QGIS Application - Bug report #17077
QGIS Crashes when using SVG marker for point layer in map units or with rotation

2017-08-26 12:19 AM - Olcay Ebcin

Status:	Closed		
Priority:	High		
Assignee:	Nyall Dawson		
Category:	Symbology		
Affected QGIS version:	2.18.12	**Regression?:**	Yes
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	24976

Description

Have more than 5000 point features and show it as SVG marker.

Give any rotation angle. (ie 45 degree)
make some Zoom in and Zoom out, then Ooops Oh! Uh!, QGIS's gone :(

Keep SVG markers in MapUnit.
make zoom in and zoom out, then again Ooops Oh! Uh!, QGIS's gone again :(

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 - 2017-08-26 05:38 AM - Nyall Dawson

- Assignee deleted (Nyall Dawson)

#2 - 2017-08-27 05:12 PM - Giovanni Manghi

- File points.zip added
- Subject changed from SVG marker in MapUnit or give Rotation angle in QGIS 3.0 to QGIS Crashes when using SVG marker fpr point layer in MapUnit or with rotation angle
- Affected QGIS version changed from master to 2.18.12
- Regression? changed from No to Yes

This also affects 2.18.12 but not 2.14, regression. Layer attached.

#3 - 2017-08-27 05:13 PM - Giovanni Manghi

- Subject changed from QGIS Crashes when using SVG marker fpr point layer in MapUnit or with rotation angle to QGIS Crashes when using SVG marker for point layer in map units or with rotation

#4 - 2017-09-22 10:29 AM - Alessandro Pasotti

- Assignee set to Alessandro Pasotti

#5 - 2017-09-22 10:51 AM - Alessandro Pasotti

- File stacktrace.txt added

- Assignee deleted (Alessandro Pasotti)

Confirmed on latest 2.18.
The debugger does not produce any meaningful information (at least for me) but I attach the stacktrace.

Master looks fine.

#6 - 2017-09-22 01:13 PM - Alessandro Pasotti

- File stacktrace2.txt added

Now crashing in a different place:
src/core/qgsvectorlayerrenderer.cpp: 291: (drawRendererV2) [0ms] [thread:0x7fff0000b3d0] Drawing of vector layer points20170922130742064 cancelled.
src/core/qgsmaprendererparalleljob.cpp: 279: (renderLayerStatic) [0ms] [thread:0x7fff0000b3d0] job e66b450 end [29 ms] (layer points20170922130742064)

- Error in `/home/ale/dev/QGIS/build-local/output/bin/qgis': malloc(): smallbin double linked list corrupted: 0x000000000a8634e0 ***

See attached stacktrace2.txt

#7 - 2017-09-25 11:33 AM - Alessandro Pasotti

I can confirm that it only happens when multi-threaded rendering options is ON (confirmed on Windows that it's the most easy to crash).

#8 - 2017-10-30 11:47 AM - Nyall Dawson

- Assignee set to Nyall Dawson

#9 - 2017-10-31 01:55 AM - Nyall Dawson

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

#10 - 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

points.zip	191 KB	2017-08-27	Giovanni Manghi
stacktrace.txt	120 KB	2017-09-22	Alessandro Pasotti
stacktrace2.txt	143 KB	2017-09-22	Alessandro Pasotti