# QGIS Application - Bug report #193
# Qgis crashes on zoom in on a vector layer

2006-07-16 11:59 PM - Gavin Macaulay -

| | | | |
|---|---|---|---|
| **Status:** | Closed | | |
| **Priority:** | Low | | |
| **Assignee:** | Brendan Morley - | | |
| **Category:** | Vectors | | |
| **Affected QGIS version:** | | **Regression?:** | No |
| **Operating System:** | Mandriva | **Easy fix?:** | No |
| **Pull Request or Patch supplied:** | | **Resolution:** | fixed |
| **Crashes QGIS or corrupts data:** | | **Copied to github as #:** | 10252 |

**Description**

Open a vector layer (ogr or postgres), zoom in, and Qgis crashes. A backtrace indicates that the problem is in [[QgsVectorLayer]]::drawFeature:

```
#3918 0xb7e2d496 in [[QgsVectorLayer]]::drawLineString (this=0x82a6928,
   feature=0x551183bc <Address 0x551183bc out of bounds>, p=0xbfffcba0,
   mtp=0x818d3e8, projectionsEnabledFlag=false, drawingToEditingCanvas=true)
```

This is with the latest from SVN (r5608). This didn't happen a couple of days ago.

## History

#### #1 - 2006-07-17 02:15 AM - anonymous -

I suspect that this problem occured in svn commit:a68f1e00 (SVN r5596).

Sometimes zoomng in is okay, but eventually, qgis will crash.

#### #2 - 2006-07-17 04:45 AM - Brendan Morley -

I acknowledge that commit:a68f1e00 (SVN r5596) could have destabilised things but I can't get it to crash!

Example, three [[MapInfo]] layers through OGR 1.3.2.0. I've zoomed in both by the mouse wheel and the toolbar (arbitrary zoom in).

I have added a new argument to [[QgsVectorLayer]]::drawLineString in commit:8645462b (SVN r5594). Maybe a full make might clear things out, or if g_j_m can do a full trace?

#### #3 - 2006-07-18 12:34 AM - Gavin Macaulay -

I tried a make clean and then a make, but the problem still exists. The full backtrace is included below. It always works fine when I load a layer, but fails eventually when zooming in. From looking at the code and the backtrace, it looks like the wkb char* given to drawlinestring is wrong. The problem never happens with polygons or points. I suspect that the caching of geometries is going wrong somewhere...

```
#0  0xb7334cec in ?? () from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3905  0xbfff98b0 in ?? ()
#3906  0xff56c447 in ?? ()
#3907  0x472e2652 in ?? ()
```

#3908  0x00000000 in ?? ()
#3909  0x00000000 in ?? ()
#3910  0xb77b8548 in ?? () from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3911  0x00000800 in ?? ()
#3912  0xbfffc268 in ?? ()
#3913  0xbfffb9a8 in ?? ()
#10 0xb7438d50 in QRasterPaintEnginePrivate::~QRasterPaintEnginePrivate ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3914 0xb7438d50 in QRasterPaintEnginePrivate::~QRasterPaintEnginePrivate ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3915 0xb7427d97 in QSpanData::initTexture ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3916 0xb7430291 in QRasterPaintEngine::drawPolygon ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3917 0xb7404204 in QPainter::drawPolyline ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3918 0xb7e2e426 in [[QgsVectorLayer]]::drawLineString (this=0x8261b60,
   feature=0x472e2652 <Address 0x472e2652 out of bounds>, p=0xbfffcba0,
   mtp=0x811c7b0, projectionsEnabledFlag=false, drawingToEditingCanvas=true)
---Type <return> to continue, or q <return> to quit---
   at qvector.h:97
#3919 0xb7e37e1f in [[QgsVectorLayer]]::drawFeature (this=0x8261b60, p=0xbfffcba0,
   fet=0x82a31b0, theMapToPixelTransform=0x811c7b0, marker=0xbfffc8b0,
   markerScaleFactor=1, projectionsEnabledFlag=false,
   drawingToEditingCanvas=96) at qgsvectorlayer.cpp:3363
#3920 0xb7e385c6 in [[QgsVectorLayer]]::draw (this=0x8261b60, p=0xbfffcba0,
   viewExtent=0xbfffc9c0, theMapToPixelTransform=0x811c7b0,
   drawingToEditingCanvas=true, widthScale=1, symbolScale=1)
   at qgsvectorlayer.cpp:905
#3921 0xb7e38f3b in [[QgsVectorLayer]]::draw (this=0x8261b60, p=0xbfffcba0,
   viewExtent=0xbfffc9c0, theMapToPixelTransform=0x811c7b0,
   drawingToEditingCanvas=true) at qgsvectorlayer.cpp:794
#3922 0xb7da9efa in [[QgsMapRender]]::render (this=0x81b0c80, painter=0xbfffcba0)
   at qgsmaprender.cpp:262
#3923 0xb7d88617 in [[QgsMapCanvasMap]]::render (this=0x81520f0)
   at qgsmapcanvasmap.cpp:65
#3924 0xb7d83991 in [[QgsMapCanvas]]::render (this=0x81b1268) at qgsmapcanvas.cpp:303
#3925 0xb7d83935 in [[QgsMapCanvas]]::drawContents (this=0x81b1268, p=0xbfffcd40,
   cx=0, cy=0, cw=432, ch=450) at qgsmapcanvas.cpp:282
#3926 0xb7a79520 in Q3ScrollView::drawContentsOffset ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQt3Support.so.4
#3927 0xb7a78683 in Q3ScrollView::viewportPaintEvent ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQt3Support.so.4
---Type <return> to continue, or q <return> to quit---
#3928 0xb7a7acc9 in Q3ScrollView::eventFilter ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQt3Support.so.4
#3929 0xb733be14 in QApplicationPrivate::notify_helper ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3930 0xb733c045 in QApplication::notify ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3931 0xb7386ca0 in qt_sendSpontaneousEvent ()
  from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3932 0xb745f7d7 in QWidgetPrivate::drawWidget ()

