QGIS Application - Bug report #12755
QGIS intermittent crash since 2.8.1

2015-05-17 04:36 AM - Sean Lin

Status:	Closed		
Priority:	High		
Assignee:			
Category:			
Affected QGIS version:	2.8.2	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	not reproducable
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	20854

Description

The following stackdump happens intermittently but usually when I move a vector point to a new location.

```
FAULTING_IP:
QtSql4!QPSQLDriver::open+410
00000000`691a37d0 41ff93d0000000  call    qword ptr [r11+0D0h]

EXCEPTION_RECORD:  ffffffffffffffff -- (.exr 0xffffffffffffffff)
ExceptionAddress: 00000000691a37d0 (QtSql4!QPSQLDriver::open+0x0000000000000410)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 0000000000000000
   Parameter[1]: ffffffffffffffff
Attempt to read from address ffffffffffffffff

DEFAULT_BUCKET_ID:  INVALID_POINTER_READ

PROCESS_NAME:  qgis-rel-dev-bin.exe

ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%08lx referenced memory at 0x%08lx. The memory could not be %s.

EXCEPTION_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%08lx referenced memory at 0x%08lx. The memory could not be %s.

EXCEPTION_PARAMETER1:  0000000000000000

EXCEPTION_PARAMETER2:  ffffffffffffffff

READ_ADDRESS:  ffffffffffffffff

FOLLOWUP_IP:
QtSql4!QPSQLDriver::open+410
00000000`691a37d0 41ff93d0000000  call    qword ptr [r11+0D0h]

APPLICATION_VERIFIER_FLAGS:  0

FAULTING_THREAD:  000000000000125c
```

