UNKNOWN WRITE · qpaintengineex_lineTo

REDO TASK

OVERVIEW

Crash State: qpaintengineex_lineTo
QStroker::joinPoints
QStroker::processCurrentSubpath

Crash Type: UNKNOWN WRITE
Created: Fri, Nov 3, 2023, 4:30 PM
Security: **YES**

Crash Address: 0x40020000
Sanitizer: address (ASAN)
Reliably Reproduces: YES

Issue: 63847
Platform: linux

Fuzzing Engine: libFuzzer
Fuzz Target: qtsvg_svg_qsvgrenderer_render
Job Type: libfu

Project: qt

Fixed: **NO**

Minimized Testcase: (80 KB)

Unminimized Testcase: (80 KB)
Re-upload Testcase:
Build:

REPRODUCE BUG

See https://code.qt.io/cgit/qt/qtbase.git/plain/tests/libfuzzer/README for instructions to reproduce this bug locally.

LAST TESTED REVISION	REGRESSION REVISION RANGE
Qtsvg: 3117386a4008f5d575d7910f130fba66c740d202	Qt: 3c38cc22ce504b221939a1cfa1e37db58010e749:83b4afd584b6

CRASH STACKTRACE

LAST TESTED STACKTRACE ON **REVISION 3117386A4008F5D575D7910F130FBA66C740D202** (77 LINES)

```
1 [Environment] ASAN_OPTIONS=allocator_may_return_null=1
2 +---------------------------------------Release Build Stacktrace---------------------------------------+
3 Command: /mnt/scratch0/clusterfuzz/resources/platform/linux/unshare -c -n /mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-b
  7180779f82d872a3188b91bfa329c/revisions/qtsvg_svg_qsvgrenderer_render -rss_limit_mb=2560 -timeout=60 -runs=100 /mnt/scratch0
  uzzer-testcases/crash-15ff6ffdf6a267eee002b0d520b03eb3dd3becc5
4 Time ran: 30.5939998626709
5
6 INFO: Running with entropic power schedule (0xFF, 100).
7 INFO: Seed: 4149591106
8 INFO: Loaded 1 modules   (426239 inline 8-bit counters): 426239 [0xba53480, 0xbabb57f),
9 INFO: Loaded 1 PC tables (426239 PCs): 426239 [0xbabb580,0xbdfbd78),
10 /mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/revisions/qtsvg_svg
  ning 1 inputs 100 time(s) each.
11 Running: /mnt/scratch0/clusterfuzz/bot/inputs/fuzzer-testcases/crash-15ff6ffdf6a267eee002b0d520b03eb3dd3becc5
12 AddressSanitizer:DEADLYSIGNAL
13 ================================================================
14 ==2162==ERROR: AddressSanitizer: SEGV on unknown address 0x40020000 (pc 0x09c5ad3a bp 0xffba2638 sp 0xffba2600 T0)
15 ==2162==The signal is caused by a WRITE memory access.
16     #0 0x9c5ad3a in add /src/qt/qtbase/src/gui/painting/qdatabuffer_p.h:66:21
17     #1 0x9c5ad3a in qpaintengineex_lineTo(double, double, void*) /src/qt/qtbase/src/gui/painting/qpaintengineex.cpp:312:35
18     #2 0x9e3c9b9 in QStroker::joinPoints(double, double, QLineF const&, QStroker::LineJoinMode) /src/qt/qtbase/src/gui/paint
19     #3 0x9e334cb in QStroker::processCurrentSubpath() /src/qt/qtbase/src/gui/painting/qstroker.cpp:394:9
20     #4 0x9e43692 in moveTo /src/qt/qtbase/src/gui/painting/qstroker_p.h:286:9
21     #5 0x9e43692 in qdashstroker_moveTo(double, double, void*) /src/qt/qtbase/src/gui/painting/qstroker.cpp:965:26
22     #6 0x9e46e25 in emitMoveTo /src/qt/qtbase/src/gui/painting/qstroker_p.h:268:5
23     #7 0x9e46e25 in QDashStroker::processCurrentSubpath() /src/qt/qtbase/src/gui/painting/qstroker.cpp:1222:25
24     #8 0x9e48e95 in end /src/qt/qtbase/src/gui/painting/qstroker.cpp:185:9
25     #9 0x9e48e95 in QDashStroker::end() /src/qt/qtbase/src/gui/painting/qstroker_p.h:362:18
26     #10 0x9c56bdc in QPaintEngineEx::stroke(QVectorPath const&, QPen const&) /src/qt/qtbase/src/gui/painting/qpaintengineex.
27     #11 0x9c000e5 in QRasterPaintEngine::stroke(QVectorPath const&, QPen const&) /src/qt/qtbase/src/gui/painting/qpaintengin
28     #12 0x9c5ef9e in QPaintEngineEx::draw(QVectorPath const&) /src/qt/qtbase/src/gui/painting/qpaintengineex.cpp:596:9
29     #13 0x9c65dab in QPaintEngineEx::drawPath(QPainterPath const&) /src/qt/qtbase/src/gui/painting/qpaintengineex.cpp:835:9
```

```
    #14 0x9c82d6e in QPainter::drawPath(QPainterPath const&) /src/qt/qtbase/src/gui/painting/qpainter.cpp:0
    #15 0x90e4e53 in QSvgPath::drawCommand(QPainter*, QSvgExtraStates&) /src/qt/qtsvg/src/svg/qsvggraphics.cpp:112:8
