

QGIS Application - Bug report #7180

Opening a project crashes QGIS

2013-02-19 01:46 AM - Paolo Cavallini

Status:	Closed	
Priority:	Severe/Regression	
Assignee:		
Category:	Project Loading/Saving	
Affected QGIS version:	master	Regression?: No
Operating System:		Easy fix?: No
Pull Request or Patch supplied:	No	Resolution:
Crashes QGIS or corrupts data:	Yes	Copied to github as #: 16231
Description		
The attached project causes QGIS to crash. Tested on several machines, several versions of QGIS (including 1.8 and current master), on Debian unstable and Windows.		

Associated revisions

Revision a4036486 - 2013-06-30 05:51 PM - Jürgen Fischer

grass provider: don't close invalid layers (fixes #7180)

History

#1 - 2013-02-19 01:47 AM - Paolo Cavallini

- File seravezza.qgs.zip added

#2 - 2013-02-19 02:12 AM - Paolo Cavallini

The culprit is the layer:

```
<maplayer minimumScale="0" maximumScale="1e+08" geometry="Polygon"
type="vector" hasScaleBasedVisibilityFlag="0">
  <id>pippo20130124131158937</id>
  <datasource>../Gis_AdB/Rischio_alluvione/mappe/pippo/1_polygon</datasource>
  <title></title>
  <abstract></abstract>
  <layername>pippo</layername>
  <srs>
    <spatialrefsys>
      <proj4>+proj=tmerc +lat_0=0 +lon_0=9 +k=0.9996
+x_0=1500000 +y_0=0 +ellps=intl
+towgs84=-104.1,-49.1,-9.9,0.971,-2.917,0.714,-11.68 +units=m
+no_defs</proj4>
      <srsid>968</srsid>
      <srid>3003</srid>
      <authid>EPSG:3003</authid>
      <description>Monte Mario / Italy zone 1</description>
      <projectionacronym>tmerc</projectionacronym>
      <ellipsoidacronym>intl</ellipsoidacronym>
      <geographicflag>>false</geographicflag>
    </spatialrefsys>
```

```

</srs>
<transparencyLevelInt>255</transparencyLevelInt>
<provider encoding="System">grass</provider>
<vectorjoins/>
<renderer-v2 symbollevels="0" type="singleSymbol">
  <symbols>
    <symbol outputUnit="MM" alpha="1" type="fill" name="0">
      <layer pass="0" class="SimpleFill" locked="0">
        <prop k="color" v="157,62,79,255"/>
        <prop k="color_border" v="0,0,0,255"/>
        <prop k="offset" v="0,0"/>
        <prop k="style" v="solid"/>
        <prop k="style_border" v="solid"/>
        <prop k="width_border" v="0.26"/>
      </layer>
    </symbol>
  </symbols>
  <rotation field=""/>
  <sizescale field=""/>
  <scalemethod="area"/>
</renderer-v2>
<customproperties/>
<displayfield>id</displayfield>
<label>0</label>
<labelattributes>
  <label fieldname="" text="Etichetta"/>
  <family fieldname="" name="MS Shell Dlg 2"/>
  <size fieldname="" units="pt" value="12"/>
  <bold fieldname="" on="0"/>
  <italic fieldname="" on="0"/>
  <underline fieldname="" on="0"/>
  <strikeout fieldname="" on="0"/>
  <color fieldname="" red="0" blue="0" green="0"/>
  <x fieldname=""/>
  <y fieldname=""/>
  <offset x="0" y="0" units="pt" yfieldname="" xfieldname=""/>
  <angle fieldname="" value="0" auto="0"/>
  <alignment fieldname="" value="center"/>
  <buffercolor fieldname="" red="255" blue="255" green="255"/>
  <bufferize fieldname="" units="pt" value="1"/>
  <bufferenabled fieldname="" on=""/>
  <multilineenabled fieldname="" on=""/>
  <selectedonly on=""/>
</labelattributes>
<editform>.</editform>
<editforminit></editforminit>
<annotationform>.</annotationform>
<editorlayout>generatedlayout</editorlayout>
<excludeAttributesWMS/>
<excludeAttributesWFS/>
<attributeactions/>
</maplayer>

```

#3 - 2013-02-21 12:24 AM - Giovanni Manghi

- Status changed from Open to Feedback

does it happen with the latest master?