PRIMARY_PROBLEM_CLASS: INVALID_POINTER_READ

BUGCHECK_STR: APPLICATION_FAULT_INVALID_POINTER_READ

LAST_CONTROL_TRANSFER: from 0000000069193b0c to 00000000691a37d0

STACK_TEXT:
00000000`11eeddd0 00000000`69193b0c : 00000000`15164d80 00000000`691c8728 00000000`0d9eeb40
00000000`0daa5990 : QtSql4!QPSQLDriver::open+0x410
00000000`11eede60 00007ff8`7c357d8a : 00000000`11eedee8 00007ff8`7c35f88c 00007ff8`7c35f888 00000000`11eedf40 :
QtSql4!QSqlDatabase::open+0x3c
00000000`11eedeb0 00000000`1e0c20a9 : 00000000`0d9eeb40 00000000`06611048 00000000`1bbb29a0
00000000`1bbb29c0 : QtSql!initQtSql+0x25d0a
00000000`11eedf40 00000000`1e112524 : 00000000`00000000 00000000`0daa5990 00000000`0d295ec8 00000000`1e0c3aba
: python27!PyCFunction_Call+0x69
00000000`11eedf70 00000000`1e115cd4 : 00000000`00000000 00000000`00000083 00000000`0d295ec8 00000000`0000006a
: python27!PyEval_GetGlobals+0x944
00000000`11eedfd0 00000000`1e1174d9 : 00000000`0d9c8a48 ffffffff`ffe9e820 00000000`00000001 00000000`00000000 :
python27!PyEval_EvalFrameEx+0x36a4
00000000`11eee0c0 00000000`1e0b3ba3 : 00000000`0845b230 00000000`00000002 00000000`00000000
00000000`1e0a2846 : python27!PyEval_EvalCodeEx+0x7e9
00000000`11eee170 00000000`1e08bef5 : 00000000`0cdde908 00000000`0d8673c8 00000000`00000002 00000000`0d8673c8
: python27!PyFunction_SetClosure+0xa73
00000000`11eee200 00000000`1e09a421 : 00000000`0d8673c8 00000000`0cdde908 00000000`00000001
00000000`00000002 : python27!PyObject_Call+0x65
00000000`11eee230 00000000`1e08bef5 : 00000000`0d7931b0 00000000`07102390 00000000`00000000 00000000`1e09a2d0
: python27!PyMethod_New+0x911
00000000`11eee480 00000000`1e1109d8 : 00000000`07102390 00000000`07102390 00000000`0d7931b0
00000000`07102390 : python27!PyObject_Call+0x65
00000000`11eee4b0 00000000`1e09ad7c : 00000000`0d6074c8 00000000`0d7931b0 00000000`0dc7d4e0 00000000`1e0f5158
: python27!PyEval_CallObjectWithKeywords+0xc8
00000000`11eee4e0 00000000`1e08bef5 : 00000000`00000000 00000000`080bfd08 00000000`07102390 00000000`00000002
: python27!PyInstance_New+0x11c
00000000`11eee510 00000000`1e111d1b : 00000000`00000000 00000000`00000001 00000000`07102390 00000000`0672ff28
: python27!PyObject_Call+0x65
00000000`11eee540 00000000`1e1125ca : 00000000`00000001 00000000`00000000 00000000`080bfd08 00000000`11eee678
: python27!PyEval_GetGlobals+0x13b
00000000`11eee580 00000000`1e115cd4 : 00000000`00000000 00000000`00000083 00000000`0dc7d360
00000000`0000006a : python27!PyEval_GetGlobals+0x9ea
00000000`11eee5e0 00000000`1e110bd8 : 00000000`0d89c0f8 00000000`00000003 00000000`00000001 00000000`00000000
: python27!PyEval_EvalFrameEx+0x36a4
00000000`11eee6d0 00000000`1e1125b4 : 00000000`00000003 00000000`00000000 00000000`082eccf8 00000000`1e0c3a66
: python27!PyEval_GetFuncDesc+0x158
00000000`11eee740 00000000`1e115cd4 : 00000000`00000000 00000000`00000083 00000000`0dc68ea0
00000000`0000006a : python27!PyEval_GetGlobals+0x9d4
00000000`11eee7a0 00000000`1e1174d9 : 00000000`0d00f798 00000000`007a5150 00000000`00000001 00000000`00000000
: python27!PyEval_EvalFrameEx+0x36a4
00000000`11eee890 00000000`1e0b3ba3 : 00000000`06a72630 00000000`00000004 00000000`00000000 00000000`68f6465f
: python27!PyEval_EvalCodeEx+0x7e9
00000000`11eee940 00000000`1e08bef5 : 00000000`082ecf28 00000000`0d7b4a48 00000000`00000027 00000000`0d7b4a48
: python27!PyFunction_SetClosure+0xa73
00000000`11eee9d0 00000000`1e09a421 : 00000000`0d7b4a48 00000000`082ecf28 00000000`00000003 00000000`00000000
: python27!PyObject_Call+0x65

