

QGIS Application - Bug report #8269

QgsDataProvider.changeAttributeValues() causes memory error when called with non-QVariant argument

2013-07-11 08:17 AM - Alexander Dunlap

Status:Closed Priority:Normal Assignee: Category:Python plugins Affected QGIS version:1.8.0 Operating System:Mac OS X Pull Request or Patch supplied: Crashes QGIS or corrupts data:Yes	Regression?:No Easy fix?:No Resolution: Copied to github as #: 17072
Description I ran the following code in the Python console, with a layer selected: >>> l = qgis.utils.iface.activeLayer() >>> l = qgis.utils.iface.activeLayer() >>> p = l.dataProvider() >>> from PyQt4.QtCore import QVariant >>> p.changeAttributeValues({0 : { 0 : QVariant(0) } }) True >>> p.changeAttributeValues({0 : { 0 : 0 } }) The second-to-last line works fine. Running the final line, however, causes QGIS to crash, with the error QGIS(89325,0x7fff7cc04180) malloc: *** error for object 0x1065d35c0: pointer being freed was not allocated *** set a breakpoint in malloc_error_break to debug Abort trap: 6 The trace given in the Apple crash report is Exception Type: EXC_CRASH (SIGABRT) Exception Codes: 0x0000000000000000, 0x0000000000000000 Application Specific Information: *** error for object 0x1065d35c0: pointer being freed was not allocated Thread 0 Crashed:: Dispatch queue: com.apple.main-thread 0 libsystem_kernel.dylib 0x00007fff8e821212 __pthread_kill + 10 1 libsystem_c.dylib 0x00007fff8f177b54 pthread_kill + 90 2 libsystem_c.dylib 0x00007fff8f1bbdce abort + 143 3 libsystem_c.dylib 0x00007fff8f18f9b9 free + 392 4 QtCore.so 0x00000001153aa567 release_QVariant_4 + 39 5 core.so 0x0000000116318444 convertTo_QMap_3800_0600QMap_1800_0100QVariant + 694 6 sip.so 0x000000011532a83d sip_api_convert_to_type + 208 7 sip.so 0x000000011532e176 parsePass2 + 2313 8 sip.so 0x00000001153314b2 parseKwdArgs + 266 9 sip.so 0x00000001153316b2 sip_api_parse_args + 133 10 core.so 0x00000001163525bb meth_QgsVectorDataProvider_changeAttributeValues + 130	

```

11 org.python.python      0x000000011509e5a9 PyEval_EvalFrameEx + 9244
12 org.python.python      0x000000011509c147 PyEval_EvalCodeEx + 1934
13 org.python.python      0x000000011509eb3e PyEval_EvalFrameEx + 10673
14 org.python.python      0x000000011509c147 PyEval_EvalCodeEx + 1934
15 org.python.python      0x00000001150a28df 0x115085000 + 121055
16 org.python.python      0x000000011509e63a PyEval_EvalFrameEx + 9389
17 org.python.python      0x000000011509c147 PyEval_EvalCodeEx + 1934
18 org.python.python      0x00000001150a28df 0x115085000 + 121055
19 org.python.python      0x000000011509e63a PyEval_EvalFrameEx + 9389
20 org.python.python      0x00000001150a2869 0x115085000 + 120937
21 org.python.python      0x000000011509e63a PyEval_EvalFrameEx + 9389
22 org.python.python      0x00000001150a2869 0x115085000 + 120937
23 org.python.python      0x000000011509e63a PyEval_EvalFrameEx + 9389
24 org.python.python      0x000000011509c147 PyEval_EvalCodeEx + 1934
25 org.python.python      0x00000001150d5d7a 0x115085000 + 331130
26 org.python.python      0x00000001150946c6 PyObject_Call + 97
27 org.python.python      0x00000001150b19bf 0x115085000 + 182719
28 org.python.python      0x00000001150946c6 PyObject_Call + 97
29 org.python.python      0x00000001150a2018 PyEval_CallObjectWithKeywords + 177
30 sip.so                  0x000000011532b706 sip_api_call_method + 186
31 QtGui.so                0x0000000115806db0 sipVH_QtGui_25(PyGILState_STATE, _object*, QKeyEvent*) + 64
32 QtGui.so                0x00000001158b308d sipQTextEdit::keyPressEvent(QKeyEvent*) + 99
33 QtGui                   0x0000000104d436cb QWidget::event(QEvent*) + 2491
34 QtGui                   0x00000001050d623c QFrame::event(QEvent*) + 44
35 QtGui                   0x000000010516365b QAbstractScrollArea::event(QEvent*) + 123
36 QtGui                   0x000000010514e98b QTextEdit::event(QEvent*) + 91
37 QtGui.so                0x00000001158b019c sipQTextEdit::event(QEvent*) + 76
38 QtGui                   0x0000000104cebb93d QApplicationPrivate::notify_helper(QObject*, QEvent*) + 189
39 QtGui                   0x0000000104cf403b QApplication::notify(QObject*, QEvent*) + 9883
40 org.qgis.qgis_core      0x0000000103d84762 QgsApplication::notify(QObject*, QEvent*) + 100
41 QtCore                  0x0000000104a3417c QCoreApplication::notifyInternal(QObject*, QEvent*) + 124
42 QtGui                   0x0000000104cebb4c qt_sendSpontaneousEvent(QObject*, QEvent*) + 44
43 QtGui                   0x0000000104d67fe1 QKeyMapper::sendKeyEvent(QWidget*, bool, QEvent::Type, int,
QFlags<Qt::KeyboardModifier>, QString const&, bool, int, unsigned int, unsigned int, unsigned int, bool*) + 225
44 QtGui                   0x0000000104d68ea3 QKeyMapperPrivate::translateKeyEvent(QWidget*,
OpaqueEventHandlerCallRef*, OpaqueEventRef*, void*, bool) + 659
45 QtGui                   0x0000000104c9dadb qt_dispatchKeyEvent(void*, QWidget*) + 223
46 QtGui                   0x0000000104c8fe3f -[QCocoaView keyDown:] + 127
47 com.apple.AppKit        0x00007fff8faf8050 -[NSWindow sendEvent:] + 9687
48 QtGui                   0x0000000104c94a37 -[QCocoaWindow sendEvent:] + 87
49 com.apple.AppKit        0x00007fff8faf3674 -[NSApplication sendEvent:] + 5761
50 QtGui                   0x0000000104c99b24 -[QNSApplication sendEvent:] + 84
51 com.apple.AppKit        0x00007fff8fa0924a -[NSApplication run] + 636
52 QtGui                   0x0000000104ca4900
QEventDispatcherMac::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) + 1824
53 QtCore                  0x0000000104a33094 QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) + 68
54 QtCore                  0x0000000104a33444 QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) + 324
55 QtCore                  0x0000000104a35b2c QCoreApplication::exec() + 188
56 org.qgis.qgis           0x000000010000996b main + 10523
57 org.qgis.qgis           0x0000000100006c04 start + 52