from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3933 0xb746013d in QWidgetBackingStore::paintSiblingsRecursive ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3934 0xb745f4cf in QWidgetPrivate::drawWidget ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3935 0xb746013d in QWidgetBackingStore::paintSiblingsRecursive ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3936 0xb745f4cf in QWidgetPrivate::drawWidget ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3937 0xb746013d in QWidgetBackingStore::paintSiblingsRecursive ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#3938 0xb745f4cf in QWidgetPrivate::drawWidget ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#36 0xb746013d in QWidgetBackingStore::paintSiblingsRecursive ()
---Type <return> to continue, or q <return> to quit---
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#37 0xb745f4cf in QWidgetPrivate::drawWidget ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#38 0xb746013d in QWidgetBackingStore::paintSiblingsRecursive ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#39 0xb745ffc4 in QWidgetBackingStore::paintSiblingsRecursive ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#40 0xb745f4cf in QWidgetPrivate::drawWidget ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#41 0xb746013d in QWidgetBackingStore::paintSiblingsRecursive ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#42 0xb745f4cf in QWidgetPrivate::drawWidget ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#43 0xb746013d in QWidgetBackingStore::paintSiblingsRecursive ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#44 0xb745ffc4 in QWidgetBackingStore::paintSiblingsRecursive ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#45 0xb745f4cf in QWidgetPrivate::drawWidget ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#46 0xb7460586 in QWidgetBackingStore::cleanRegion ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#47 0xb7460ac1 in qt_syncBackingStore ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
---Type <return> to continue, or q <return> to quit---
#48 0xb73807f3 in QWidget::event ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#49 0xb7592a90 in QFrame::event ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#50 0xb733be38 in QApplicationPrivate::notify_helper ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#51 0xb733c045 in QApplication::notify ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#52 0xb6f60bfe in QCoreApplication::sendPostedEvents ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtCore.so.4
#53 0xb6f7fe1a in QEventDispatcherUNIX::processEvents ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtCore.so.4
#54 0xb73a4463 in QEventDispatcherX11::processEvents ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4

#55 0xb6f5bbd5 in QEventLoop::processEvents ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtCore.so.4
#56 0xb6f5be1f in QEventLoop::exec ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtCore.so.4
#57 0xb6f60d21 in QCoreApplication::exec ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtCore.so.4
#58 0xb733b4f6 in QApplication::exec ()
from /usr/local/Trolltech/Qt-4.1.4/lib/libQtGui.so.4
#59 0x0804cd07 in main (argc=1, argv=0xbffff5b4) at main.cpp:597

**#4 - 2006-07-18 06:38 PM - anonymous -**

*- Status changed from Open to In Progress*

I still can't reproduce. I would appreciate if anyone else can confirm or deny this behaviour on their own systems.

Given your stack trace, it appears that the [[QgsFeature]] object is OK but its embedded [[QgsGeometry]] object is the one with the invalid address.

Browsing through the source code, I can only see a possible problem if you are displaying a geometry that has been freshly edited ( http://svn.qgis.org/trac/browser/trunk/qgis/src/gui/qgsvectorlayer.cpp#L882). Otherwise the problem is probably originating from the data provider in use. What layer provider/format are you using? Is the layer small/free enough to send over here?

**#5 - 2006-07-18 06:44 PM - Brendan Morley -**

*- Status changed from In Progress to Open*

The previous comment was by morb_au by the way (I forgot to log into trac first)

**#6 - 2006-07-18 06:49 PM - Gavin Macaulay -**

It happens on vector layers from the postgres provider and the ogr provider. I'll attach a .shp file here later today.

The feature address in item 15 in the backtrace varies, suggesting to me that the memory is uninitialised or is being stomped on by some other part of the code.

I had a reasonable look through the code yesterday and didn't find anything except for the minor thing I resolved in commit:269d4ef5 (SVN r5611).

**#7 - 2006-07-19 04:06 AM - anonymous -**

The problem only happens if both items in the Rendering part of the QGIS Options dialog box are unticked. And then only when the coordinates passed to the call to drawPolyline() in qgsvectorlayer.cpp include negative values.

All of this implies that drawing to a Qt QImage with negative coordinates is causing the crash.

I think that the backtrace and its 'address out of bounds' message are a red herring.

I'm using Qt 4.1.4.

#### #8 - 2006-07-19 03:25 PM - Gavin Macaulay -

*- Status changed from Open to Closed*

*- Resolution set to fixed*

Fixed in SVN commit:79023aa0 (SVN r5613). Problem was that qgis was drawing to a QImage using negative coordinates, and QT doesn't like that. I'm not sure why this only happened now.

#### #9 - 2009-08-22 12:46 AM - Anonymous

Milestone Version 0.8 deleted

### Files

| | | | |
|---|---|---|---|
| water.tgz | 17.3 KB | 2006-07-18 | Gavin Macaulay - |