

## QGIS Application - Bug report #16685

### QgsSpatialLiteProvider::loadFieldsAbstractInterface trying to assign default values to non-existent fields

2017-06-08 11:11 AM - Juliusz Hoffman

|                                        |                           |                                     |
|----------------------------------------|---------------------------|-------------------------------------|
| <b>Status:</b>                         | Closed                    |                                     |
| <b>Priority:</b>                       | High                      |                                     |
| <b>Assignee:</b>                       |                           |                                     |
| <b>Category:</b>                       | Data Provider/SpatialLite |                                     |
| <b>Affected QGIS version:</b>          | master                    | <b>Regression?:</b> Yes             |
| <b>Operating System:</b>               | Ubuntu 16.04 LTS          | <b>Easy fix?:</b> Yes               |
| <b>Pull Request or Patch supplied:</b> |                           | <b>Resolution:</b>                  |
| <b>Crashes QGIS or corrupts data:</b>  |                           | <b>Copied to github as #:</b> 24584 |

#### Description

I have encountered a core dump while working with spatialite layers with latest master  
commit:e052933b1452b5e45715c1a71f62be9d49ffe0d9

```
#0 __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:58
#1 0x00007ffff30bc37a in __GI_abort () at abort.c:89
#2 0x0000555555555d7c1 in qgisCrash (signal=-1) at /home/migra/nt1/src/QGIS/src/app/main.cpp:329
#3 0x0000555555555da6a in myMessageOutput (type=QtFatalMsg, msg=0x555555e45878 "ASSERT failure in
QVector<T>::operator[]: \"index out of range\", file /usr/include/x86_64-linux-gnu/qt5/QtCore/qvector.h, line 433")
    at /home/migra/nt1/src/QGIS/src/app/main.cpp:382
#4 0x00007ffff3a7c99d in ?? () from /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#5 0x00007ffff3a7e439 in QMessageLogger::fatal(char const*, ...) const () from /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#6 0x00007ffff3a79981 in qt_assert_x(char const*, char const*, char const*, int) () from /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#7 0x00007ffff565c78b in QVector<QgsFields::Field>::operator[] (this=0x555555c79b68, i=5) at
/usr/include/x86_64-linux-gnu/qt5/QtCore/qvector.h:433
#8 0x00007ffff565abe4 in QgsFields::at (this=0x555557fb02e8, i=5) at /home/migra/nt1/src/QGIS/src/core/qgsfields.cpp:137
#9 0x00007ffff6175b8b2 in QgsSpatialLiteProvider::insertDefaultValue (this=0x555557fb0260, fieldIndex=5, defaultVal=...) at
/home/migra/nt1/src/QGIS/src/providers/spatialite/qgsspatialiteprovider.cpp:890
#10 0x00007ffff6175a2eb in QgsSpatialLiteProvider::loadFieldsAbstractInterface (this=0x555557fb0260, lyr=0x555555e6daf0) at
/home/migra/nt1/src/QGIS/src/providers/spatialite/qgsspatialiteprovider.cpp:735
#11 0x00007ffff617587a9 in QgsSpatialLiteProvider::QgsSpatialLiteProvider (this=0x555557fb0260, uri=...) at
/home/migra/nt1/src/QGIS/src/providers/spatialite/qgsspatialiteprovider.cpp:568
#12 0x00007ffff6176e0eb in classFactory (uri=0x555556590fe8) at
/home/migra/nt1/src/QGIS/src/providers/spatialite/qgsspatialiteprovider.cpp:5244
#13 0x00007ffff57c3573 in QgsProviderRegistry::createProvider (this=0x555556acb340, providerKey=..., dataSource=...) at
/home/migra/nt1/src/QGIS/src/core/qgsproviderregistry.cpp:411
#14 0x00007ffff5872dfa in QgsVectorLayer::setDataProvider (this=0x555556590fb0, provider=...) at
/home/migra/nt1/src/QGIS/src/core/qgsvectorlayer.cpp:1480
#15 0x00007ffff5872b38 in QgsVectorLayer::setDataSource (this=0x555556590fb0, dataSource=..., baseName=..., provider=...,
loadDefaultStyleFlag=false) at /home/migra/nt1/src/QGIS/src/core/qgsvectorlayer.cpp:1439
#16 0x00007ffff586a9b9 in QgsVectorLayer::QgsVectorLayer (this=0x555556590fb0, vectorLayerPath=..., baseName=...,
providerKey=..., loadDefaultStyleFlag=false) at /home/migra/nt1/src/QGIS/src/core/qgsvectorlayer.cpp:167
#17 0x00007ffff718d19e in QgisApp::addVectorLayer (this=0x555555d08020, vectorLayerPath=..., baseName=...,
providerKey=...) at /home/migra/nt1/src/QGIS/src/app/qgisapp.cpp:9741
```

It is caused by trying to assign default field values in QgsSpatialLiteProvider::loadFieldsAbstractInterface to the geometry column, which was skipped while creating fields.

Attached patch fixed this issue for me, but I am in no way familiar with the QGIS codebase so cannot guarantee this is the right approach.

## Associated revisions

**Revision f677eaf0 - 2017-06-09 08:15 AM - Juliusz Hoffman**

consider middle geometry column when retrieving default values (fixes #16685)

## History

**#1 - 2017-06-08 11:35 AM - Giovanni Manghi**

- *Status changed from Open to Feedback*

Please submit the patch as Pull Request on GitHub, chances of being seen and reviewed here in the bug tracker are very low.

**#2 - 2017-06-09 08:17 AM - Juliusz Hoffman**

- *% Done changed from 0 to 100*

- *Status changed from Feedback to Closed*

Applied in changeset commit:qgis|f677eaf04f73331b1ef5180b2f30018d5e1faa53.

## Files

|                                   |         |            |                 |
|-----------------------------------|---------|------------|-----------------|
| qgis-spatialite-provider-fix.diff | 1.21 KB | 2017-06-08 | Juliusz Hoffman |
|-----------------------------------|---------|------------|-----------------|