    #16 0x908acf0 in QSvgNode::fillThenStroke(QPainter*, QSvgExtraStates&) /src/qt/qtsvg/src/svg/qsvgnode.cpp:101:9
    #17 0x9087c90 in QSvgNode::draw(QPainter*, QSvgExtraStates&) /src/qt/qtsvg/src/svg/qsvgnode.cpp:71:17
    #18 0x8f8a66a in QSvgTinyDocument::draw(QPainter*, QRectF const&) /src/qt/qtsvg/src/svg/qsvgtinydocument.cpp:258:19
    #19 0x8f8f83a in QSvgTinyDocument::draw(QPainter*) /src/qt/qtsvg/src/svg/qsvgtinydocument.cpp:406:5
    #20 0x8f80c22 in QSvgRenderer::render(QPainter*) /src/qt/qtsvg/src/svg/qsvgrenderer.cpp:456:20
    #21 0x81af958 in LLVMFuzzerTestOneInput /src/qt/qtsvg/tests/libfuzzer/svg/qsvgrenderer/render/main.cpp:24:14
    #22 0x80b727e in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned int) /src/llvm-project/compiler-rt/lib/f
15
    #23 0x80a24de in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned int) /src/llvm-project/compiler-rt/lib/fuzzer
    #24 0x80a80e0 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned int)) /src/llvm-project/comp
Driver.cpp:860:9
    #25 0x80d0a67 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #26 0xf7c4eed4 in __libc_start_main
    #27 0x80999a5 in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3
tsvg_svg_qsvgrenderer_render+0x9c5ad3a)
==2162==ABORTING


+---------------------------------------Release Build Unsymbolized Stacktrace (diff)---------------------------------------

==2162==ERROR: AddressSanitizer: SEGV on unknown address 0x40020000 (pc 0x09c5ad3a bp 0xffba2638 sp 0xffba2600 T0)
==2162==The signal is caused by a WRITE memory access.
    #0 0x9c5ad3a  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
enderer_render+0x9c5ad3a)
    #1 0x9e3c9b9  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
enderer_render+0x9e3c9b9)
    #2 0x9e334cb  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
enderer_render+0x9e334cb)
    #3 0x9e43692  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
enderer_render+0x9e43692)
    #4 0x9e46e25  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
enderer_render+0x9e46e25)
    #5 0x9e48e95  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
enderer_render+0x9e48e95)
    #6 0x9c56bdc  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
enderer_render+0x9c56bdc)
    #7 0x9c000e5  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
enderer_render+0x9c000e5)
    #8 0x9c5ef9e  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
enderer_render+0x9c5ef9e)
    #9 0x9c65dab  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
enderer_render+0x9c65dab)
    #10 0x9c82d6e  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
renderer_render+0x9c82d6e)
    #11 0x90e4e53  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
renderer_render+0x90e4e53)
    #12 0x908acf0  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
renderer_render+0x908acf0)
    #13 0x9087c90  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
renderer_render+0x9087c90)
    #14 0x8f8a66a  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
renderer_render+0x8f8a66a)
    #15 0x8f8f83a  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
renderer_render+0x8f8f83a)
    #16 0x8f80c22  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
renderer_render+0x8f80c22)
    #17 0x81af958  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
renderer_render+0x81af958)
    #18 0x80b727e  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
renderer_render+0x80b727e)
```

```
    #19 0x80a24de  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c renderer_render+0x80a24de)
    #20 0x80a80e0  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c renderer_render+0x80a80e0)
    #21 0x80d0a67  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c renderer_render+0x80d0a67)
    #22 0xf7c4eed4  (/lib32/libc.so.6+0x1aed4) (BuildId: 8c11d7b4ac6d685f0bba1cf2506a80f64d314582)
    #23 0x80999a5  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c renderer_render+0x80999a5)
```