#4 - 2013-06-02 07:45 AM - Giovanni Manghi

- Status changed from Feedback to Open
- Crashes QGIS or corrupts data changed from No to Yes
- Priority changed from High to Severe/Regression

still true

gio@sibirica ~ \$ qgis

Warning: loading of qt translation failed [/usr/share/qt4/translations/qt_en_US]

ERROR 4: 'X:/cartografie/q25_bn/0962.tif' does not exist in the file system,
and is not recognised as a supported dataset name.

ERROR 4: 'X:/cartografie/q25_bn/1041.tif' does not exist in the file system,
and is not recognised as a supported dataset name.

ERROR 4: 'M:/cartografia/raster/ctr/10000/da vettoriale/249090.TIF' does not exist in the file system,
and is not recognised as a supported dataset name.

ERROR 4: 'M:/cartografia/raster/ctr/10000/da vettoriale/249100.TIF' does not exist in the file system,
and is not recognised as a supported dataset name.

ERROR 4: 'M:/cartografia/raster/ctr/10000/da vettoriale/249130.TIF' does not exist in the file system,
and is not recognised as a supported dataset name.

ERROR 4: 'M:/cartografia/raster/ctr/10000/da vettoriale/249140.TIF' does not exist in the file system,
and is not recognised as a supported dataset name.

ERROR 4: 'M:/B.T.N/cartografia/ctr10k/RASTER/btn/260040.TIF' does not exist in the file system,
and is not recognised as a supported dataset name.

ERROR 4: 'M:/B.T.N/cartografia/ctr10k/RASTER/btn/261010.TIF' does not exist in the file system,
and is not recognised as a supported dataset name.

ERROR 10: Pointer 'hDS' is NULL in 'OGR_DS_Destroy'.

ERROR 10: Pointer 'hDS' is NULL in 'OGR_DS_Destroy'.

ERROR 10: Pointer 'hDS' is NULL in 'OGR_DS_Destroy'.

ERROR 10: Pointer 'hDS' is NULL in 'OGR_DS_Destroy'.

ERROR 10: Pointer 'hDS' is NULL in 'OGR_DS_Destroy'.

ERROR 10: Pointer 'hDS' is NULL in 'OGR_DS_Destroy'.

ERROR 10: Pointer 'hDS' is NULL in 'OGR_DS_Destroy'.

