QGIS Application - Bug report #9213
'bad_alloc' error at QGIS start

2013-12-14 01:57 PM - Ivan Mincik

Status:	Closed		
Priority:	High		
Assignee:			
Category:	Map Canvas		
Affected QGIS version:	master	**Regression?:**	No
Operating System:	XUbuntu 12.04	**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	17837

Description

There is an error message 'std::bad_alloc' just after QGIS window is started (see qgis-bad-alloc.png). This problem is confirmed on QGIS-dev list [1] by one user.

This error appears very randomly. Sometimes I can start QGIS multiple times without this error, sometimes there are sequences where when it always appears. Error appears also in QGIS 2.0.1. In 2.0.1 it causes application crash after a few operations are done (for example after opening leayer and moving in map).

I have compiled QGIS master in my PPA [2] with debug messages and I am attaching output messages of QGIS start without error (qgis-bad-alloc-debug-messages-no-error.txt) and with error (qgis-bad-alloc-debug-messages-error.txt - output is finished on error). From my point of view there is no significant difference between those files other than 'no-error' file continues until successful application start.

Software versions:
OS: XUbuntu 12.04 32bit
QGIS version 2.1.0-Master
Compiled against Qt 4.8.1 - Running against Qt 4.8.1
Compiled against GDAL/OGR 1.10.0 - Running against GDAL/OGR 1.10.0
Compiled against GEOS 3.3.8-CAPI-1.7.8 - Running against GEOS 3.3.8-CAPI-1.7.8
PostgreSQL Client Version 9.1.11
SpatiaLite Version 4.1.0
QWT Version 5.2.2
PROJ.4 Version 480

--
1 - https://www.mail-archive.com/qgis-developer@lists.osgeo.org/msg19096.html
2 - https://launchpad.net/~imincik/+archive/qgis-master

Associated revisions

Revision 3a075a6b - 2014-02-10 02:29 AM - Kiith-Sa

Fix #9213 ('bad_alloc' error at QGIS start)

Revision ac9eed7e - 2014-02-10 04:59 AM - Martin Dobias

Merge pull request #1157 from kiith-sa/master

Fix #9213 ('bad_alloc' error at QGIS start)

History

#1 - 2013-12-14 02:08 PM - Luigi Pirelli

append to me too...

first we had experienced with this error on windows (32b) loading plugin containing a lot of data (300MB) and we solved separating plugin from test data. But I started to have this error since last week randomly (three times) and I'm on debian wheezy. I wasn't able to reproduce the error.

#2 - 2013-12-14 02:22 PM - Giovanni Allegri

I confirm the same random problem, both on Ubuntu and Xubuntu 12.04 with QGIS 2.0.1 packages from UbuntuGis PPA

#3 - 2013-12-15 03:05 AM - Luigi Pirelli

Luigi Pirelli wrote:

> *append to me too...*
>
> *first we had experienced with this error on windows (32b) loading plugin containing a lot of data (300MB) and we solved separating plugin from test data. But I started to have this error since last week randomly (three times) and I'm on debian wheezy (compiled). I wasn't able to reproduce the error.*

#4 - 2013-12-16 08:50 AM - Ivan Mincik

At least in my case, it seems that this problem appears more frequently when running Ubuntu in VirtualBox than on physical machine.

#5 - 2013-12-16 11:26 AM - Jürgen Fischer

- Assignee deleted (Jürgen Fischer)

#6 - 2013-12-18 12:47 AM - Matthias Kuhn

Just got the same for the first time on my Fedora machine (using a freshly compiled master). The last time I have seen this was on a Windows machine using an early 1.9 dev build.

At the same time I lost my whole local configuration.

#7 - 2013-12-18 02:04 AM - Ivan Mincik

Could it be some problem in counting extent and starting scale of map canvas from QGIS application window ? From debug messages it seems that the error is thrown just before setting scale.

#8 - 2014-01-01 01:32 PM - Ivan Mincik

I have found that if I run QGIS from command line this problem occurs less frequently than when running from applications menu. Any ideas ?

#9 - 2014-02-04 03:54 PM - Ivan Mincik

Tests with latest master has shown that QGIS will throw bad_alloc error when there is less than 880 MiB of virtual memory on 64bit system or 310 MiB on 32 bit system. Error is thrown from 'setEditText' from 'QgsScaleComboBox::setScaleString' in 'src/gui/qgsscalecombobox.cpp'.

QGIS is allocating 64 MiB at start. I do not understand why it grows to 800 suddenly.

Test was done by Ferdinand Majerech.

#10 - 2014-02-05 12:48 PM - Ferdinand Majerech

Memory usage doesn't really 'grow' to ~880 MiB; QGIS is simply unable to allocate if it doesn't have that much virtual memory
(which can be limited by `ulimit -Sv <SIZE>` where <SIZE> is the virtual memory limit in kiB).
The same thing happens to various other programs that pull a lot of dependencies (e.g. Gimp, KDevelop).

I think that's not really a 'bug', but rather a performance problem - QGIS **always** crashes with
std::bad_alloc (or a different alloc error, based on where it fails to alloc, although
the setEditText() call mentioned above is the most common cause, and produces a matching log to
this bugreport) if it doesn't have that much free virtual memory. I also suspect it may vary between
machines (e.g. the 32bit system I tested on has 2 GiB of RAM, the 64bit one has 16 GiB).

