QGIS Application - Bug report #200
QGIS crashes on broken SHP file

2006-07-20 09:39 PM - anonymous -

Status:	Closed		
Priority:	Low		
Assignee:	Tim Sutton		
Category:	Vectors		
Affected QGIS version:		**Regression?:**	No
Operating System:	OS X	**Easy fix?:**	No
Pull Request or Patch supplied:		**Resolution:**	wontfix
Crashes QGIS or corrupts data:		**Copied to github as #:**	10259

Description

I tried to open a broken SHP file with 0.8 preview version, which crashed.

A sample SHP file which caused QGIS crash is available here:
homepage.mac.com/babayoshihiko/sw/JRline.tar.gz

The above file got broken when I tried to convert projection using [[ArcToolbox]]. ogrinfo says it's ESRI Shapefile, but when I tried to fix with ogr2ogr, it returns error (ERROR 3: Error in fseek() or fread() reading object from .shp file.). For qgis, it simply crashes the application.

History

#1 - 2006-07-21 01:38 AM - Gavin Macaulay -

I was a bit rash in assigning this bug to myself - my version of qgis running on Linux loads and displays the shp file fine, making it a bit hard to fix the problem. ogrinfo also gives sensible results.

#2 - 2006-08-16 07:13 AM - Tim Sutton

I tested on linux and the file loads fine for me too - I will test on mac and see if I can reproduce the issue.

#3 - 2006-08-22 06:35 PM - Tim Sutton

- Status changed from Open to In Progress

I was able to replicate this bug (on OSX). It produces the following stacktrace (see below). It looks like there is no attribute table or something...will investigate further...

0 <<00000000>> 0xffff0691 +bzero + 145 (cpu_capabilities.h:187)
1 libSystem.B.dylib 0x9000adb8 strncpy + 216
2 libgdal.1.dylib 0x01e34578 DBFIsAttributeNULL + 39
3 libgdal.1.dylib 0x01eb3d8a SHPReadOGRFeature(SHPInfo*, DBFInfo*, OGRFeatureDefn*, int) + 274
4 libgdal.1.dylib 0x01e9f035 OGRShapeLayer::GetNextFeature() + 239
5 ogrprovider.so 0x185fd2ff [[QgsOgrProvider]]::getNextFeature(std::list<int, std::allocator<int> > const&, int) + 161 (bundle1.s:110)
6 libqgis_gui.0.dylib 0x018e2186 [[QgsVectorLayer]]::draw(QPainter*, [[QgsRect]]*, [[QgsMapToPixel]]*, bool, double, double) + 368
7 libqgis_gui.0.dylib 0x018e2d22 [[QgsVectorLayer]]::draw(QPainter*, [[QgsRect]]*, [[QgsMapToPixel]]*, bool) + 72
8 libqgis_gui.0.dylib 0x0187f702 [[QgsMapRender]]::render(QPainter*) + 888
9 libqgis_gui.0.dylib 0x01866c62 [[QgsMapCanvasMap]]::render() + 646

```
10  libqgis_gui.0.dylib    0x01862703 [[QgsMapCanvas]]::render() + 57
11  libqgis_gui.0.dylib    0x018623ac [[QgsMapCanvas]]::drawContents(QPainter*, int, int, int, int) + 90
12  Qt3Support             0x003baae7 Q3ScrollView::viewportPaintEvent(QPaintEvent*) + 679
13  Qt3Support             0x003bd4a7 Q3ScrollView::eventFilter(QObject*, QEvent*) + 425
14  [[QtGui]]              0x01216d41 QApplicationPrivate::notify_helper(QObject*, QEvent*) + 275
15  [[QtGui]]              0x0121c507 QApplication::notify(QObject*, QEvent*) + 1197
16  [[QtGui]]              0x0125ea18 QWidgetPrivate::qt_widget_event(OpaqueEventHandlerCallRef*, [[OpaqueEventRef]]
```

#4 - 2006-08-22 07:37 PM - Tim Sutton

I had a more detailed look at this.

```
0  <<00000000>>    0xffff0691 +bzero + 145 (cpu_capabilities.h:187)
1  libSystem.B.dylib      0x9000adb8 strncpy + 216
2  libgdal.1.dylib        0x01ba934c DBFIsAttributeNULL + 39
3  libgdal.1.dylib        0x01c4ca86 SHPReadOGRFeature(SHPInfo*, DBFInfo*, OGRFeatureDefn*, int) + 274
4  libgdal.1.dylib        0x01c2f1cf OGRShapeLayer::GetNextFeature() + 239
5  ogrprovider.so         0x175a1fff [[QgsOgrProvider]]::getNextFeature(std::list<int, std::allocator<int> > const&, int) + 161
```

