QGIS Application - Bug report #17089
concurrent rendering of a single SVG picture freezes / crashes QGIS

2017-08-30 10:17 AM - Mathieu Pellerin - nIRV

Status:	Closed		
Priority:	High		
Assignee:	Nyall Dawson		
Category:	Symbology		
Affected QGIS version:	master	**Regression?:**	Yes
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	24988

Description

This was uncovered by the (amazing) composer map item preview rendering upgrade.

It appears that when a single SVG picture (possibly cached?) is rendered concurrently, QGIS either crashes or a thread is stuck and the app can't exit properly. On the thread frozen front, it translates into a composer map item stuck in "rendering map..." mode.

Steps to reproduce

1. Open the attached test project
2. Open the "Composer 01" composer
3. Notice either a QGIS crash, or one of the two map items stuck in "rendering map..."
4. If a crash doesn't occur on first try, just re-launch QGIS and re-do the steps a couple of times, you'll hit the crash

GDB where

```
(gdb) where
#0  0x00007f75f08344aa in  () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#1  0x00007f75f083d68e in  () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#2  0x00007f75f080be0e in  () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#3  0x00007f75f0814556 in  () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#4  0x00007f75f087b055 in QRasterPaintEngine::stroke(QVectorPath const&, QPen const&) () at
/usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#5  0x00007f75f088e70f in QPainter::strokePath(QPainterPath const&, QPen const&) () at
/usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#6  0x00007f75f088e88f in QPainter::drawArc(QRectF const&, int, int) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#7  0x00007f75f0689d69 in QPicture::exec(QPainter*, QDataStream&, int) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#8  0x00007f75f068bce9 in QPicture::play(QPainter*) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#9  0x00007f75f08953b2 in QPainter::drawPicture(QPointF const&, QPicture const&) () at
/usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#10 0x00007f75f1881d85 in QPainter::drawPicture(QPoint const&, QPicture const&) (this=0x10327a0d0, pt=..., p=...) at
/usr/include/x86_64-linux-gnu/qt5/QtGui/qpainter.h:928
#11 0x00007f75f1881d20 in QPainter::drawPicture(int, int, QPicture const&) (this=0x10327a0d0, x=0, y=0, p=...) at
/usr/include/x86_64-linux-gnu/qt5/QtGui/qpainter.h:923
#12 0x00007f75f18775ee in QgsSvgMarkerSymbolLayer::renderPoint(QPointF, QgsSymbolRenderContext&)
(this=0x10341c5f0, point=..., context=...)
    at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgsmarkersymbollayer.cpp:2007
#13 0x00007f75f18fde76 in QgsMarkerSymbol::renderPointUsingLayer(QgsMarkerSymbolLayer*, QPointF,
QgsSymbolRenderContext&) (this=0x10341c760, layer=0x10341c5f0, point=..., context=...) at
/home/webmaster/dev/cpp/QGIS/src/core/symbology/qgssymbol.cpp:1443
#14 0x00007f75f18fe219 in QgsMarkerSymbol::renderPoint(QPointF, QgsFeature const*, QgsRenderContext&, int, bool)
(this=0x10341c760, point=..., f=
    0x7f7514004d90, context=..., layerIdx=-1, selected=false) at
```