It doesn't exactly match the behavior of this bug (**randomly** throws std::bad_alloc at startup regardless of memory size), which
I've reproduced only with 2.0.1 so far (still testing). It just produces the same log as above (and even that may not be the case
if it fails to alloc elsewhere)

#11 - 2014-02-07 05:54 AM - Giovanni Manghi

- Priority changed from Normal to High

#12 - 2014-02-07 06:05 PM - Ferdinand Majerech

- File std_bad_alloc_before_adjust_extent_to_size.txt added

I've now reproduced the random std::bad_alloc at startup bug. I think it's unrelated to the
std::bad_alloc on low RAM described in the 2 above updates.

It seems the std::bad_alloc is actually thrown before adjustExtentToSize() is called.
I added some prints to QgsApplication::notify() where the std::bad_alloc is caught, log is in the attached file.

The interesting part of the log (see the '//' comments)
The std::bad_alloc always seems to happen when QgsApplication::notify() is called with a QEvent::MouseMove event and a QWidget receiver. I'm not yet sure if it's always the same widget since I can't reproduce this bug in GDB.

```
src/core/qgsmessagelog.cpp: 45: (logMessage) 2014-02-08T00:46:44 [0] QGIS Ready!
src/app/qgisapp.cpp: 723: (QgisApp) Before processEvents

// BEFORE EXCEPTION CAUGHT (event 5 is QEvent::MouseMove)
src/core/qgsapplication.cpp: 232: (notify) notify QWidget, event 5
// AFTER EXCEPTION CAUGHT
src/core/qgsapplication.cpp: 270: (notify) Exception info: std::bad_alloc
receiver class: QWidget
event type:     5
```

src/gui/qgsmapcanvas.cpp: 1042: (paintEvent) QgsMapCanvas::paintEvent
src/gui/qgsmapcanvasmap.cpp: 46: (resize) resizing to 844x598
src/core/qgsmaprenderer.cpp: 193: (adjustExtentToSize) Map units per pixel (x,y) : 0, 0
src/core/qgsmaprenderer.cpp: 194: (adjustExtentToSize) Pixmap dimensions (x,y) : 844, 598
src/core/qgsmaprenderer.cpp: 195: (adjustExtentToSize) Extent dimensions (x,y) : 0, 0
src/core/qgsmaprenderer.cpp: 196: (adjustExtentToSize) Empty
src/core/qgsmaprenderer.cpp: 204: (adjustExtentToSize) Adjusted map units per pixel (x,y) : 0, 0
src/core/qgsmaprenderer.cpp: 206: (adjustExtentToSize) Recalced pixmap dimensions (x,y) : nan, nan
src/core/qgsscalecalculator.cpp: 131: (calculateGeographicDistance) Distance across map extent (m): 0
src/core/qgsscalecalculator.cpp: 88: (calculate) scale = 0 conversionFactor = 39.3701
src/core/qgsmaprenderer.cpp: 211: (adjustExtentToSize) Scale (assuming meters as map units) = 1:0
src/gui/qgsmapcanvas.cpp: 1098: (paintEvent) QgsMapCanvas::paintEvent exit

#13 - 2014-02-09 04:15 PM - Ferdinand Majerech

I found the source of the bug.

The QgisApp class defined in src/app/qgisapp.h and src/app/qgisapp.cpp has a data member unsigned int mMousePrecisionDecimalPlaces, which is not initialized to any value by QgisApp constructor.
This member is then used uninitialized in QgisApp::showMouseCoordinate() to specify precision for a QgsPoint::toString() call. Since mMousePrecisionDecimalPlaces is unsigned, any value it may have without initialization is valid as a precision specifier. If this value happens to be e.g. 2bln, it will create a 2bln character string, which takes 2GiB. The worst-case is a 4GiB allocation, which is why the bug can't be (easily) reproduced oh high-RAM machines.

Also, there is a mMousePrecisionAutomatic data member, which seems related, but is not used anywhere in QGIS.

Also, I noticed that there is quite a lot of data members not initialized by the constructor of QgisApp (and likely in the rest of QGIS?). This should be avoided if possible; even if a variable is expected to be set right after the constructor by e.g. a method call, not every user of the class may know that and it may result in more similar bugs. It's better to find a workable default and use that in the constructor, or to set an absurd value that is guaranteed to blow up if not set before use to detect bugs immediately (rather than an uninitialized value that **may or may not** crash resulting in heisenbugs like this)

#14 - 2014-02-09 05:36 PM - Ferdinand Majerech

Pull request with the fix:

https://github.com/qgis/QGIS/pull/1157

#15 - 2014-02-09 07:59 PM - Martin Dobias

- Status changed from Open to Closed

Fixed in changeset commit:"ac9eed7e052428722cd66ce0e39aee933c8176e6".

Files

qgis-bad-alloc.png	76.6 KB	2013-12-14	Ivan Mincik
qgis-bad-alloc-debug-messages-error.txt	25.4 KB	2013-12-14	Ivan Mincik

qgis-bad-alloc-debug-messages-no-error.txt	31.7 KB	2013-12-14	Ivan Mincik
std_bad_alloc_before_adjust_extent_to_size.txt	26.5 KB	2014-02-07	Ferdinand Majerech