QGIS Application - Bug report #10471
Segmentation fault while zooming out

2014-06-05 05:21 AM - luca76 -

Status:	Closed		
Priority:	Severe/Regression		
Assignee:	Alvaro Huarte		
Category:			
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	fixed/implemented
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	18883

Description

Hi,

here is a test case with QGIS master version:
- import this GPX file;
- click on "Tracks" from dialog box;
- zoom out one or two times with mouse scroll

QGIS master crashes with a segmentation fault.

Related issues:

Related to QGIS Application - Bug report # 10433: QGIS master crashes when ch...	**Closed**	**2014-06-03**

History

#1 - 2014-06-05 05:24 AM - Giovanni Manghi

- Crashes QGIS or corrupts data changed from No to Yes

- Status changed from Open to Feedback

- Priority changed from Severe/Regression to High

Does not happen on QGIS master just compiled on Ubuntu. How old is your revision?

#2 - 2014-06-05 05:26 AM - luca76 -

I did a "git pull" 4 or 5 minutes ago :-)

Now I'm compiling QGIS with debug to watch more on this error...

#3 - 2014-06-05 07:33 AM - luca76 -

Doing gdb, the error is here:

```
0x00007ffff3dd3438 in QgsClipper::clippedLineWKB (wkb=0x7fff70033ffb "", clipExtent=..., line=...) at
/home/manganelll/qgis-git/QGIS/src/core/qgsclipper.cpp:72
72          memcpy( &p1x, wkb, sizeof( double ) ); wkb += sizeOfDoubleX;
```

The error is "Program received signal SIGSEGV, Segmentation fault."

#4 - 2014-06-05 07:40 AM - Giovanni Manghi

it works ok on previous qgis releases?

#5 - 2014-06-05 07:44 AM - luca76 -

Another machine - 32 bit, Debian Squeeze, QGIS 2.0: all is running fine.

#6 - 2014-06-05 07:48 AM - Giovanni Manghi

- Priority changed from High to Severe/Regression
- Status changed from Feedback to Open
- Target version set to Version 2.4

#7 - 2014-06-05 08:00 AM - luca76 -

Testing with QGIS last weekly (2014-06-02) on Windows 2003 Server: after loading the layer, QGIS crashes.

#8 - 2014-06-07 03:23 AM - Leyan Ouyang

- Assignee set to Alvaro Huarte

Your gpx file has a <trkseg /> on third line, which creates a multilinestring with an empty linestring. Then the geometry simplification modifies the internal wkb representation to remove the empty linestring, but keeps a reference to two linestrings, leading to the crash when the clipping functions tries to access the inexistant second linestring.

If I am not mistaken, Alvaro Huarte is responsible for the simplification ?

As a workaround, you can simply disable the geometry simplification, or manually edit your gpx file to remove line 3.

#9 - 2014-06-07 03:52 PM - Anita Graser

I also get many crashes with the following (mostly SpatiaLite-based) project
https://drive.google.com/folderview?id=0Bwc-5JFVTnfIZURsbzVHOHVYMjA&usp=sharing

Sometimes - but not always - when opening the project, sometimes when zooming.

#10 - 2014-06-08 01:50 AM - Giovanni Manghi

Anita Graser wrote:

> *I also get many crashes with the following (mostly SpatiaLite-based) project*
> *https://drive.google.com/folderview?id=0Bwc-5JFVTnfIZURsbzVHOHVYMjA&usp=sharing*
>
> *Sometimes - but not always - when opening the project, sometimes when zooming.*

confirmed here all the time when zooming. But it happens also if disabling simplification on all layers, so it may be worth a different ticket.

```
giovanni@sibirica ~ $ qgis
Warning: loading of qt translation failed [/usr/share/qt4/translations/qt_en_US]
Warning: QGraphicsScene::addItem: item has already been added to this scene
Warning: Loading a file that was saved with an older version of qgis (saved in 2.2.0-Valmiera, loaded in 2.3.0-Master). Problems may occur.
Warning 1: Self-intersection at or near point 266731.1539876138 2221823.4959021132
Warning 1: Self-intersection at or near point 273211.30081749696 2199190.1640909663
Warning 1: Self-intersection at or near point 273580.23986159556 2199690.4234136418
Warning 1: Self-intersection at or near point 282130.39047160413 2185188.3562248088
Warning 1: Self-intersection at or near point 307220.52828227985 2223378.6779606258
ERROR 1: Shell is not a LinearRing
ERROR 1: IllegalArgumentException: geometries must not contain null elements

QGIS died on signal 11[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[New Thread 0x7f13d23c8700 (LWP 12412)]
[New Thread 0x7f142eecf700 (LWP 12401)]
[New Thread 0x7f142f7e8700 (LWP 12400)]
0x00007f144afada43 in poll () from /lib/x86_64-linux-gnu/libc.so.6
[Current thread is 1 (Thread 0x7f145257e7c0 (LWP 12399))]
#0  0x00007f144afada43 in poll () from /lib/x86_64-linux-gnu/libc.so.6
No symbol table info available.
#1  0x00007f144980aff6 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
No symbol table info available.
#2  0x00007f144980b124 in g_main_context_iteration () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
No symbol table info available.
#3  0x00007f144dbbb3bf in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from
/usr/lib/x86_64-linux-gnu/libQtCore.so.4
No symbol table info available.
#4  0x00007f144cfb6d9e in ?? () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
No symbol table info available.
#5  0x00007f144db8ac82 in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from
/usr/lib/x86_64-linux-gnu/libQtCore.so.4
No symbol table info available.
#6  0x00007f144db8aed7 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
No symbol table info available.
#7  0x00007f144db8ff67 in QCoreApplication::exec() () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
No symbol table info available.
#8  0x0000000000560806 in main ()
No symbol table info available.
gdb returned 0
Aborted (core dumped)
```

#11 - 2014-06-10 06:18 AM - Martin Dobias

Giovanni / Anita: looks like a different problem. I haven't checked with Anita's data thoroughly yet, but the problem may be related to fix for #9655 (used also if simplification is turned off). Could you please verify it happens just with labeling turned on?

#12 - 2014-06-10 06:39 AM - Martin Dobias

Anita / Giovanni: seems to be the same thing as #10433

#13 - 2014-06-10 07:05 AM - Giovanni Manghi

Martin Dobias wrote:

> *Anita / Giovanni: seems to be the same thing as #10433*

Hi Martin it seems at least that the crash is caused by two different actions: in one case is the zoom, in the other is a change of symbology.

Anyway I'm compiling and see if both cases are still true.

#14 - 2014-06-10 07:56 AM - Giovanni Manghi

Martin Dobias wrote:

> *Anita / Giovanni: seems to be the same thing as #10433*

Hi Martin, I just compiled the latest code and now by just simply opening/zooming Anita's project I cannot replicate anymore the crash.

On the other hand #10433 is confirmed and it seems caused by labels, see my last comment there.

#15 - 2014-06-11 08:11 AM - Giovanni Manghi

- Resolution set to fixed/implemented

- Status changed from Open to Closed

this seems fixed in master, reopen if necessary.

#16 - 2014-06-11 11:57 PM - luca76 -

Yes, now it works! Great! :-)

Files

2014-06-05_12-46_gio.gpx.bz2	7.08 KB	2014-06-05	luca76 -