QGIS Application - Bug report #6817
Qgis crashes while trying to edit a symbol in "graduated symbology"

2012-12-04 04:21 AM - Filipe Dias

Status:	Closed		
Priority:	Severe/Regression		
Assignee:			
Category:	Symbology		
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	fixed
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	15962

Description

Qgis crashes while trying to edit a symbol in "graduated symbology". Steps to reproduce:

Add layer -> define graduated symbology -> try do edit a symbol of one of the categories

This message appears in the terminal

Segmentation fault (core dumped)

Associated revisions

Revision 80319e31 - 2012-12-06 02:33 AM - Giuseppe Sucameli

fix #6817 (introduce with a1a1fb7be)

History

#1 - 2012-12-04 04:38 AM - Giovanni Manghi

- Status changed from Open to Feedback

is this a regression since 1.8?

#2 - 2012-12-04 05:01 AM - Salvatore Larosa

- Priority changed from Normal to Severe/Regression

Giovanni Manghi wrote:

> *is this a regression since 1.8?*

Yes!

#3 - 2012-12-05 02:17 PM - Giovanni Manghi

- Status changed from Feedback to Open

#4 - 2012-12-05 05:34 PM - Giuseppe Sucameli

- Status changed from Open to Closed

Fixed in changeset commit:"80319e310b09ec73cbbd8d9dba2c2634b2ae2745".

#5 - 2012-12-06 06:06 AM - Giuseppe Sucameli

- % Done changed from 0 to 50

- Status changed from Closed to Reopened

The problem was partially fixed: before the fix it crashed everytime the model tried to get a value, not when it tries to store the new one.

#6 - 2012-12-06 06:06 AM - Giuseppe Sucameli

- OS version deleted (12.04 64 bits)

- Operating System deleted (Linux)

#7 - 2012-12-07 01:12 AM - Giuseppe Sucameli

- Status changed from Reopened to Feedback

I was able to reproduce the problem yesterday, now on the same machine and same revision I do not get any crash...

#8 - 2012-12-07 01:15 AM - Filipe Dias

I just downloaded the version from 2012/12/05 and I get the crash. Does that version include your code revision?

#9 - 2012-12-07 04:48 AM - Salvatore Larosa

I am still getting the crash here.
The backtrace throws as following:

```
Program received signal SIGSEGV, Segmentation fault.
0x00007ffff2b46f83 in QTreeViewPrivate::layout(int, bool, bool) ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
(gdb) bt
#0  0x00007ffff2b46f83 in QTreeViewPrivate::layout(int, bool, bool) ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#1  0x00007ffff2b473ae in QTreeViewPrivate::layout(int, bool, bool) ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#2  0x00007ffff2b473ae in QTreeViewPrivate::layout(int, bool, bool) ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#3  0x00007ffff2b473ae in QTreeViewPrivate::layout(int, bool, bool) ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
```

and never ends !

#10 - 2012-12-07 06:06 AM - Giuseppe Sucameli

Filipe Dias wrote:

> *I just downloaded the version from 2012/12/05 and I get the crash. Does that version include your code revision?*

The revision commit:80319e310 includes my fix (see the above #6817-4)

Now I'm on revision commit:ef6da72a79, but I'm unable to reproduce it.

#11 - 2012-12-07 07:25 AM - Salvatore Larosa

- Crashes QGIS or corrupts data changed from No to Yes

here a video on how I get the crash:

http://lrssvt.ns0.it/img/crash_graduated_symbol.ogv

#12 - 2012-12-08 02:00 PM - Pedro Venâncio

Hi Giuseppe,

Here with version 1.9.0+git20121205+56bba06~precise-ubuntugis1 still crashes (segmentation fault).

Thanks!

#13 - 2012-12-08 03:01 PM - Salvatore Larosa

- File patch_symbol_graduated.patch added

I did a trivial changing and it seem works !

Patch attached!

#14 - 2012-12-08 03:20 PM - Giuseppe Sucameli

Salvatore Larosa wrote:

> *I did a trivial changing and it seem works !*
>
> *Patch attached!*

How your patch fixes the problem above?

#15 - 2012-12-09 08:48 AM - Salvatore Larosa

I am aware that my patch is very odd !!!

