QGIS Application - Bug report #14001
Crash in QGIS Server running without project in CGI mode

2015-12-16 10:00 AM - Alessandro Pasotti

Status:	Closed		
Priority:	Severe/Regression		
Assignee:	Matthias Kuhn		
Category:	Symbology		
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	22015

Description

Recently I've started to see segfaults when qgis server is running in CGI mode.

I couldn't find the source of the problem because running from the console or in the debugger doesn't show the error. Note that the server was running without any loaded project (I was just testing error responses) hence the error is not related to any particular layer or project.

It should be something introduced recently.

Attaching gdb to the cgi process provides this information:

```
(gdb) bt
#0  0x0000000000001c1 in ?? ()
#1  0x00007ff143edfe56 in qDeleteAll<QList<QgsSymbolLayerV2*>::const_iterator> (begin=..., end=...) at
/usr/include/qt4/QtCore/qalgorithms.h:322
#2  0x00007ff143ede9f8 in qDeleteAll<QList<QgsSymbolLayerV2*> > (c=...) at /usr/include/qt4/QtCore/qalgorithms.h:330
#3  0x00007ff143ed2560 in QgsSymbolV2::~QgsSymbolV2 (this=0x7ff1448b7b20
<QgsCategorizedSymbolRendererV2::sSkipRender>, __in_chrg=<optimized out>)
   at /home/ale/dev/QGIS/src/core/symbology-ng/qgssymbolv2.cpp:237
#4  0x00007ff143ee1182 in QgsMarkerSymbolV2::~QgsMarkerSymbolV2 (this=0x7ff1448b7b20
<QgsCategorizedSymbolRendererV2::sSkipRender>, __in_chrg=<optimized out>)
   at /home/ale/dev/QGIS/src/core/symbology-ng/qgssymbolv2.h:381
#5  0x00007ff13fa315ea in __cxa_finalize (d=0x7ff1448b6600) at cxa_finalize.c:56
#6  0x00007ff143ec6fd3 in __do_global_dtors_aux () from /home/ale/apps/lib/libqgis_core.so.2.13.0
#7  0x00007fff5409d2b0 in ?? ()
#8  0x00007ff1448c973a in _dl_fini () at dl-fini.c:252
```

Associated revisions

Revision 036eada9 - 2015-12-25 09:18 AM - Matthias Kuhn

Fix #14001

History

#1 - 2015-12-16 11:05 AM - Nyall Dawson

How recently are we talking here? Any chance you could bisect to the offending commit?

#2 - 2015-12-17 09:09 AM - Alessandro Pasotti

I've done dozens of clean builds going back and I tracked it down to:
Last working commit: 29a3c64
First segfaulting build: 123a60e

I couldn't successfully build the three commits in between the two indicated above, so I can't tell where exactly the problem is.

Updated stacktrace on first segfaulting commit 123a60e:

```
(gdb) bt
#0  0x00000000000001c1 in ?? ()
#1  0x00007efee23c02b8 in qDeleteAll<QList<QgsSymbolLayerV2*>::const_iterator> (begin=..., end=...) at
/usr/include/qt4/QtCore/qalgorithms.h:322
#2  0x00007efee23bed6a in qDeleteAll<QList<QgsSymbolLayerV2*> > (c=...) at /usr/include/qt4/QtCore/qalgorithms.h:330
#3  0x00007efee23b2d7e in QgsSymbolV2::~QgsSymbolV2 (this=0x7efee2d88a60 <QgsCategorizedSymbolRendererV2::sSkipRender>,
__in_chrg=<optimized out>)
   at /home/ale/dev/QGIS/src/core/symbology-ng/qgssymbolv2.cpp:255
#4  0x00007efee23c15fe in QgsMarkerSymbolV2::~QgsMarkerSymbolV2 (this=0x7efee2d88a60
<QgsCategorizedSymbolRendererV2::sSkipRender>, __in_chrg=<optimized out>)
   at /home/ale/dev/QGIS/src/core/symbology-ng/qgssymbolv2.h:366
#5  0x00007efeddf135ea in __cxa_finalize (d=0x7efee2d87540) at cxa_finalize.c:56
#6  0x00007efee23a74b3 in __do_global_dtors_aux () from /home/ale/apps/lib/libqgis_core.so.2.13.0
#7  0x00007fff7bf20580 in ?? ()
#8  0x00007efee2d9a73a in _dl_fini () at dl-fini.c:252
Backtrace stopped: frame did not save the PC
```

#3 - 2015-12-17 11:59 AM - Nyall Dawson

- Assignee changed from Nyall Dawson to Matthias Kuhn

In that case it's related to geoemtry modifiers. Have you tested with current master? There's been a number of related fixes since this feature landed.

