

QGIS Application - Bug report #13781

Segfault on adding TopoGeometry column

2015-11-06 09:11 AM - Sandro Santilli

Status:	Closed	
Priority:	High	
Assignee:	Sandro Santilli	
Category:		
Affected QGIS version:	2.8.3	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 #: 21807
Description		
I'm not sure exactly what triggered this, anyway, here's a backtrace: <pre>(gdb) bt #0 0x00007f6eef97b8c8 in QgsPostgresConn::PQstatus (this=0x0) at /usr/src/qgis/qgis-2.8/src/providers/postgres/qgspostgresconn.cpp:1050 #1 0x00007f6eef9798c1 in QgsPostgresConn::PQexec (this=0x0, query=..., logError=true) at /usr/src/qgis/qgis-2.8/src/providers/postgres/qgspostgresconn.cpp:869 #2 0x00007f6eef95ae94 in QgsPostgresProvider::extent (this=0x6b9f570) at /usr/src/qgis/qgis-2.8/src/providers/postgres/qgspostgresprovider.cpp:2467 #3 0x00007f6f76082669 in QgsVectorLayer::extent (this=0x581fc00) at /usr/src/qgis/qgis-2.8/src/core/qgsvectorlayer.cpp:823 #4 0x00007f6f75fa2b66 in QgsMapRenderer::updateFullExtent (this=0x2d95be0) at /usr/src/qgis/qgis-2.8/src/core/qgsmaprender.cpp:950 #5 0x00007f6f75fa3356 in QgsMapRenderer::setLayerSet (this=0x2d95be0, layers=...) at /usr/src/qgis/qgis-2.8/src/core/qgsmaprender.cpp:1006 #6 0x00007f6f75667350 in QgsMapCanvasRendererSync::onLayersC2R (this=0x2958b00) at /usr/src/qgis/qgis-2.8/src/gui/qgsmapcanvas.cpp:179 #7 0x00007f6f756fb1c3 in QgsMapCanvasRendererSync::qt_static_metacall (_o=0x2958b00, _c=QMetaObject::InvokeMetaMethod, _id=10, _a=0x7ffec18b200) at /usr/src/qgis/build/2.8/src/gui/moc_qgsmapcanvas.cxx:400 #8 0x00007f6f74a0687a in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4 #9 0x00007f6f756fad8f in QgsMapCanvas::layersChanged (this=0x2d7de20) at /usr/src/qgis/build/2.8/src/gui/moc_qgsmapcanvas.cxx:269 #10 0x00007f6f75668485 in QgsMapCanvas::setLayerSet (this=0x2d7de20, layers=...) at /usr/src/qgis/qgis-2.8/src/gui/qgsmapcanvas.cpp:448 #11 0x00007f6f755bc5aa in QgsLayerTreeMapCanvasBridge::setCanvasLayers (this=0x2ec5f80) at /usr/src/qgis/qgis-2.8/src/gui/layertree/qgslayertreemapcanvasbridge.cpp:158 #12 0x00007f6f7571470d in QgsLayerTreeMapCanvasBridge::qt_static_metacall (_o=0x2ec5f80, _c=QMetaObject::InvokeMetaMethod, _id=4, _a=0x67db010) at /usr/src/qgis/build/2.8/src/gui/layertree/moc_qgslayertreemapcanvasbridge.cxx:74 #13 0x00007f6f74a0ac1e in QObject::event(QEvent*) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4 #14 0x00007f6f73d8be2c in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4 #15 0x00007f6f73d924a0 in QApplication::notify(QObject*, QEvent*) () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4 #16 0x00007f6f75ea6223 in QgsApplication::notify (this=0x7ffec18c390, receiver=0x2ec5f80, event=0x67daf00) at /usr/src/qgis/qgis-2.8/src/core/qgsapplication.cpp:252 #17 0x00007f6f749f24dd in QCoreApplication::notifyInternal(QObject*, QEvent*) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4 #18 0x00007f6f749f5b3d in QCoreApplicationPrivate::sendPostedEvents(QObject*, int, QThreadData*) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4 #19 0x00007f6f74a1ff83 in ?? () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4</pre>		

```
#20 0x00007f6f6f16de04 in g_main_context_dispatch () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#21 0x00007f6f6f16e048 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#22 0x00007f6f6f16e0ec in g_main_context_iteration () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
```

Associated revisions

Revision 54cf972a - 2015-11-06 09:37 PM - Sandro Santilli

Properly set invalid topology layer as invalid

Fixes #13781 (crash)

Revision 65fb72a9 - 2015-11-06 10:45 PM - Sandro Santilli

Properly set invalid topology layer as invalid

Fixes #13781 (crash)

(cherry-picked from 54cf972ac2334451e69d2171cc4f3e42da3880df)

History

#1 - 2015-11-06 09:12 AM - Sandro Santilli

- Assignee set to Sandro Santilli

It's actually easy to reproduce for me. Just start qgis, select a TopoGeometry column (not registered in topology.layer) and "Add" --> crash.