access: No such file or directory

Fatal: QGIS died on signal 11

Stacktrace (run through c++filt):

```
/usr/bin/qgis.bin(myMessageOutput(QtMsgType, char const*)+0xac)[0x4e6b5c]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(qt_message_output(QtMsgType, char const*)+0x2e)[0x7fde72b8a41e]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(+0x718bf)[0x7fde72b8a8bf]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(qFatal(char const*, ...)+0x94)[0x7fde72b8aa64]
/lib/x86_64-linux-gnu/libc.so.6(+0x364a0)[0x7fde7007b4a0]
/usr/lib/libqgisgrass.so.1.9.0(QgsGrassProvider::closeLayer(int)+0x23)[0x7fde4f73ff63]
/usr/lib/libqgisgrass.so.1.9.0(QgsGrassProvider::~QgsGrassProvider()+0x33)[0x7fde4f740133]
/usr/lib/libqgisgrass.so.1.9.0(QgsGrassProvider::~QgsGrassProvider()+0x9)[0x7fde4f7402a9]
/usr/lib/libqgis_core.so.1.9.0(QgsVectorLayer::~QgsVectorLayer()+0x37)[0x7fde73ceff87]
/usr/lib/libqgis_core.so.1.9.0(QgsVectorLayer::~QgsVectorLayer()+0x9)[0x7fde73cf0669]
/usr/lib/libqgis_core.so.1.9.0(QgsProject::addLayer(QDomElement const&, QList<QDomNode>&, QList<QPair<QgsVectorLayer*, QDomElement> >&)+0x1bb)[0x7fde73ca1a3b]
/usr/lib/libqgis_core.so.1.9.0(QgsProject::_getMapLayers(QDomDocument const&)+0x570)[0x7fde73ca4ef0]
/usr/lib/libqgis_core.so.1.9.0(QgsProject::read()+0xb69)[0x7fde73ca5f09]
/usr/lib/libqgis_core.so.1.9.0(QgsProject::read(QFileInfo const&)+0x3b)[0x7fde73ca6a7b]
/usr/bin/qgis.bin(QgisApp::addProject(QString)+0x12f)[0x51a74f]
/usr/bin/qgis.bin(QgisApp::fileOpen()+0x281)[0x51cf21]
/usr/bin/qgis.bin[0x7b9bba]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QMetaObject::activate(QObject*, QMetaObject const*, int, void**)+0x2b1)[0x7fde72ca8281]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QAction::triggered(bool)+0x32)[0x7fde72010132]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QAction::activate(QAction::ActionEvent)+0x6f)[0x7fde7201031f]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x59ad4a)[0x7fde723e5d4a]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QAbstractButton::mouseReleaseEvent(QMouseEvent*)+0x8c)[0x7fde723e5ffc]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QToolButton::mouseReleaseEvent(QMouseEvent*)+0xa)[0x7fde724a35da]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QWidget::event(QEvent*)+0x684)[0x7fde72067144]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QApplicationPrivate::notify_helper(QObject*, QEvent*)+0xb4)[0x7fde72016894]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QApplication::notify(QObject*, QEvent*)+0xabf)[0x7fde7201c0bf]
/usr/lib/libqgis_core.so.1.9.0(QgsApplication::notify(QObject*, QEvent*)+0x96)[0x7fde73ba0c46]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QCoreApplication::notifyInternal(QObject*, QEvent*)+0x8c)[0x7fde72c93e9c]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget*, QWidget**, QPointer<QWidget>&, bool)+0x172)[0x7fde72017862]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x24bbf5)[0x7fde72096bf5]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QApplication::x11ProcessEvent(_XEvent*)+0xdce)[0x7fde72095bae]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x2740d2)[0x7fde720bf0d2]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_dispatch+0x133)[0x7fde6eba7d53]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(+0x480a0)[0x7fde6eba80a0]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_iteration+0x34)[0x7fde6eba8164]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)+0x6f)[0x7fde72cc33bf]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x273d5e)[0x7fde720bed5e]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)+0x32)[0x7fde72c92c82]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>)+0xf7)[0x7fde72c92ed7]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QCoreApplication::exec()+0x87)[0x7fde72c97f67]
/usr/bin/qgis.bin(main+0x229e)[0x4e2b0e]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xed)[0x7fde7006676d]
/usr/bin/qgis.bin[0x4e6901]
Aborted (core dumped)
gio@sibirica ~ $
```

Still confirmed here

removing the layer as suggested by Paolo the prj is loaded properly !