00000000`11eeea00 00000000`1e08bef5 : 00000000`080d9750 00000000`0d9ebc60 00000000`00000000 00000000`1e09a2d0 : python27!PyMethod_New+0x911
00000000`11eeec50 00000000`1e1109d8 : 00000000`0d9ebc60 00000000`11eeed18 00000000`080d9750 00000000`00000000 : python27!PyObject_Call+0x65
00000000`11eeec80 00007ff8`7d1fb9f0 : 00000000`080d9750 00000000`00000000 00000000`0d9ebc60 00007ff8`6f96c71c : python27!PyEval_CallObjectWithKeywords+0xc8
00000000`11eeecb0 00007ff8`6f85dbd4 : 00000000`1bbb2980 00000000`11eeee60 00007ff8`70032e88 00000000`1bbb2980 : sip!initsip+0x12e0
00000000`11eeed00 00007ff8`6fe170fc : 00000000`11eeee50 00000000`00000001 00000000`00000000 00000000`0842ae18 : _core!sipVH__core_227+0x124 [c:\\src\\qgis\\ms-windows\\osgeo4w\\build-nightly-x86_64\\python\\core\\sip_corepart0.cpp @ 8432]
00000000`11eeedb0 00007ff8`78188037 : 00000000`05bc8fb0 00000000`11eeee50 00000000`11eeee60 00000000`11eef270 : _core!sipQgsExpression_Function::func+0xdc
[c:\\src\\qgis\\ms-windows\\osgeo4w\\build-nightly-x86_64\\python\\core\\sip_corepart3.cpp @ 71919]
00000000`11eeee20 00007ff8`781820a8 : 00000000`17eefb70 00000000`11eef0f0 00000000`17af91e0 00000000`11eef270 : qgis_core!QgsExpression::NodeFunction::eval+0x727 [c:\\src\\qgis\\src\\core\\qgsexpression.cpp @ 2628]
00000000`11eef010 00007ff8`77f4127f : 00000000`17af91e0 00000000`11eef0f0 00000000`11eef270 00000000`12c61a70 : qgis_core!QgsExpression::evaluate+0xf8 [c:\\src\\qgis\\src\\core\\qgsexpression.cpp @ 2039]
00000000`11eef080 00007ff8`78394d6c : 00000000`17af91e0 00000000`11eef0f0 00000000`11eef270 00000000`19251640 : qgis_core!QgsExpression::evaluate+0x2f [c:\\src\\qgis\\src\\core\\qgsexpression.h @ 126]
00000000`11eef0c0 00007ff8`7839344d : 00000000`175f3c60 00000000`11eef270 00000000`00000000 00007ff8`7808d4e3 : qgis_core!QgsVectorLayerFeatureIterator::addVirtualAttributes+0x10c [c:\\src\\qgis\\src\\core\\qgsvectorlayerfeatureiterator.cpp @ 562]
00000000`11eef130 00007ff8`781a2013 : 00000000`175f3c60 00000000`11eef270 00000000`11eeead8 00000000`11eeead8 : qgis_core!QgsVectorLayerFeatureIterator::fetchFeature+0x2dd [c:\\src\\qgis\\src\\core\\qgsvectorlayerfeatureiterator.cpp @ 225]
00000000`11eef1b0 00007ff8`77f45d44 : 00000000`175f3c60 00000000`11eef270 00000000`11eef208 ffffffff`fffffffe : qgis_core!QgsAbstractFeatureIterator::nextFeature+0x83 [c:\\src\\qgis\\src\\core\\qgsfeatureiterator.cpp @ 51]
00000000`11eef200 00007ff8`783a37ac : 00000000`11eef4a0 00000000`11eef270 00000000`11eef270 00000000`1954eef0 : qgis_core!QgsFeatureIterator::nextFeature+0x34 [c:\\src\\qgis\\src\\core\\qgsfeatureiterator.h @ 196]
00000000`11eef240 00007ff8`783a35a3 : 00000000`1515d250 00000000`11eef4a0 00000000`11eef4b0 00000000`00000000 : qgis_core!QgsVectorLayerRenderer::drawRendererV2+0x3c [c:\\src\\qgis\\src\\core\\qgsvectorlayerrenderer.cpp @ 249]
00000000`11eef440 00007ff8`7824de13 : 00000000`1515d250 00007ff8`00000001 00007ff8`787c7f30 00007ff8`787c7f00 : qgis_core!QgsVectorLayerRenderer::render+0xdc3 [c:\\src\\qgis\\src\\core\\qgsvectorlayerrenderer.cpp @ 219]
00000000`11eef9d0 00007ff8`7824ee8a : 00000000`1954eef0 00000000`68eb69f1 00000000`690f8b68 00007ff8`7824f1ee : qgis_core!QgsMapRendererParallelJob::renderLayerStatic+0x163 [c:\\src\\qgis\\src\\core\\qgsmaprendererparalleljob.cpp @ 215]
00000000`11eefb40 00007ff8`7824ed73 : 00000000`19a4a830 00000000`1954eef0 00000000`11eefc08 00000000`00000007 : qgis_core!QtConcurrent::FunctionWrapper1<void,LayerRenderJob & __ptr64>::operator()+0x1a
[c:\\osgeo4w64\\include\\qt4\\qtcore\\qtconcurrentfunctionwrappers.h @ 87]
00000000`11eefb70 00007ff8`7824ee21 : 00000000`19a4a7f0 00000000`11eefbd0 00000000`00000001 00000000`00000000 : qgis_core!QtConcurrent::MapKernel<QList<LayerRenderJob>::iterator,QtConcurrent::FunctionWrapper1<void,LayerRenderJob & __ptr64> >::runIteration+0x33 [c:\\osgeo4w64\\include\\qt4\\qtcore\\qtconcurrentmapkernel.h @ 74]
00000000`11eefba0 00007ff8`7824f87b : 00000000`19a4a7f0 00000000`11eefcb8 00042a07`00000001 00007ff8`00000002 : qgis_core!QtConcurrent::MapKernel<QList<LayerRenderJob>::iterator,QtConcurrent::FunctionWrapper1<void,LayerRenderJob & __ptr64> >::runIterations+0x91 [c:\\osgeo4w64\\include\\qt4\\qtcore\\qtconcurrentmapkernel.h @ 83]
00000000`11eefc00 00007ff8`7824f5d7 : 00000000`19a4a7f0 00000000`00000000 00000000`0ea17b50 00000000`00000000 : qgis_core!QtConcurrent::IterateKernel<QList<LayerRenderJob>::iterator,void>::forThreadFunction+0x26b
[c:\\osgeo4w64\\include\\qt4\\qtcore\\qtconcurrentiteratekernel.h @ 263]
00000000`11eefd00 00000000`68e57ef9 : 00000000`19a4a838 00000000`02d18708 00000000`19a4a840 00000000`0ea17b50 : qgis_core!QtConcurrent::IterateKernel<QList<LayerRenderJob>::iterator,void>::threadFunction+0x27
[c:\\osgeo4w64\\include\\qt4\\qtcore\\qtconcurrentiteratekernel.h @ 225]
00000000`11eefd30 00000000`68e59672 : 00000000`19a4a840 00000000`02d186e8 00000000`02d186e9 00000000`0ea17b50 : QtCore4!QtConcurrent::ThreadEngineBase::run+0x59

