

QGIS Application - Bug report #12771

error Segmentation fault

2015-05-19 03:42 AM - reiko fuerst

Status: Closed	
Priority: High	
Assignee:	
Category: Data Provider/SpatialLite	
Affected QGIS version: 2.8.2	Regression?: No
Operating System:	Easy fix?: No
Pull Request or Patch supplied: No	Resolution:
Crashes QGIS or corrupts data: Yes	Copied to github as #: 20870
Description	
<p>Hi evrybody,</p> <p>since a view days qgis (after an update) crashes when open a sqlite database.</p> <p>message: src/core/qgsproviderregistry.cpp: 368: (provider) [0ms] Library name is /usr/lib/qgis/plugins/libspatialiteprovider.so Segmentation fault</p> <p>qgis version 2.9.0-master qt 4.8.7 spatialite-version 4.1.1 debian unstable</p> <p>also tested with the qgis version 2.8.2, same result.</p> <p>is there a solution or workaround to fix that?</p> <p>thanks a lot in advance</p>	

Associated revisions

Revision 252aaab8 - 2015-05-26 02:36 PM - Jürgen Fischer

adopt 'new' spatialite initialization scheme via thin wrapper around sqlite3_open and sqlite3_close (fixes #12771)

Revision d7ca1902 - 2015-05-28 12:11 AM - Jürgen Fischer

adopt 'new' spatialite initialization scheme via thin wrapper around sqlite3_open and sqlite3_close (fixes #12771)

(cherry picked from commit 252aaab, 23ef9da, d4b72a2, c7cb963 and e255d6c)

History

#1 - 2015-05-19 04:04 AM - Paolo Cavallini

- Status changed from Open to Rejected
- Resolution set to up/downstream

Problem with Debian packaging. They are aware of it, going to fix, hopefully soon.

#2 - 2015-05-24 03:02 AM - Bas Couwenberg

This issue should be reopened, because qgsspatialiteprovider.cpp uses the deprecated spatialite_init() method causing the segfault.

The spatialite code in QGIS needs to be ported to use the spatialite_init_ex() method instead:

```
python/ext-libs/pyspatialite/src/connection.h:36:// int spatialite_init(int verbose);
python/ext-libs/pyspatialite/src/connection.c:84: spatialite_init(0);
src/providers/spatialite/qspatialite/qsqldb_connection.cpp:551: spatialite_init(0);
src/providers/spatialite/qspatialite/README:4:spatialite_init(0).
src/providers/spatialite/qgsspatialiteprovider.cpp:136: spatialite_init( 0 );
src/providers/spatialite/qgsspatialiteprovider.cpp:442: spatialite_init( 0 );
src/providers/spatialite/qgsspatialiteprovider.cpp:5061: spatialite_init( 0 );
src/providers/spatialite/qgsspatialiteprovider.cpp:5096: spatialite_init( 0 );
src/providers/spatialite/qgsspatialiteprovider.cpp:5177: spatialite_init( 0 );
src/providers/spatialite/qgsspatialiteprovider.cpp:5367: spatialite_init( 0 );
src/providers/spatialite/qgsspatialiteprovider.cpp:5423: spatialite_init( 0 );
src/providers/spatialite/qgsspatialiteprovider.cpp:5536: spatialite_init( 0 );
src/providers/spatialite/qgsspatialiteconnection.cpp:142: spatialite_init( 0 );
src/app/qgsnewspatialitelayerdialog.cpp:384: spatialite_init( 0 );
src/core/qgsofflineediting.cpp:77: spatialite_init( 0 );
src/core/qgsofflineediting.cpp:383: spatialite_init( 0 );
src/analysis/openstreetmap/qgsosmimport.cpp:61: spatialite_init( 0 );
src/analysis/openstreetmap/qgsosmdatabase.cpp:53: spatialite_init( 0 );
```

Since QGIS is the most significant user of pyspatialite and its upstream development has stopped, updating the embedded pyspatialite copy in qgis to fix [pyspatialite issue 24](#) seems the most promising road towards a solution.

See also the comments by Sandro on [qgis-developer](#) about porting QGIS to use spatialite_init_ex() instead.

The spatialite_init() method is highly unlikely to be fixed in Debian and upstream, all software built on top of libspatialite needs to be adapted to use spatialite_init_ex(). GDAL did this in 1.11.x, qgis and pyspatialite both don't (yet).

#3 - 2015-05-24 03:49 AM - Giovanni Manghi

- OS version deleted (unstable)
- Operating System deleted (debian)
- Category changed from Browser to Data Provider/Spatialite
- Status changed from Rejected to Reopened
- Crashes QGIS or corrupts data changed from No to Yes
- Resolution deleted (up/downstream)

#4 - 2015-05-26 05:37 AM - Jürgen Fischer

- Status changed from Reopened to Closed

Fixed in changeset commit:"252aaab89e5701d1d7c0ec147ce02c8865ffa452".

