

QGIS Application - Bug report #10515

QGIS Crash when trying to load a point layer to georss file

2014-06-09 11:12 AM - Richard Duivenvoorde

Status:	Closed	
Priority:	High	
Assignee:		
Category:	Vectors	
Affected QGIS version:	master	Regression?: No
Operating System:	Ubuntu	Easy fix?: No
Pull Request or Patch supplied:	No	Resolution:
Crashes QGIS or corrupts data:	Yes	Copied to github as #: 18925

Description

I'm on commit:a715ce6 debian testing.

And wanted to try to save a point shp file to save as georss (via saveAs), QGIS crashes.

Easy to reproduce: you can even create a memory layer with one point (epsg:4326), save as GeoRSS and QGIS crashes with segfault.

Tried to run with gdb, but only got this backtrace (first saved as geojson, which was ok):

```
src/core/qgsvectorfilewriter.cpp: 1862: (writeAsVectorFormat) newFilename = /tmp/georss.geojson
[Thread 0x7fff73c56700 (LWP 11325) exited]
src/gui/qgscollapsiblegroupbox.cpp: 112: (showEvent) found a QScrollArea parent: scrollArea
src/gui/qgscollapsiblegroupbox.cpp: 372: (updateStyle) groupbox: mExtentGroupBox style: gtk+ offset: left=0 top=1 top2=5
src/gui/qgscollapsiblegroupbox.cpp: 112: (showEvent) found a QScrollArea parent: scrollArea
src/gui/qgscollapsiblegroupbox.cpp: 372: (updateStyle) groupbox: mLayerOptionsGroupBox style: gtk+ offset: left=0 top=1 top2=5
src/gui/qgscollapsiblegroupbox.cpp: 112: (showEvent) found a QScrollArea parent: scrollArea
src/gui/qgscollapsiblegroupbox.cpp: 372: (updateStyle) groupbox: mOgrOptionsGroupBox style: gtk+ offset: left=0 top=1 top2=5
src/gui/qgscollapsiblegroupbox.cpp: 112: (showEvent) found a QScrollArea parent: scrollArea
src/gui/qgscollapsiblegroupbox.cpp: 372: (updateStyle) groupbox: mDataSourceOptionsGroupBox style: gtk+ offset: left=0 top=1 top2=5
[New Thread 0x7fff73c56700 (LWP 11413)]
[New Thread 0x7fff73455700 (LWP 11414)]
[Thread 0x7fff73c56700 (LWP 11413) exited]
[New Thread 0x7fff73c56700 (LWP 11415)]
[Thread 0x7fff73c56700 (LWP 11415) exited]
src/core/qgsvectorfilewriter.cpp: 230: (QgsVectorFileWriter) Created data source
src/core/qgsvectorfilewriter.cpp: 254: (QgsVectorFileWriter) WKT to save as is GEOGCS["WGS
84",DATUM["WGS_1984",SPHEROID["WGS
84",6378137,298.257223563,AUTHORITY["EPSG","7030"]],AUTHORITY["EPSG","6326"],PRIMEM["Greenwich",0,AUTHORITY["EPSG","8
Y["EPSG","8901"]],UNIT["degree",0.0174532925199433,AUTHORITY["EPSG","9122"]],AUTHORITY["EPSG","4326"]]
src/core/qgsvectorfilewriter.cpp: 322: (QgsVectorFileWriter) created layer
src/core/qgsvectorfilewriter.cpp: 325: (QgsVectorFileWriter) creating 0 fields
src/core/qgsvectorfilewriter.cpp: 470: (QgsVectorFileWriter) Done creating fields
src/core/qgsvectorfilewriter.cpp: 1862: (writeAsVectorFormat) newFilename = /tmp/georss.xml

Program received signal SIGSEGV, Segmentation fault.
0x0000000000000041 in ?? ()

Tested also on windows, but there is seems ok.
```

Anybody can confirm?

Associated revisions

Revision cee63c84 - 2015-10-18 04:51 PM - Jürgen Fischer

vector file writer: defer destroying spatial reference (fixes #10515)

Revision 44767492 - 2015-11-26 08:32 PM - Jürgen Fischer

vector file writer: defer destroying spatial reference (fixes #10515)

(cherry picked from commit cee63c84f7f85586ddcb5348e70a0af0b1bcd5e)

History

#1 - 2014-06-09 11:38 AM - Giovanni Manghi

- *Crashes QGIS or corrupts data changed from No to Yes*
- *Category set to Vectors*
- *Affected QGIS version changed from 2.2.0 to master*

I can confirm on Ubuntu/master/64 self compiled.

#2 - 2014-06-17 08:49 AM - Martin Dobias

I can replicate - the crash happens inside the OGR library:

```
#0 0x0000000000000040 in ?? ()
#1 0x00007ffff4f8b089 in OGRGeomFieldDefn::~OGRGeomFieldDefn (this=0x49aa510, __in_chrg=<optimized out>) at
ogrgeomfielddefn.cpp:124
#2 0x00007ffff4f4544f in OGRFeatureDefn::~OGRFeatureDefn (this=0x1134be0, __in_chrg=<optimized out>) at ogrfeaturedefn.cpp:116
#3 0x00007ffff4f454a9 in OGRFeatureDefn::~OGRFeatureDefn (this=0x1134be0, __in_chrg=<optimized out>) at ogrfeaturedefn.cpp:120
#4 0x00007ffff4de77d3 in OGRGeoRSSLayer::~OGRGeoRSSLayer (this=0x49aa360, __in_chrg=<optimized out>) at ogrgeorsslayer.cpp:156
#5 0x00007ffff4de78e9 in OGRGeoRSSLayer::~OGRGeoRSSLayer (this=0x49aa360, __in_chrg=<optimized out>) at ogrgeorsslayer.cpp:180
#6 0x00007ffff4de675f in OGRGeoRSSDataSource::~OGRGeoRSSDataSource (this=0x498ed70, __in_chrg=<optimized out>) at
ogrgeorssdatasource.cpp:82
#7 0x00007ffff4de6809 in OGRGeoRSSDataSource::~OGRGeoRSSDataSource (this=0x498ed70, __in_chrg=<optimized out>) at
ogrgeorssdatasource.cpp:85
#8 0x00007ffff40a7207 in QgsVectorFileWriter::~QgsVectorFileWriter (this=0x4e93950, __in_chrg=<optimized out>) at
/home/martin/qgis/git-master/src/core/qgsvectorfilewriter.cpp:1777
```

#3 - 2014-06-18 04:39 AM - Richard Duivenvoorde

but ogr/ogr2ogr seems ok?

I can happily create a georss file from given shp file with:

```
ogr2ogr -f GeoRSS output.xml -dsco USE_EXTENSIONS=YES poly4326.shp
```

(where poly4326.shp is a one polygon in epsg:4326)

Exact trying to save that shape in QGIS crashes it.

I thought to create an issue at GDAL, but I cannot reproduce it with ogr2ogr or so...

#4 - 2014-10-30 10:28 AM - Giovanni Manghi

still true on the latest master.

#5 - 2015-10-18 07:52 AM - Jürgen Fischer

- *Status changed from Open to Closed*

Fixed in changeset commit:"cee63c84f7f85586ddcb5348e70a0af0b1bcd5e".