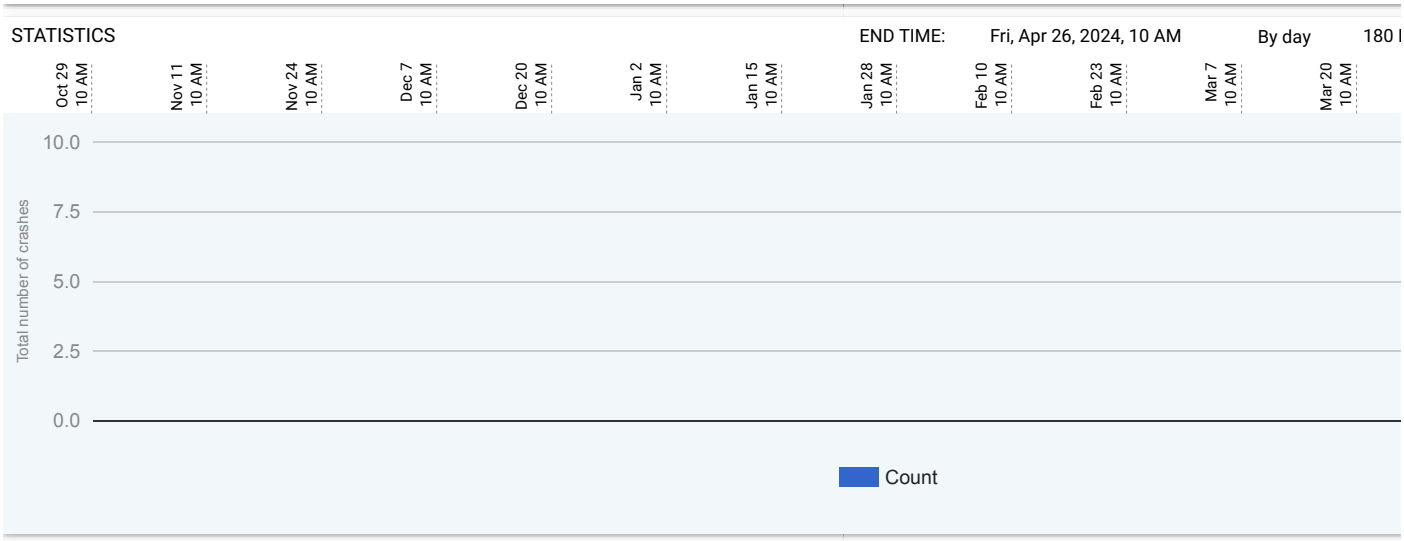
ORIGINAL STACKTRACE ON **REVISION 59962414B7D77EAEA1CEC5AA7FBD9E011C107FC9** (74 LINES)

```
[Environment] ASAN_OPTIONS=allocator_may_return_null=1:dedup_token_length=3:symbolize=1
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /mnt/scratch0/clusterfuzz/resources/platform/linux/unshare -c -n /mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-b
7180779f82d872a3188b91bfa329c/revisions/qtsvg_svg_qsvgrenderer_render -rss_limit_mb=2560 -timeout=60 -runs=100 /mnt/scratch0
uzzer-testcases/crash-15ff6ffdf6a267eee002b0d520b03eb3dd3becc5
Time ran: 28.31761646270752

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4166657522
INFO: Loaded 1 modules   (415154 inline 8-bit counters): 415154 [0xb619330, 0xb67e8e2),
INFO: Loaded 1 PC tables (415154 PCs): 415154 [0xb67e8e4,0xb9a9674),
/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/revisions/qtsvg_svg
ning 1 inputs 100 time(s) each.
Running: /mnt/scratch0/clusterfuzz/bot/inputs/fuzzer-testcases/crash-15ff6ffdf6a267eee002b0d520b03eb3dd3becc5
AddressSanitizer:DEADLYSIGNAL
=================================================================
==7379==ERROR: AddressSanitizer: SEGV on unknown address 0x40020000 (pc 0x09956602 bp 0xff88ba18 sp 0xff88b9e0 T0)
==7379==The signal is caused by a WRITE memory access.
SCARINESS: 30 (wild-addr-write)
    #0 0x9956602 in add /src/qt/qtbase/src/gui/painting/qdatabuffer_p.h:66:21
    #1 0x9956602 in qpaintengineex_lineTo(double, double, void*) /src/qt/qtbase/src/gui/painting/qpaintengineex.cpp:312:35
    #2 0x9b162c3 in QStroker::joinPoints(double, double, QLineF const&, QStroker::LineJoinMode) /src/qt/qtbase/src/gui/paint
    #3 0x9b0d3fa in QStroker::processCurrentSubpath() /src/qt/qtbase/src/gui/painting/qstroker.cpp:394:9
    #4 0x9b1cf5a in moveTo /src/qt/qtbase/src/gui/painting/qstroker_p.h:286:9
    #5 0x9b1cf5a in qdashstroker_moveTo(double, double, void*) /src/qt/qtbase/src/gui/painting/qstroker.cpp:965:26
    #6 0x9b2037b in emitMoveTo /src/qt/qtbase/src/gui/painting/qstroker_p.h:268:5
    #7 0x9b2037b in QDashStroker::processCurrentSubpath() /src/qt/qtbase/src/gui/painting/qstroker.cpp:1222:25
    #8 0x9b2230d in end /src/qt/qtbase/src/gui/painting/qstroker.cpp:185:9
    #9 0x9b2230d in QDashStroker::end() /src/qt/qtbase/src/gui/painting/qstroker_p.h:362:18
    #10 0x9952517 in QPaintEngineEx::stroke(QVectorPath const&, QPen const&) /src/qt/qtbase/src/gui/painting/qpaintengineex.
    #11 0x98ffd4b in QRasterPaintEngine::stroke(QVectorPath const&, QPen const&) /src/qt/qtbase/src/gui/painting/qpaintengin
    #12 0x995a5e1 in QPaintEngineEx::draw(QVectorPath const&) /src/qt/qtbase/src/gui/painting/qpaintengineex.cpp:596:9
    #13 0x9960e5b in QPaintEngineEx::drawPath(QPainterPath const&) /src/qt/qtbase/src/gui/painting/qpaintengineex.cpp:835:9
    #14 0x997ccdd in QPainter::drawPath(QPainterPath const&) /src/qt/qtbase/src/gui/painting/qpainter.cpp:0
    #15 0x9509471 in QSvgPath::draw(QPainter*, QSvgExtraStates&) /src/qt/qtsvg/src/svg/qsvggraphics.cpp:173:9
    #16 0x941a2ae in QSvgTinyDocument::draw(QPainter*, QRectF const&) /src/qt/qtsvg/src/svg/qsvgtinydocument.cpp:249:19
    #17 0x941ee5d in QSvgTinyDocument::draw(QPainter*) /src/qt/qtsvg/src/svg/qsvgtinydocument.cpp:398:5