/home/webmaster/dev/cpp/QGIS/src/core/symbology/qgssymbol.cpp:1477
#15 0x00007f75f1825694 in QgsCentroidFillSymbolLayer::renderPolygon(QPolygonF const&, QList<QPolygonF>*, QgsSymbolRenderContext&) (this=0x10341b900, points=..., rings=0x0, context=...) at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgsfillsymbollayer.cpp:3479
#16 0x00007f75f1900879 in QgsFillSymbol::renderPolygonUsingLayer(QgsSymbolLayer*, QPolygonF const&, QList<QPolygonF>*, QgsSymbolRenderContext&) (this=0x103357770, layer=0x10341b900, points=..., rings=0x0, context=...) at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgssymbol.cpp:1801
#17 0x00007f75f19002ae in QgsFillSymbol::renderPolygon(QPolygonF const&, QList<QPolygonF>*, QgsFeature const*, QgsRenderContext&, int, bool) (this=0x103357770, points=..., rings=0x0, f=0x7f7514004d90, context=..., layerIdx=0, selected=false) at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgssymbol.cpp:1752
#18 0x00007f75f18fa7c0 in QgsSymbol::renderFeature(QgsFeature const&, QgsRenderContext&, int, bool, bool, int, int) (this=0x103357770, feature=..., context=..., layer=0, selected=false, drawVertexMarker=false, currentVertexMarkerType=1, currentVertexMarkerSize=3) at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgssymbol.cpp:918
#19 0x00007f75f18905aa in QgsFeatureRenderer::renderFeatureWithSymbol(QgsFeature&, QgsSymbol*, QgsRenderContext&, int, bool, bool) (this=0x102fc0450, feature=..., symbol=0x103357770, context=..., layer=0, selected=false, drawVertexMarker=false) at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgsrenderer.cpp:110
#20 0x00007f75f1890540 in QgsFeatureRenderer::renderFeature(QgsFeature&, QgsRenderContext&, int, bool, bool) (this=0x102fc0450, feature=..., context=..., layer=0, selected=false, drawVertexMarker=false) at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgsrenderer.cpp:104
#21 0x00007f75f1df206c in QgsVectorLayerRenderer::drawRendererLevels(QgsFeatureIterator&) (this=0x103418160, fit=...)
    at /home/webmaster/dev/cpp/QGIS/src/core/qgsvectorlayerrenderer.cpp:453
#22 0x00007f75f1df096c in QgsVectorLayerRenderer::render() (this=0x103418160) at /home/webmaster/dev/cpp/QGIS/src/core/qgsvectorlayerrenderer.cpp:248
#23 0x00007f75f1bee5ae in QgsMapRendererCustomPainterJob::doRender() (this=0x10341a890) at /home/webmaster/dev/cpp/QGIS/src/core/qgsmaprenderercustompainterjob.cpp:265
#24 0x00007f75f1bee1ee in QgsMapRendererCustomPainterJob::staticRender(QgsMapRendererCustomPainterJob*) (self=0x10341a890)
    at /home/webmaster/dev/cpp/QGIS/src/core/qgsmaprenderercustompainterjob.cpp:216
#25 0x00007f75f1bf0f89 in QtConcurrent::StoredFunctorCall1<void, void (*)(QgsMapRendererCustomPainterJob*), QgsMapRendererCustomPainterJob*>::runFunctor() (this=0x1033dd660)
    at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentstoredfunctioncall.h:432
#26 0x00007f75f1bef69b in QtConcurrent::RunFunctionTask<void>::run() (this=0x1033dd660) at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentrunbase.h:136
#27 0x00007f75efe74581 in () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#28 0x00007f75efe7829d in () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#29 0x00007f75e79e274a in start_thread (arg=0x7f752a09b700) at pthread_create.c:456

Associated revisions

Revision a6eea720 - 2017-10-31 01:24 AM - Nyall Dawson

Fix crashes caused by concurrent rendering of cached QPictures from QgsSvgCache

QgsSvgCache::svgAsPicture was rendering an implicitly shared copy when
the picture had already been cached. It turns out that rendering an
implicitly shared QPicture copy isn't thread safe, and rendering shared
copies simulataneously across different threads leads quickly to a crash.

Accordingly we always detach the QPicture objects returned by
svgAsPicture, so that the returned QPicture is safe to use across threads.

Also add unit tests for this, and a similar unit test to verify that

rendering of QImage based cached copies does **not** suffer the same
issue.

Fixes #17089, #17077

History

#1 - 2017-08-30 10:25 AM - Mathieu Pellerin - nIRV

I've been able to duplicate this both on my ubuntu as well as windows machines.

#2 - 2017-08-30 10:26 AM - Giovanni Manghi

- Crashes QGIS or corrupts data changed from No to Yes

regression?

#3 - 2017-08-30 12:48 PM - Nyall Dawson

I'm fairly certain I've seen a similar crash in 2.18

#4 - 2017-09-04 05:15 AM - Mathieu Pellerin - nIRV

Nyall, I've tested this project with QGIS 2.18, and I failed to get it to crash. It might be that the underlying issue is exposed by the composer map item's improved rendering mode under master. Nevertheless, I'm inclined to mark it as a regression. OK with that?

#5 - 2017-09-04 12:26 PM - Giovanni Manghi

- Regression? changed from No to Yes

#6 - 2017-10-30 11:47 AM - Nyall Dawson

- Assignee set to Nyall Dawson

#7 - 2017-10-31 01:55 AM - Nyall Dawson

PR at https://github.com/qgis/QGIS/pull/5497

#8 - 2017-10-31 07:21 PM - Nyall Dawson

- % Done changed from 0 to 100

- Status changed from Open to Closed

Applied in changeset commit:qgis|a6eea7205c72a1be837ab43b79aad0c67a92a9b2.

Files

crash_freeze.zip	761 KB	2017-08-30	Mathieu Pellerin - nIRV