QGIS Application - Bug report #14260
Crash on exit

2016-02-09 06:43 AM - Sandro Santilli

Status:	Closed		
Priority:	Severe/Regression		
Assignee:			
Category:	Unknown		
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	invalid
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	22256

Description

To reproduce:

1. Open qgis
2. Close qgis

Backtrace:

```
(gdb) bt
#0  0x00007f7c55d85441 in QBrush::~QBrush() () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#1  0x00007f7c56e65138 in QgsSimpleMarkerSymbolLayerV2::~QgsSimpleMarkerSymbolLayerV2 (this=0x2aa2f50,
__in_chrg=<optimized out>)
    at /usr/src/qgis/qgis-master/src/core/symbology-ng/qgsmarkersymbollayerv2.h:34
#2  0x00007f7c56e651f2 in QgsSimpleMarkerSymbolLayerV2::~QgsSimpleMarkerSymbolLayerV2 (this=0x2aa2f50,
__in_chrg=<optimized out>)
    at /usr/src/qgis/qgis-master/src/core/symbology-ng/qgsmarkersymbollayerv2.h:34
#3  0x00007f7c56eca45b in qDeleteAll<QList<QgsSymbolLayerV2*>::const_iterator> (begin=..., end=...) at
/usr/include/qt4/QtCore/qalgorithms.h:322
#4  0x00007f7c56ec9ea1 in qDeleteAll<QList<QgsSymbolLayerV2*> > (c=...) at /usr/include/qt4/QtCore/qalgorithms.h:330
#5  0x00007f7c56ebf09e in QgsSymbolV2::~QgsSymbolV2 (this=0x7f7bbd039440
<QgsCategorizedSymbolRendererV2::sSkipRender>, __in_chrg=<optimized out>)
    at /usr/src/qgis/qgis-master/src/core/symbology-ng/qgssymbolv2.cpp:241
#6  0x00007f7c56eca5c0 in QgsMarkerSymbolV2::~QgsMarkerSymbolV2 (this=0x7f7bbd039440
<QgsCategorizedSymbolRendererV2::sSkipRender>,
    __in_chrg=<optimized out>) at /usr/src/qgis/qgis-master/src/core/symbology-ng/qgssymbolv2.h:415
#7  0x00007f7c55208259 in __run_exit_handlers (status=0, listp=0x7f7c5558a6c8 <__exit_funcs>,
run_list_atexit=run_list_atexit@entry=true)
    at exit.c:82
#8  0x00007f7c552082a5 in __GI_exit (status=<optimized out>) at exit.c:104
#9  0x00007f7c551edecc in __libc_start_main (main=0x405aa7 <main(int, char**)>, argc=1, argv=0x7fff3208f0e8,
init=<optimized out>,
    fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fff3208f0d8) at libc-start.c:321
#10 0x00000000004051a9 in _start ()
```

Tested with commit:ded1ebb33b4f8a44d6080f02e87144b2d69756e8

History

#1 - 2016-02-09 06:45 AM - Sandro Santilli

NOTE: I've disabled *all* plugins (including core) and the issue is still reproducible

#2 - 2016-02-09 06:55 AM - Sandro Santilli

Running make check confirms the problem:

> 44% tests passed, 107 tests failed out of 192
>
> Total Test time (real) = 155.69 sec
>
> The following tests FAILED:
>
> 4 - qgis_applicationtest (SEGFAULT)
> 5 - qgis_atlascompositiontest (SEGFAULT)
> 6 - qgis_authcryptotest (SEGFAULT)
> 7 - qgis_authconfigtest (SEGFAULT)
> 8 - qgis_authmanagertest (SEGFAULT)
> 9 - qgis_blendmodestest (SEGFAULT)
> 13 - qgis_composerddtest (SEGFAULT)
> 14 - qgis_composereffectstest (SEGFAULT)
>
> ...