Accordingly to the backtrace, I just compared the QTreeView
class both categorized and graduated ui files, and I noticed
they were different. I guess they have behavior similar so
by adding the missing property in graduated ui file (iconSize, allColumnsShowFocus)
I do not get any crash.

I also think you will have one more solid solution ! :-)

I forgot add that the patch solve the issue in my case, under Linux !
I am not sure if it works in other cases, I suppose !

#16 - 2012-12-09 09:21 AM - Giuseppe Sucameli

Salvatore Larosa wrote:

> *I am aware that my patch is very odd !!!*

please, could you try to build QGis again w/o your fix? It's just to understand if the problem is really related to your patch of to something in a mess state: the code of the graduated view's model was re-written by Radim, so probably it's due to some lines expecting the old view model (see my previous fix).

> *I forgot add that the patch solve the issue in my case, under Linux !*
> *I am not sure if it works in other cases, I suppose !*

Me too.

#17 - 2012-12-09 09:41 AM - Salvatore Larosa

Giuseppe Sucameli wrote:

> *please, could you try to build QGis again w/o your fix?*

Right now my built version is w/o patch and QGIS crashes !

#18 - 2012-12-23 12:53 PM - Pedro Venâncio

I think this is fixed now.

Anyone confirms?

#19 - 2012-12-23 01:40 PM - Filipe Dias

With today's QGIS Master I still get the crash.

#20 - 2012-12-24 08:03 AM - Giovanni Manghi

- Status changed from Feedback to Open

Filipe Dias wrote:

> *With today's QGIS Master I still get the crash.*

crash still confirmed on master

#21 - 2012-12-31 02:06 AM - Arunmozhi P

Here is a backtrace that might be helpful.

```
---Type <return> to continue, or q <return> to quit---
#32708 0x03aecef1 in QTreeViewPrivate::layout(int, bool, bool) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32709 0x03aecef1 in QTreeViewPrivate::layout(int, bool, bool) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32710 0x03aecef1 in QTreeViewPrivate::layout(int, bool, bool) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32711 0x03aecef1 in QTreeViewPrivate::layout(int, bool, bool) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32712 0x03aecef1 in QTreeViewPrivate::layout(int, bool, bool) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32713 0x03aecef1 in QTreeViewPrivate::layout(int, bool, bool) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32714 0x03aee6bf in QTreeViewPrivate::expand(int, bool) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32715 0x03aefbf5 in QTreeView::mouseDoubleClickEvent(QMouseEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32716 0x035451ca in QWidget::event(QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32717 0x03962e55 in QFrame::event(QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32718 0x039f5ab1 in QAbstractScrollArea::viewportEvent(QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32719 0x03a9bacc in QAbstractItemView::viewportEvent(QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32720 0x03ae9b66 in QTreeView::viewportEvent(QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32721 0x039f81d6 in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32722 0x0324fb16 in QCoreApplicationPrivate::sendThroughObjectEventFilters(QObject*, QEvent*) () from
/usr/lib/i386-linux-gnu/libQtCore.so.4
#32723 0x034eaea2 in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32724 0x034f1024 in QApplication::notify(QObject*, QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32725 0x024f8a9c in QgsApplication::notify (this=0xbfffed10, receiver=0xa0bd498, event=0xbfffd294)
    at /home/teco/code/Quantum-GIS/src/core/qgsapplication.cpp:222
#32726 0x0324f97e in QCoreApplication::notifyInternal(QObject*, QEvent*) () from /usr/lib/i386-linux-gnu/libQtCore.so.4
#32727 0x034ebe95 in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget*, QWidget**,
QPointer<QWidget>&, bool) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32728 0x03578074 in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32729 0x03576c0d in QApplication::x11ProcessEvent(_XEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32730 0x035a3eac in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32731 0x0465cd86 in g_main_context_dispatch () from /lib/i386-linux-gnu/libglib-2.0.so.0
#32732 0x0465d125 in ?? () from /lib/i386-linux-gnu/libglib-2.0.so.0
#32733 0x0465d201 in g_main_context_iteration () from /lib/i386-linux-gnu/libglib-2.0.so.0
#32734 0x03282887 in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from
/usr/lib/i386-linux-gnu/libQtCore.so.4
#32735 0x035a3aaa in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32736 0x0324e50d in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/i386-linux-gnu/libQtCore.so.4
#32737 0x0324e7a9 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/i386-linux-gnu/libQtCore.so.4
#32738 0x03a3d0d9 in QDialog::exec() () from /usr/lib/i386-linux-gnu/libQtGui.so.4
```