00000000`11eefd90 00000000`68e67de7 : 00000000`0e8a27d0 00000000`02d186e8 00000000`0ea17b50 00000000`15156788 : QtCore4!QThreadPool::globalInstance+0xf2
00000000`11eefe10 00000000`67e31d9f : 00000000`12b1e550 00000000`0f247ef0 00000000`00000000 00000000`0f247ef0 : QtCore4!QThread::setPriority+0x307
00000000`11eefe60 00000000`67e31e3b : 00000000`67ec2ac0 00000000`0f247ef0 00000000`00000000 00000000`00000000 : msvcr100!endthreadex+0x43
00000000`11eefe90 00007ff8`a08e13d2 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : msvcr100!endthreadex+0xdf
00000000`11eefec0 00007ff8`a31e5444 : 00007ff8`a08e13b0 00000000`00000000 00000000`00000000 00000000`00000000 : kernel32!BaseThreadInitThunk+0x22
00000000`11eefef0 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x34

SYMBOL_STACK_INDEX: 0

SYMBOL_NAME: QtSql4!QPSQLDriver::open+410

FOLLOWUP_NAME: MachineOwner

MODULE_NAME: QtSql4

IMAGE_NAME: QtSql4.dll

DEBUG_FLR_IMAGE_TIMESTAMP: 52f7d87e

STACK_COMMAND: ~13s; .ecxr ; kb

FAILURE_BUCKET_ID: INVALID_POINTER_READ_c0000005_QtSql4.dll!QPSQLDriver::open

BUCKET_ID: X64_APPLICATION_FAULT_INVALID_POINTER_READ_QtSql4!QPSQLDriver::open+410

Followup: MachineOwner

History

#1 - 2015-05-17 04:40 AM - Sean Lin

I'm using pgbouncer with postgresql 9.3.5 x64. Had a prior problem with idle connections being left opened.

#2 - 2015-05-17 04:47 AM - Jürgen Fischer

You're using virtual field with a custom function that directly accesses the database via QtSql?

#3 - 2015-05-17 04:31 PM - Sean Lin

I'm using dbsql(connectionName,sqlQuery) from the refFunctions plugin to get random rows from the postgres db which is displayed as a maptip on mouse over.

#4 - 2015-05-21 12:14 AM - Giovanni Manghi

- Priority changed from Normal to High

- Crashes QGIS or corrupts data changed from No to Yes

#5 - 2015-06-14 12:34 AM - Giovanni Manghi

- Status changed from Open to Feedback

please test qgis master and report back.

#6 - 2015-10-05 03:21 AM - Jürgen Fischer

- Resolution set to not reproducable

- Status changed from Feedback to Closed

closing for the lack of feedback.