Stacktrace:

```
Program received signal SIGSEGV, Segmentation fault.
0x00007ffffd73f5539 in QgsGrassProvider::closeLayer (layerId=-1)
    at /home/sam/pacchetti_gis/Quantum-GIS/src/providers/grass/qgsgrassprovider.cpp:680
680   QgsDebugMsg( QString( "Close layer %1 nUsers = %2" ).arg( layerId ).arg( mLayers[layerId].nUsers ) );
(gdb) bt full
#0 0x00007ffffd73f5539 in QgsGrassProvider::closeLayer (layerId=-1)
    at /home/sam/pacchetti_gis/Quantum-GIS/src/providers/grass/qgsgrassprovider.cpp:680
    __FUNCTION__ = "closeLayer"
#1 0x00007ffffd73f2472 in QgsGrassProvider::~QgsGrassProvider (this=0x5bdf6c0,
    __in_chrg=<optimized out>)
    at /home/sam/pacchetti_gis/Quantum-GIS/src/providers/grass/qgsgrassprovider.cpp:267
No locals.
#2 0x00007ffffd73f25ee in QgsGrassProvider::~QgsGrassProvider (this=0x5bdf6c0,
    __in_chrg=<optimized out>)
    at /home/sam/pacchetti_gis/Quantum-GIS/src/providers/grass/qgsgrassprovider.cpp:268
No locals.
#3 0x00007ffff4a64376 in QgsVectorLayer::~QgsVectorLayer (this=0x5bdb6c0,
    __in_chrg=<optimized out>)
    at /home/sam/pacchetti_gis/Quantum-GIS/src/core/qgsvectorlayer.cpp:195
    overlayIt = {i = 0x7fffffb1b0}
#4 0x00007ffff4a649b8 in QgsVectorLayer::~QgsVectorLayer (this=0x5bdb6c0,
    __in_chrg=<optimized out>)
    at /home/sam/pacchetti_gis/Quantum-GIS/src/core/qgsvectorlayer.cpp:213
No locals.
#5 0x00007ffff4a18656 in QgsProject::addLayer (this=0x123fa80, layerElem=..., brokenNodes=...,
    vectorLayerList=...) at /home/sam/pacchetti_gis/Quantum-GIS/src/core/qgsproject.cpp:767
    type = {static null = {<No data fields>}, static shared_null = {ref = {_q_value = 56639},
    alloc = 0, size = 0, data = 0xe0749a, clean = 0, simpletext = 0, righttoleft = 0,
    ---Type <return> to continue, or q <return> to quit---
    asciiCache = 0, capacity = 0, reserved = 0, array = {0}}, static shared_empty = {
    ref = {_q_value = 1099}, alloc = 0, size = 0, data = 0x7fff38368da, clean = 0,
    simpletext = 0, righttoleft = 0, asciiCache = 0, capacity = 0, reserved = 0, array = {
    0}}, d = 0x579f230, static codecForCStrings = 0x0}
    __FUNCTION__ = "addLayer"
    mapLayer = 0x5bdb6c0
#6 0x00007ffff4a17d67 in QgsProject::_getMapLayers (this=0x123fa80, doc=...)
    at /home/sam/pacchetti_gis/Quantum-GIS/src/core/qgsproject.cpp:699
    node = {impl = 0x579f3e0}
    element = {<QDomNode> = {impl = 0x579f3e0}, <No data fields>}
    name = {static null = {<No data fields>}, static shared_null = {ref = {_q_value = 56639},
    alloc = 0, size = 0, data = 0xe0749a, clean = 0, simpletext = 0, righttoleft = 0,
    asciiCache = 0, capacity = 0, reserved = 0, array = {0}}, static shared_empty = {
    ref = {_q_value = 1099}, alloc = 0, size = 0, data = 0x7fff38368da, clean = 0,
    simpletext = 0, righttoleft = 0, asciiCache = 0, capacity = 0, reserved = 0, array = {
```

```
0}}, d = 0x5bdd750, static codecForCStrings = 0x0}
i = 19
nl = {impl = 0x53fcf90}
wk = {static null = {<No data fields>}, static shared_null = {ref = {_q_value = 56639},
  alloc = 0, size = 0, data = 0xe0749a, clean = 0, simpletext = 0, righttoleft = 0,
  asciiCache = 0, capacity = 0, reserved = 0, array = {0}}, static shared_empty = {
  ref = {_q_value = 1099}, alloc = 0, size = 0, data = 0x7fff38368da, clean = 0,
  simpletext = 0, righttoleft = 0, asciiCache = 0, capacity = 0, reserved = 0, array = {
```

#6 - 2013-06-30 08:51 AM - Jürgen Fischer
- *Status changed from Open to Closed*

Fixed in changeset commit:"a40364866ea41cd6b4cfed5064d2004eee2fa921".

Files			
seravezza.qgs.zip	10.2 KB	2013-02-19	Paolo Cavallini