    #18 0x94111da in QSvgRenderer::render(QPainter*) /src/qt/qtsvg/src/svg/qsvgrenderer.cpp:407:20
    #19 0x81adde8 in LLVMFuzzerTestOneInput /src/qt/qtsvg/tests/libfuzzer/svg/qsvgrenderer/render/main.cpp:24:14
    #20 0x80b570e in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned int) /src/llvm-project/compiler-rt/lib/f
15
    #21 0x80a096e in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned int) /src/llvm-project/compiler-rt/lib/fuzzer
    #22 0x80a6570 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned int)) /src/llvm-project/comp
Driver.cpp:860:9
    #23 0x80ceef7 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #24 0xf7c4fed4 in __libc_start_main
    #25 0x8097e35 in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3
tsvg_svg_qsvgrenderer_render+0x9956602)
==7379==ABORTING
```

```
47
48
49 +----------------------------------------Release Build Unsymbolized Stacktrace (diff)----------------------------------------
50
51 ==7379==The signal is caused by a WRITE memory access.
52 SCARINESS: 30 (wild-addr-write)
53     #0 0x9956602  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
   enderer_render+0x9956602)
54     #1 0x9b162c3  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
   enderer_render+0x9b162c3)
55     #2 0x9b0d3fa  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
   enderer_render+0x9b0d3fa)
56     #3 0x9b1cf5a  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
   enderer_render+0x9b1cf5a)
57     #4 0x9b2037b  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
   enderer_render+0x9b2037b)
58     #5 0x9b2230d  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
   enderer_render+0x9b2230d)
59     #6 0x9952517  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
   enderer_render+0x9952517)
60     #7 0x98ffd4b  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
   enderer_render+0x98ffd4b)
61     #8 0x995a5e1  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
   enderer_render+0x995a5e1)
62     #9 0x9960e5b  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c/
   enderer_render+0x9960e5b)
63     #10 0x997ccdd  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x997ccdd)
64     #11 0x9509471  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x9509471)
65     #12 0x941a2ae  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x941a2ae)
66     #13 0x941ee5d  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x941ee5d)
67     #14 0x94111da  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x94111da)
68     #15 0x81adde8  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x81adde8)
69     #16 0x80b570e  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x80b570e)
70     #17 0x80a096e  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x80a096e)
71     #18 0x80a6570  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x80a6570)
72     #19 0x80ceef7  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x80ceef7)
73     #20 0xf7c4fed4  (/lib32/libc.so.6+0x1aed4) (BuildId: 8c11d7b4ac6d685f0bba1cf2506a80f64d314582)
74     #21 0x8097e35  (/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-i386_qt_dd046324bcb7180779f82d872a3188b91bfa329c
   renderer_render+0x8097e35)
```



