernel<QList<LayerRenderJob>::iterator, QtConcurrent::FunctionWrapper1<void,
LayerRenderJob&> >::runIterations (
    this=0x55555c0d3f90, sequenceBeginIterator=..., beginIndex=0, endIndex=1) at
/usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentmapkernel.h:72
#15 0x00007ffff5ec088e in QtConcurrent::IterateKernel<QList<LayerRenderJob>::iterator, void>::forThreadFunction (this=0x55555c0d3f90)
    at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentiteratekernel.h:250
#16 0x00007ffff5ec0550 in QtConcurrent::IterateKernel<QList<LayerRenderJob>::iterator, void>::threadFunction (this=0x55555c0d3f90)
    at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentiteratekernel.h:212
#17 0x00007ffff7e23c2d in QtConcurrent::ThreadEngineBase::run() () from /usr/lib/x86_64-linux-gnu/libQt5Concurrent.so.5
#18 0x00007ffff49aaf6f in ?? () from /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#19 0x00007ffff49aec68 in ?? () from /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#20 0x00007fffee16470a in start_thread (arg=0x7fff26ffd700) at pthread_create.c:333
#21 0x00007ffff40a30ff in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:105
```

#2 - 2016-09-17 09:37 PM - Mathieu Pellerin - nIRV

Under 2.16, QGIS does **not** crash.

#3 - 2016-09-18 09:57 PM - Mathieu Pellerin - nIRV

One more finding: crash occurs only when geometries are clipped to visible extent (i.e., if features of a given diagram-enabled layer are all visible within the

extent, it won't crash).

#4 - 2016-09-19 06:14 AM - Mathieu Pellerin - nIRV

- *Status changed from Open to Closed*

Fixed in changeset commit:"9264be89e319282f307edcb961395d82c12d1b3e".