QGIS Application - Bug report #18996
QGIS crash when SVG for styling is not available

2018-05-21 05:42 PM - Saber Razmjooei

Status:	Closed		
Priority:	High		
Assignee:			
Category:	Symbology		
Affected QGIS version:	3.1(master)	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	
Crashes QGIS or corrupts data:	No	**Copied to github as #:**	26827

Description

I seem to remember there was a similar issue in the past: #10153.

The missing SVGs are rendered as question marks (?) in QGIS 2.x but in QGIS master, it causes core dump.

Associated revisions

Revision 75b7edf1 - 2018-06-01 10:00 PM - Even Rouault

QgsSvgCache::svgAsPicture(): make sure the returned picture is not shared (fixes #18996)

For some reason QPicture.detach() doesn't seem to always work as intended, at
least with QT 5.5 on Ubuntu 16.04
Serialization/deserialization is a safe way to be ensured we don't
share a copy.

Relates to a6eea7205c72a1be837ab43b79aad0c67a92a9b2

Revision 2ed200a8 - 2018-06-01 10:33 PM - Even Rouault

Merge pull request #7142 from rouault/fix_18996

QgsSvgCache::svgAsPicture(): make sure the returned picture is not shared (fixes #18996)

History

#1 - 2018-05-22 03:56 AM - Nyall Dawson

- Status changed from Open to Feedback

Works OK here - maybe it's specific to a certain fill/marker type? Can you share a project?

#2 - 2018-05-22 03:55 PM - Saber Razmjooei

- Status changed from Feedback to Open

Here is the gpkg file:
https://www.dropbox.com/s/5c3uk8sea31bta2/test.gpkg?dl=0

and the project file:
https://www.dropbox.com/s/8tnigxaxc0mfrtb/no_svg.qgs?dl=0

#3 - 2018-05-23 03:01 AM - Nyall Dawson

- Status changed from Open to Feedback

Can't reproduce - works fine here (windows)

#4 - 2018-05-23 04:30 PM - Saber Razmjooei

- Status changed from Feedback to Open

Did you try to zoom in/out several times?

#5 - 2018-05-24 12:09 AM - Nyall Dawson

Yep, zoom in and out and no crash. Can you get a trace?

#6 - 2018-05-29 10:13 AM - Saber Razmjooei

Here is the debug info:

```
Starting program: /usr/local/src/QGIS_master/build/output/bin/qgis
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[New Thread 0x7fffd6b00700 (LWP 32637)]
[New Thread 0x7fffd2cdf700 (LWP 32638)]
[New Thread 0x7fffc54d2700 (LWP 32639)]
[New Thread 0x7fffb42f6700 (LWP 32641)]
[New Thread 0x7fffb38e5700 (LWP 32642)]
Warning: QSqlQuery::prepare: database not open
Warning: QSqlDatabasePrivate::addDatabase: duplicate connection name 'userprofile', old connection removed.
Warning: QSqlQuery::prepare: database not open
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
```

Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: !!! prefix path was requested, but it is not valid - we do not run from installed path !!!
[New Thread 0x7fff55598700 (LWP 32650)]
[New Thread 0x7fff4f9fd700 (LWP 32652)]
rendering stop!
rendering stop!
rendering stop!
Warning: QPicture::play: Invalid command 255
Warning: QBuffer::seek: Invalid pos: -14090218
Warning: QPicture::play: Invalid command 240
Warning: QPicture::play: Invalid command 240
Warning: QPicture::play: Invalid command 240
Warning: QPicture::play: Invalid command 240
Warning: QPicture::play: Invalid command 240
Warning: QPicture::play: Invalid command 71
Warning: QPicture::play: Invalid command 115

Thread 7 "Thread (pooled)" received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0x7fff55598700 (LWP 32650)]
0x00007ffff4dc8306 in ?? () from /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5

#7 - 2018-05-29 10:54 AM - Nyall Dawson

- Status changed from Open to Feedback

That's not a full trace - it doesn't help unfortunately.

#8 - 2018-05-29 11:53 AM - Saber Razmjooei

How about this:

Starting program: /usr/local/src/QGIS_master/build/output/bin/qgis
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[New Thread 0x7fffd6b00700 (LWP 3199)]
[New Thread 0x7fffd2cdf700 (LWP 3200)]
[New Thread 0x7fffc54d2700 (LWP 3201)]
[New Thread 0x7fffb42f6700 (LWP 3202)]
[New Thread 0x7fffb38e5700 (LWP 3203)]
Warning: QSqlQuery::prepare: database not open
Warning: QSqlDatabasePrivate::addDatabase: duplicate connection name 'userprofile', old connection removed.
Warning: QSqlQuery::prepare: database not open
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile

Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: libpng warning: iCCP: known incorrect sRGB profile
Warning: !!! prefix path was requested, but it is not valid - we do not run from installed path !!!
[New Thread 0x7fff55598700 (LWP 3212)]
Warning: QPicture::play: Invalid command 255
Warning: QBuffer::seek: Invalid pos: -14090218
Warning: QPicture::play: Invalid command 240
Warning: QPicture::play: Invalid command 240
Warning: QPicture::play: Invalid command 240
Warning: QPicture::play: Invalid command 240
Warning: QPicture::play: Invalid command 240
Warning: QPicture::play: Invalid command 71
Warning: QPicture::play: Invalid command 115
[New Thread 0x7fff4f977700 (LWP 3219)]

Thread 7 "Thread (pooled)" received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0x7fff55598700 (LWP 3212)]
0x00007ffff4dc8306 in ?? () from /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
(gdb)
(gdb) bt full
#0 0x00007ffff4dc8306 in () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#1 0x00007ffff4e426bd in () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#2 0x00007ffff4c0262b in QPicture::exec(QPainter*, QDataStream&, int) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#3 0x00007ffff4c04379 in QPicture::play(QPainter*) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#4 0x00007ffff4e0da92 in QPainter::drawPicture(QPointF const&, QPicture const&) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#5 0x00007ffff5e21fda in QgsSVGFillSymbolLayer::applyPattern(QBrush&, QString const&, double, QgsUnitTypes::RenderUnit, QColor const&,
QColor const&, double, QgsUnitTypes::RenderUnit, QgsSymbolRenderContext const&, QgsMapUnitScale const&, QgsMapUnitScale const&) ()
at /usr/local/src/QGIS_master/build/output/lib/libqgis_core.so.3.1.0
#6 0x00007ffff5e22296 in QgsSVGFillSymbolLayer::startRender(QgsSymbolRenderContext&) () at
/usr/local/src/QGIS_master/build/output/lib/libqgis_core.so.3.1.0
#7 0x00007ffff5f07042 in QgsSymbol::startRender(QgsRenderContext&, QgsFields const&) () at
/usr/local/src/QGIS_master/build/output/lib/libqgis_core.so.3.1.0
#8 0x00007ffff5de09ef in QgsCategorizedSymbolRenderer::startRender(QgsRenderContext&, QgsFields const&) () at
/usr/local/src/QGIS_master/build/output/lib/libqgis_core.so.3.1.0
#9 0x00007ffff644ef6e in QgsVectorLayerRenderer::render() () at /usr/local/src/QGIS_master/build/output/lib/libqgis_core.so.3.1.0
#10 0x00007ffff6240b62 in QgsMapRendererCustomPainterJob::doRender() () at
/usr/local/src/QGIS_master/build/output/lib/libqgis_core.so.3.1.0
#11 0x00007ffff62409ca in QgsMapRendererCustomPainterJob::staticRender(QgsMapRendererCustomPainterJob*) () at
/usr/local/src/QGIS_master/build/output/lib/libqgis_core.so.3.1.0
#12 0x00007ffff6243267 in QtConcurrent::StoredFunctorCall1<void, void (*)(QgsMapRendererCustomPainterJob*),
QgsMapRendererCustomPainterJob*>::runFunctor() ()
    at /usr/local/src/QGIS_master/build/output/lib/libqgis_core.so.3.1.0
#13 0x00007ffff624194d in QtConcurrent::RunFunctionTask<void>::run() () at /usr/local/src/QGIS_master/build/output/lib/libqgis_core.so.3.1.0
#14 0x00007ffff43ea2a2 in () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#15 0x00007ffff43ed16d in () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5

#16 0x00007fffe97936db in start_thread (arg=0x7fff55598700) at pthread_create.c:463
pd = 0x7fff55598700
now = <optimised out>
unwind_buf =
{cancel_jmp_buf = {{jmp_buf = {140734625318656, 408835854063029335, 140734625316288, 0, 93825065674880, 140737488339424, -409035119007970217, -408797352122725289}, mask_was_saved = 0}}, priv = {pad = {0x0, 0x0, 0x0, 0x0}, data = {prev = 0x0, cleanup = 0x0, canceltype = 0}}}
not_first_call = <optimised out>
#17 0x00007ffff3acb88f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95
(gdb)

#9 - 2018-05-29 11:55 AM - Saber Razmjooei

- Status changed from Feedback to Open

#10 - 2018-06-01 04:24 PM - Even Rouault

I could reliably reproduce on Ubuntu 16.04 with the same stacktrace. The issue is linked to multi-threading rendering of non cached SVG symbol. I've created https://github.com/qgis/QGIS/pull/7142 with a proposed fix.

#11 - 2018-06-01 10:33 PM - Even Rouault

- Status changed from Open to Closed

- % Done changed from 0 to 100

Applied in changeset commit:qgis|75b7edf1d211cd136fb54d2216cfea6e9fd2e120.

#12 - 2018-06-04 11:15 AM - Saber Razmjooei

Thanks @Even...works well now.