TESTCASE ANALYSIS ON OTHER JOBS

JOB NAME	STATUS	REVISION	CRASH TYPE	CRASH STATE	SECURITY	SI
libfuzzer_asan_qt	Reproducible	202311030611	Out-of-memory	qtsvg_svg_qsvgrenderer_render	false	fal
libfuzzer_ubsan_qt	Reproducible	202311030611	Out-of-memory	qtsvg_svg_qsvgrenderer_render	false	fal

METADATA

[2023-11-03 23:30:03 UTC] oss-fuzz-linux-zone1-host-snxl-2: Fuzz task : Fuzzer libFuzzer_qt_qtsvg_svg_qsvgrenderer_render generated testcase crashed in 4170
[2023-11-04 00:47:35 UTC] oss-fuzz-linux-zone7-host-qhr7-9: Minimize task started.
[2023-11-04 01:49:44 UTC] oss-fuzz-linux-zone7-host-qhr7-9: Minimize task errored out: LibFuzzer minimization failed.
[2023-11-04 02:42:44 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task started.
[2023-11-04 02:44:52 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202311020603.
[2023-11-04 02:45:37 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202311010629.
[2023-11-04 02:46:25 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202310310619.
[2023-11-04 02:47:15 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202203110600 (current range 202004160344:20231103061
[2023-11-04 02:48:01 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202103130609 (current range 202004160344:20220311060
[2023-11-04 02:52:35 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202108230609 (current range 202103130609:20220311060
[2023-11-04 03:03:40 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202111210601 (current range 202108230609:20220311060
[2023-11-04 03:04:25 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202109280605 (current range 202108230609:20211121060
[2023-11-04 03:15:34 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202110220600 (current range 202109280605:20211121060
[2023-11-04 03:26:43 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202111010602 (current range 202110220600:20211121060
[2023-11-04 03:37:52 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202111060605 (current range 202111010602:20211121060
[2023-11-04 03:49:01 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202111080609 (current range 202111060605:20211121060
[2023-11-04 04:00:10 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202111090609 (current range 202111080609:20211121060
[2023-11-04 04:11:20 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202111100600 (current range 202111090609:20211121060
[2023-11-04 04:22:30 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202111080609.
[2023-11-04 04:33:39 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task in-progress: Testing r202110310603.
[2023-11-04 04:44:48 UTC] oss-fuzz-linux-zone5-host-r8xb-14: Regression task finished: regressed in range 202111100600:202111210601.
[2024-04-26 07:35:31 UTC] oss-fuzz-linux-zone8-host-rcp6-14: Progression task started.
[2024-04-26 07:37:18 UTC] oss-fuzz-linux-zone8-host-rcp6-14: Progression task finished: Still crashes on latest revision r202404260610.