#3 - 2016-02-09 06:58 AM - Sandro Santilli

Valgrind report on the run of output/bin/qgis_applicationtest

```
QPaintDevice: Cannot destroy paint device that is being painted
==11523== Invalid read of size 8
==11523==    at 0x7418439: QBrush::~QBrush() (in /usr/lib/x86_64-linux-gnu/libQtGui.so.4.8.6)
==11523==    by 0x67BA137: QgsSimpleMarkerSymbolLayerV2::~QgsSimpleMarkerSymbolLayerV2() (in
/usr/src/qgis/build/0-master/output/lib/libqgis_core.so.2.13.0)
==11523==    by 0x67BA1F1: QgsSimpleMarkerSymbolLayerV2::~QgsSimpleMarkerSymbolLayerV2() (qgsmarkersymbollayerv2.h:34)
==11523==    by 0x681F45A: void qDeleteAll<QList<QgsSymbolLayerV2*>::const_iterator>(QList<QgsSymbolLayerV2*>::const_iterator,
QList<QgsSymbolLayerV2*>::const_iterator) (qalgorithms.h:322)
==11523==    by 0x681EEA0: void qDeleteAll<QList<QgsSymbolLayerV2*> >(QList<QgsSymbolLayerV2*> const&) (qalgorithms.h:330)
==11523==    by 0x681409D: QgsSymbolV2::~QgsSymbolV2() (qgssymbolv2.cpp:241)
==11523==    by 0x681F5BF: QgsMarkerSymbolV2::~QgsMarkerSymbolV2() (in /usr/src/qgis/build/0-master/output/lib/libqgis_core.so.2.13.0)
==11523==    by 0x8347258: __run_exit_handlers (exit.c:82)
==11523==    by 0x83472A4: exit (exit.c:104)
==11523==    by 0x832CECB: (below main) (libc-start.c:321)
==11523==  Address 0x2b7b6e98 is 8 bytes before a block of size 24 alloc'd
==11523==    at 0x4C2B105: operator new(unsigned long) (vg_replace_malloc.c:327)
==11523==    by 0x69A795E: QgsFields::QgsFields() (qgsfield.cpp:276)
==11523==    by 0x67EED96: QgsSymbolLayerV2::QgsSymbolLayerV2(QgsSymbolV2::SymbolType, bool) (qgssymbollayerv2.cpp:332)
==11523==    by 0x67EFA03: QgsMarkerSymbolLayerV2::QgsMarkerSymbolLayerV2(bool) (qgssymbollayerv2.cpp:498)
==11523==    by 0x2F76718B: QgsSimpleMarkerSymbolLayerV2::QgsSimpleMarkerSymbolLayerV2(QString, QColor, QColor, double, double,
QgsSymbolV2::ScaleMethod) (qgsmarkersymbollayerv2.cpp:51)
==11523==    by 0x2F72BBB1: QgsMarkerSymbolV2::QgsMarkerSymbolV2(QList<QgsSymbolLayerV2*>) (qgssymbolv2.cpp:545)
==11523==    by 0x2F7ADA7C: __static_initialization_and_destruction_0(int, int) (qgscategorizedsymbolrendererv2.cpp:879)
==11523==    by 0x2F7ADADE: _GLOBAL__sub_I_qgscategorizedsymbolrendererv2.cpp (qgscategorizedsymbolrendererv2.cpp:911)
```

```
==11523==    by 0x4010139: call_init.part.0 (dl-init.c:78)
==11523==    by 0x4010222: call_init (dl-init.c:36)
==11523==    by 0x4010222: _dl_init (dl-init.c:126)
==11523==    by 0x4014C6F: dl_open_worker (dl-open.c:577)
==11523==    by 0x400FFF3: _dl_catch_error (dl-error.c:187)
```

#4 - 2016-02-09 08:19 AM - Sandro Santilli

- Resolution set to invalid

- Status changed from Open to Closed

I cannot reproduce with a clean build against commit:b9726d7285733c27d42456c115e28d5a37f3e0be, so closing.

#5 - 2017-09-22 10:05 AM - Jürgen Fischer

- Category set to Unknown