QGIS Application - Bug report #14212
output/bin/qgis_diagramtest segfaults

2016-02-02 01:33 AM - Sandro Santilli

Status:	Closed		
Priority:	Severe/Regression		
Assignee:	Sandro Santilli		
Category:	Data Provider/OGR		
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	Yes	**Resolution:**	fixed/implemented
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	22214

Description

Another case of segfault-on-exit

```
QDEBUG : TestQgsDiagram::cleanupTestCase() src/core/qgsproviderregistry.cpp: 237: (clean) [0ms] cleanup:spatialite
QDEBUG : TestQgsDiagram::cleanupTestCase() src/core/qgsproviderregistry.cpp: 237: (clean) [0ms] cleanup:virtual
QDEBUG : TestQgsDiagram::cleanupTestCase() src/core/qgsproviderregistry.cpp: 237: (clean) [0ms] cleanup:wcs
QDEBUG : TestQgsDiagram::cleanupTestCase() src/core/qgsproviderregistry.cpp: 237: (clean) [0ms] cleanup:wms
QDEBUG : TestQgsDiagram::cleanupTestCase() src/core/auth/qgsauthmethodregistry.cpp: 154: (~QgsAuthMethodRegistry)
[0ms] cleanup: Basic
QDEBUG : TestQgsDiagram::cleanupTestCase() src/core/auth/qgsauthmethodregistry.cpp: 154: (~QgsAuthMethodRegistry)
[0ms] cleanup: Identity-Cert
QDEBUG : TestQgsDiagram::cleanupTestCase() src/core/auth/qgsauthmethodregistry.cpp: 154: (~QgsAuthMethodRegistry)
[0ms] cleanup: PKI-PKCS#12
QDEBUG : TestQgsDiagram::cleanupTestCase() src/core/auth/qgsauthmethodregistry.cpp: 154: (~QgsAuthMethodRegistry)
[0ms] cleanup: PKI-Paths
QDEBUG : TestQgsDiagram::cleanupTestCase() src/core/qgsmaprenderercustompainterjob.cpp: 41:
(~QgsMapRendererCustomPainterJob) [1ms] QPAINTER destruct
QDEBUG : TestQgsDiagram::cleanupTestCase() src/core/qgsmaprenderercustompainterjob.cpp: 41:
(~QgsMapRendererCustomPainterJob) [0ms] QPAINTER destruct
QFATAL : TestQgsDiagram::cleanupTestCase() Received signal 11
FAIL!  : TestQgsDiagram::cleanupTestCase() Received a fatal error.
  Loc: [Unknown file(0)]
Totals: 3 passed, 1 failed, 0 skipped
********* Finished testing of TestQgsDiagram *********
Aborted (core dumped)
```

See also #14176

Last tested with commit:490236f2f2e02e4222f842ea144e8ea3968e63da

History

#1 - 2016-02-02 01:37 AM - Sandro Santilli

- Category changed from Authentication system to Data Provider/OGR

It actually seem to be the same issue of #14176 as this is valgrind finding:

```
==15933== Invalid read of size 8
```