#4 - 2015-12-18 12:27 AM - Alessandro Pasotti

I first notice this on master, re-tested now on latest master 4511cc474e5b7 and it still segfaults.

#5 - 2015-12-20 11:23 PM - Alessandro Pasotti

- Priority changed from High to Severe/Regression

#6 - 2015-12-22 07:28 AM - Matthias Kuhn

I'm pretty sure it's related to

static QgsMarkerSymbolV2 sSkipRender;

in qgscategorizedsymbolrendererv2.h

It may help to use a local static instead of a global static or some other tricks. I wasn't able to reproduce it quickly.

#7 - 2015-12-22 07:41 AM - Matthias Kuhn

Pushed a commit to master that prevents from copying QgsSymbolV2 (that would be a possible reason for this crash. In fact I couldn't think of another one).
I would have expected the compiler to fail at the root of the problem but it did not... Maybe it's caused by a python plugin?

#8 - 2015-12-22 08:07 AM - Alessandro Pasotti

The good is that with latest master I can now reproduce it in the Qt-Creator debugger, the bad is that it still segfaults with complete different trace:

```
0  malloc_consolidate  malloc.c  4157  0x7ffff2f9c8f3
1  _int_free  malloc.c  4057  0x7ffff2f9d56d
2  ??  0x7ffff5c331cc
3  ??  0x7ffff5c3323f
4  ??  0x7ffff59e9c2b
5  GDALDriver::~GDALDriver()  0x7ffff5c0c742
6  GDALDriver::~GDALDriver()  0x7ffff5c0c779
7  GDALDriverManager::~GDALDriverManager()  0x7ffff5c0ecae
8  GDALDriverManager::~GDALDriverManager()  0x7ffff5c0ece9
9  ??  0x7ffff590133a
10  _dl_fini  dl-fini.c  252  0x7ffff7dea73a
11  __run_exit_handlers  exit.c  82  0x7ffff2f5a259
12  __GI_exit  exit.c  104  0x7ffff2f5a2a5
13  __libc_start_main  libc-start.c  321  0x7ffff2f3fecc
14  _start  0x4198b9
```

I guess that you solved the issue reported here (and maybe also #13986) but there is still something wrong happening.

Disabling all plugins doesn't help.

#9 - 2015-12-23 01:25 AM - Alessandro Pasotti

Just tested with python disabled: still crashing.

#10 - 2015-12-23 02:09 AM - Alessandro Pasotti

Update: testing e6a265c1030bae01aa8d0eca905693e371ff0bd7

CGI still crashes with the same error:

```
(gdb) bt
#0  0x0000000000000181 in ?? ()
#1  0x00007f5d01f85ebc in qDeleteAll<QList<QgsSymbolLayerV2*>::const_iterator> (begin=..., end=...) at
/usr/include/qt4/QtCore/qalgorithms.h:322
#2  0x00007f5d01f84a5e in qDeleteAll<QList<QgsSymbolLayerV2*> > (c=...) at /usr/include/qt4/QtCore/qalgorithms.h:330
```

#3 0x00007f5d01f78180 in QgsSymbolV2::~QgsSymbolV2 (this=0x7f5d02956a60 <QgsCategorizedSymbolRendererV2::sSkipRender>, __in_chrg=<optimized out>)
    at /home/ale/dev/QGIS/src/core/symbology-ng/qgssymbolv2.cpp:239
#4 0x00007f5d01f871e8 in QgsMarkerSymbolV2::~QgsMarkerSymbolV2 (this=0x7f5d02956a60 <QgsCategorizedSymbolRendererV2::sSkipRender>, __in_chrg=<optimized out>)
    at /home/ale/dev/QGIS/src/core/symbology-ng/qgssymbolv2.h:384
#5 0x00007f5cfdad25ea in __cxa_finalize (d=0x7f5d02955560) at cxa_finalize.c:56
#6 0x00007f5d01f6cbf3 in __do_global_dtors_aux () from /home/ale/apps/lib/libqgis_core.so.2.13.0
#7 0x00007ffe49868810 in ?? ()
#8 0x00007f5d0296873a in _dl_fini () at dl-fini.c:252
Backtrace stopped: frame did not save the PC

#11 - 2015-12-25 12:20 AM - Anonymous

- Status changed from Open to Closed

Fixed in changeset commit:"036eada9903d4e658fe7fcb6c399b61598665d7a".

#12 - 2015-12-26 09:58 AM - Alessandro Pasotti

Confirmed: thanks!