#32739 0x081a2224 in QgisApp::showLayerProperties (this=0x894a500, ml=0x9b992a0) at
/home/teco/code/Quantum-GIS/src/app/qgisapp.cpp:8234
---Type <return> to continue, or q <return> to quit---
#32740 0x0818ede6 in QgisApp::layerProperties (this=0x894a500) at /home/teco/code/Quantum-GIS/src/app/qgisapp.cpp:4272
#32741 0x083e8717 in QgsLegend::mouseDoubleClickEvent (this=0x892b878, e=0xbfffe3c4)
at /home/teco/code/Quantum-GIS/src/app/legend/qgslegend.cpp:727
#32742 0x035451ca in QWidget::event(QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32743 0x03962e55 in QFrame::event(QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32744 0x039f5ab1 in QAbstractScrollArea::viewportEvent(QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32745 0x03a9bacc in QAbstractItemView::viewportEvent(QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32746 0x03ae9b66 in QTreeView::viewportEvent(QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32747 0x039f81d6 in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32748 0x0324fb16 in QCoreApplicationPrivate::sendThroughObjectEventFilters(QObject*, QEvent*) () from
/usr/lib/i386-linux-gnu/libQtCore.so.4
#32749 0x034eaea2 in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32750 0x034f1024 in QApplication::notify(QObject*, QEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32751 0x024f8a9c in QgsApplication::notify (this=0xbfffed10, receiver=0x8b15490, event=0xbfffe3c4)
at /home/teco/code/Quantum-GIS/src/core/qgsapplication.cpp:222
#32752 0x0324f97e in QCoreApplication::notifyInternal(QObject*, QEvent*) () from /usr/lib/i386-linux-gnu/libQtCore.so.4
#32753 0x034ebe95 in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget*, QWidget**,
QPointer<QWidget>&, bool) ()
from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32754 0x03578074 in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32755 0x03576c0d in QApplication::x11ProcessEvent(_XEvent*) () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32756 0x035a3eac in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32757 0x0465cd86 in g_main_context_dispatch () from /lib/i386-linux-gnu/libglib-2.0.so.0
#32758 0x0465d125 in ?? () from /lib/i386-linux-gnu/libglib-2.0.so.0
#32759 0x0465d201 in g_main_context_iteration () from /lib/i386-linux-gnu/libglib-2.0.so.0
#32760 0x03282887 in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from
/usr/lib/i386-linux-gnu/libQtCore.so.4
#32761 0x035a3aaa in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32762 0x0324e50d in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/i386-linux-gnu/libQtCore.so.4
#32763 0x0324e7a9 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/i386-linux-gnu/libQtCore.so.4
#32764 0x03253eba in QCoreApplication::exec() () from /usr/lib/i386-linux-gnu/libQtCore.so.4
#32765 0x034e8a74 in QApplication::exec() () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#32766 0x0816daa3 in main (argc=1, argv=0xbfffeff4) at /home/teco/code/Quantum-GIS/src/app/main.cpp:859
(gdb)

#22 - 2012-12-31 02:17 AM - Arunmozhi P

Giuseppe Sucameli wrote:

> *Salvatore Larosa wrote:*
>
> > *I did a trivial changing and it seem works !*
> >
> > *Patch attached!*
>
> *How your patch fixes the problem above?*

From the previously posted backtrace. The segfault is caused by the infinite loop triggered by the expand signal sent to the QTreeView. But our model doesn't seem to possess the required data, making the QTreeView to query repeatedly until seg fault.

Hence by setting isExpandable to false, I think this can be avoided.

#23 - 2012-12-31 02:19 AM - Arunmozhi P

I meant itemsExapandable in the previous post.

P.S: Is there a way to edit posted updates? I am sorry I have to post again to correct typos.

#24 - 2013-01-09 12:29 AM - Matthias Kuhn

#6966 was marked as a duplicate of this.

#25 - 2013-02-20 04:32 AM - Salvatore Larosa

- Status changed from Open to Closed

- Resolution set to fixed

Fixed in commit:d6cd228e5e12c28b348cf471a21daf2fdca389b5

Files

patch_symbol_graduated.patch	881 Bytes	2012-12-08	Salvatore Larosa