==15933== at 0xC2D65A5: OGR_DS_Destroy (ogrdatasource.cpp:69)
==15933== by 0x2E1EB4A6: qgsConnectionPool_ConnectionDestroy(QgsOgrConn*) (qgsogrconnpool.h:45)
==15933== by 0x2E1EC2A5: QgsConnectionPoolGroup<QgsOgrConn*>::~QgsConnectionPoolGroup() (qgsconnectionpool.h:77)
==15933== by 0x2E1FDB0D: QgsOgrConnPoolGroup::~QgsOgrConnPoolGroup() (in /usr/src/qgis/build/0-master/output/lib/qgis/plugins/libogrprovider.so)
==15933== by 0x2E1FDB49: QgsOgrConnPoolGroup::~QgsOgrConnPoolGroup() (qgsogrconnpool.h:59)
==15933== by 0x2E1EB7E5: QgsOgrConnPool::unref(QString const&) (qgsogrconnpool.h:113)
==15933== by 0x2E1EB850: QgsOgrConnPool::unrefS(QString const&) (qgsogrconnpool.h:126)
==15933== by 0x2E1F88BB: QgsOgrFeatureSource::~QgsOgrFeatureSource() (qgsogrfeatureiterator.cpp:412)
==15933== by 0x2E1F8947: QgsOgrFeatureSource::~QgsOgrFeatureSource() (qgsogrfeatureiterator.cpp:413)
==15933== by 0x5AD4DF9: QgsVectorLayerFeatureSource::~QgsVectorLayerFeatureSource() (qgsvectorlayerfeatureiterator.cpp:79)
==15933== by 0x5AD4EA9: QgsVectorLayerFeatureSource::~QgsVectorLayerFeatureSource() (qgsvectorlayerfeatureiterator.cpp:80)
==15933== by 0x5AC8741: QgsVectorLayerDiagramProvider::~QgsVectorLayerDiagramProvider() (qgsvectorlayerdiagramprovider.cpp:74)
==15933== Address 0x31965110 is 0 bytes inside a block of size 280 free'd
==15933== at 0x4C2C131: operator delete(void*) (vg_replace_malloc.c:510)
==15933== by 0xC080FF5: GDALDriverManager::~GDALDriverManager() (gdaldrivermanager.cpp:183)
==15933== by 0xC081158: GDALDriverManager::~GDALDriverManager() (gdaldrivermanager.cpp:289)
==15933== by 0x2B979B4D: cleanupProvider (qgsgdalprovider.cpp:3024)
==15933== by 0x5A5A0F1: QgsProviderRegistry::clean() (qgsproviderregistry.cpp:244)
==15933== by 0x5A5A205: QgsProviderRegistry::~QgsProviderRegistry() (qgsproviderregistry.cpp:253)
==15933== by 0x5A5A2A5: QgsProviderRegistry::~QgsProviderRegistry() (qgsproviderregistry.cpp:254)
==15933== by 0x5842EA2: QgsApplication::exitQgis() (qgsapplication.cpp:868)
==15933== by 0x409DC6: TestQgsDiagram::cleanupTestCase() (testqgsdiagram.cpp:115)
==15933== by 0x4084E7: TestQgsDiagram::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) (testqgsdiagram.moc:55)
==15933== by 0x4FBB907: QMetaMethod::invoke(QObject*, Qt::ConnectionType, QGenericReturnArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument) const (in /usr/lib/x86_64-linux-gnu/libQtCore.so.4.8.6)
==15933== by 0x532408E: ??? (in /usr/lib/x86_64-linux-gnu/libQtTest.so.4.8.6)

#2 - 2016-02-02 01:45 AM - Sandro Santilli

The ref/unref management in QgsOgrFeatureIterator is not clear to me, and surely doesn't seem to be RAII compliant.
What are ref/unref calls needed for ? I'd rather just drop them completely.

#3 - 2016-02-02 02:23 AM - Sandro Santilli

I confirm removing the ref / unref methods and calls fixes the crash.

#4 - 2016-02-02 02:24 AM - Sandro Santilli

Also, valgrind shows no additional leak

#5 - 2016-02-02 02:26 AM - Sandro Santilli

- Pull Request or Patch supplied changed from No to Yes

Patch for review: https://github.com/qgis/QGIS/pull/2755

#6 - 2016-02-02 09:28 AM - Sandro Santilli

The suggested fix in pull 2755 reverts changed meant to fix #13082 -- I'll look at that ticket to see if it breaks

#7 - 2016-02-02 09:35 AM - Sandro Santilli

Ticket #13082 does not break. The shapefile is closed some time after the layer is closed. This is based on an expiration time for connections in the now-centralized connection pool (it seems to be an hard-coded 60 seconds).

#8 - 2016-02-03 01:57 AM - Sandro Santilli

- Resolution set to fixed/implemented

- Status changed from In Progress to Closed

I cannot reproduce as of commit:b6c714ac20ea595ebf3136ae8facae0520acbe5f
Assuming fixed by commit:051253888810b06f6b055bfea57a7c6a009e3fdc