So the crash is occurring withing gdal itself. There doesnt seem to be any way to manage a bad read in src/providers/ogr/qgsogrprovider.cpp:

```
330    OGRFeature *fet;
331    while ((fet = ogrLayer->GetNextFeature()) != NULL) {
332      if (fet->GetGeometryRef())
333        break;
334    }
```

If the ogr call [[GetNextFeature]] fails there is no error that is returned and no decent way that I can see to smoothly handle the problem. I will need to write to the gdal list and see if there is any option for a fix but it doesnt look promising at this point....

#5 - 2006-08-23 12:07 PM - Tim Sutton

- Status changed from In Progress to Closed

- Resolution set to wontfix

I reported this issue to GDAL and Frank Warmerdam will include some better error handling in the next release of gdal. Until then there is nothing we can do about it from the qgis side so I am closing this bug.

#6 - 2006-08-28 07:24 AM - Mateusz Loskot -

As we talked with Tim and Frank on the #gdal, the problem is that attached jrline.shp file includes truncated features with id **62** and it seems invalid shapefile. I'm eager to learn what's wrong with this file. What's certain thing, is that **fseek and fread fail on this shapefile** (lines 1451-1452 in the shpopen.c file).

I fixed it in OGR and its Shape driver adding stronger tests to results of Shapefile operations.
The main changes have been applied to **SHPReadOGRFeature()** function.
So, now **GetFeature()** and **GetNextFeature()** will **return NULL** if Shapelib (fseek/fread, see above) fail to read shape object from layer.

Here is sample test trying to read feature **62** from **jrline.shp**.

```
mloskot:~/dev/gdal/bugs/qgis_200$ ~/dev/gdal/_cvs/gdal/ogr/ogrinfo -fid 62 jrline.shp jrline
INFO: Open of @jrline.shp'
    using driver @ESRI Shapefile' successful.

Layer name: jrline
Geometry: Line String
Feature Count: 63
Extent: (135.613700, 34.820579) - (135.890390, 35.085503)
Layer SRS WKT:
PROJCS["JGD2000_Japan_Zone_6",
  GEOGCS["GCS_JGD_2000",
    DATUM["JGD_2000",
      SPHEROID[[GRS_1980]],
    PRIMEM[[Greenwich]],
    UNIT[[Degree]],
  PROJECTION[[Transverse_Mercator]],
  PARAMETER[[False_Easting]],
  PARAMETER[[False_Northing]],
  PARAMETER[[Central_Meridian]],
  PARAMETER[[Scale_Factor]],
  PARAMETER[[Latitude_Of_Origin]],
  UNIT[[Meter]]
[[ArcID]]: Real (16.6)
[[ArcType]]: String (20.0)
[[FromNode]]: Real (16.6)
[[ToNode]]: Real (16.6)
[[LeftPoly]]: Real (16.6)
[[RightPoly]]: Real (16.6)
Length: Real (16.6)
[[NumericUse]]: Real (16.6)
[[TextUserId]]: String (50.0)
SEQUENTIAL: Real (16.6)
ENTITY: Real (16.6)
ARCNUM: Real (16.6)
CLASS: Real (16.6)
ERROR 3: Error in fseek() or fread() reading object from .shp file.
ERROR 1: Couldn't read geometry from shape with feature id (62), likely data is corrupted.
Unable to locate feature id 62 on this layer
```

As you can see, there are 3 error messages at the end of the output:
ERROR 3 - comes from shpopen.c
ERROR 1 - comes from SHPReadOGRFeature() function and indicates that Shapelib's **SHPReadObject()** failed (what ERROR 3 confirms).
Unable to locate feature id 62 on this layer - comes from ogrinfo utility.

So, obviously, in case of similar problems in QGIS, you should see first two messages in the console.

In case of GDAL/OGR problems, don't hesitate to **give me a note**.

Files

JRline.tar.gz	19.2 KB	2006-07-20	anonymous -