#2 - 2015-11-06 09:14 AM - Sandro Santilli

I don't know if this could be related:

```
src/providers/postgres/qgspostgresconn.cpp: 903: (PQexec) [0ms] Not logged erroneous query: SELECT styleQML FROM layer_styles WHERE
f_table_catalog
='nibio_test' AND f_table_schema='public' AND f_table_name='testing' AND f_geometry_column='tg' ORDER BY CASE WHEN useAsDefault THEN 1
ELSE 2 END,u
pdate_time DESC LIMIT 1 returned 7 [ERROR: relation "layer_styles" does not exist
LINE 1: SELECT styleQML FROM layer_styles WHERE f_table_catalog='nib...
      ^
]
```

#3 - 2015-11-06 09:21 AM - Jürgen Fischer

- Status changed from Open to Feedback

#4 - 2015-11-06 09:34 AM - Giovanni Manghi

- Priority changed from Normal to High

#5 - 2015-11-06 10:15 AM - Sandro Santilli

To reproduce:

```
createdb bug13781
psql bug13781 <<EOF
create extension postgis;
create extension postgis_topology;
select createtopology('t');
create table t(id serial primary key);
select addtopogeometrycolumn('t','public','t','tg','point');
create table t2(id serial primary key, tg TopoGeometry);
insert into t2(tg) values ( (1,1,1,1) );
EOF
```

Then start qgis, Add PostGIS Layer, select public.t2, "Add".

#6 - 2015-11-06 10:42 AM - Sandro Santilli

NOTE: I've tested the crash to also happen with master branch from some weeks ago (commit:a0a44f2)

#7 - 2015-11-06 11:26 AM - Sandro Santilli

Debug log seems interesting:

```
src/providers/postgres/qgspgtablemodel.cpp: 379: (layerURI) [16593ms] returning uri dbname='bug13781' port=5493 sslmode=disable key="" srid=0
type=MultiPoint table="public"."t2" (tg) sql=
src/core/qgsmaplayer.cpp: 66: (QgsMapLayer) [1ms] original name: 't2'
src/core/qgsmaplayer.cpp: 68: (QgsMapLayer) [0ms] display name: 't2'
src/core/qgsvectorlayer.cpp: 585: (geometryType) [1ms] invalid layer or pointer to mDataProvider is null
src/core/qgsvectorlayer.cpp: 593: (geometryType) [0ms] WARNING: This code should never be reached. Problems may occur...
```

#8 - 2015-11-06 12:31 PM - Sandro Santilli

I see that QgsPostgresProvider::QgsPostgresProvider has lots of early returns. The crash happens because a QgsPostgresProvider does not have an associated connection (possibly due to these early returns).

Another bit of the output log shows this is a case of early return:

```
src/providers/postgres/qgspostgresprovider.cpp: 2847: (getGeometryDetails) [0ms] Spatial column type is TopoGeometry
src/core/qgsmessageolog.cpp: 45: (logMessage) [1ms] 2015-11-06T21:29:32 PostGIS: Could not find topology of layer 'public'.t2.tg'
src/core/qgsmessageolog.cpp: 45: (logMessage) [0ms] 2015-11-06T21:29:32 PostGIS: invalid PostgreSQL topology layer
src/core/qgsproviderregistry.cpp: 370: (provider) [0ms] Instantiated the data provider plugin: postgres
src/core/qgsvectorlayer.cpp: 1378: (setDataProvider) [0ms] Instantiated the data provider plugin
```

#9 - 2015-11-06 12:31 PM - Sandro Santilli

Should a failed construction throw an exception rather than building partially ?

#10 - 2015-11-06 12:34 PM - Sandro Santilli

Found the issue: while mValid member is initialized to false, the call to QgsPostgresProvider::getGeometryDetails() sets it to true, then the "invalid PostgreSQL topology layer" condition fails to set it back to false

#11 - 2015-11-06 12:36 PM - Sandro Santilli

- Status changed from Feedback to In Progress

Confirmed, setting mValid=false when disconnecting the DB fixes this crash.

Should I provide a testcase for this ? Would it be "easy" to do in 2.8 branch ?

#12 - 2015-11-06 12:39 PM - Sandro Santilli

- Status changed from In Progress to Closed

Fixed in changeset commit:"54cf972ac2334451e69d2171cc4f3e42da3880df".

#13 - 2015-11-06 01:19 PM - Sandro Santilli

- Status changed from Closed to Reopened

Still needs to be fixed in trunk

#14 - 2015-11-06 02:27 PM - Sandro Santilli

- Status changed from Reopened to Closed

Fixed in changeset commit:"65fb72a958c0d0cb0edce9c974cb6b2720d483b4".