```

Thread 1:: Dispatch queue: com.apple.libdispatch-manager

```
0 libsystem_kernel.dylib 0x00007fff8e821d16 kevent + 10
```

```
1 libdispatch.dylib      0x00007fff8d833dea _dispatch_mgr_invoke + 883
2 libdispatch.dylib      0x00007fff8d8339ee _dispatch_mgr_thread + 54
```

Thread 2:

```
0 libsystem_kernel.dylib  0x00007fff8e8216d6 __workq_kernreturn + 10
1 libsystem_c.dylib       0x00007fff8f178f4c _pthread_workq_return + 25
2 libsystem_c.dylib       0x00007fff8f178d13 _pthread_wqthread + 412
3 libsystem_c.dylib       0x00007fff8f1631d1 start_wqthread + 13
```

Thread 3:

```
0 libsystem_kernel.dylib  0x00007fff8e8216d6 __workq_kernreturn + 10
1 libsystem_c.dylib       0x00007fff8f178f4c _pthread_workq_return + 25
2 libsystem_c.dylib       0x00007fff8f178d13 _pthread_wqthread + 412
3 libsystem_c.dylib       0x00007fff8f1631d1 start_wqthread + 13
```

Thread 4:

```
0 libsystem_kernel.dylib  0x00007fff8e8216d6 __workq_kernreturn + 10
1 libsystem_c.dylib       0x00007fff8f178f4c _pthread_workq_return + 25
2 libsystem_c.dylib       0x00007fff8f178d13 _pthread_wqthread + 412
3 libsystem_c.dylib       0x00007fff8f1631d1 start_wqthread + 13
```

Thread 0 crashed with X86 Thread State (64-bit):

```
rax: 0x0000000000000000 rbx: 0x0000000000000006 rcx: 0x00007fff5fbcad8  rdx: 0x0000000000000000
rdi: 0x0000000000000707 rsi: 0x0000000000000006 rbp: 0x00007fff5fbcb00  rsp: 0x00007fff5fbcad8
r8: 0x00007fff7cc03278  r9: 0x0000000000000000 r10: 0x0000000020000000 r11: 0x0000000000000206
r12: 0x00000000107830e0 r13: 0x00000000105f4f00 r14: 0x00007fff7cc04180 r15: 0x0000000000000004
rip: 0x00007fff8e821212 rfl: 0x0000000000000206 cr2: 0x00007fff7cbfcff0
```

Logical CPU: 0

History

#1 - 2013-11-21 11:24 PM - Matthias Kuhn

- Status changed from Open to Closed

This works with QGIS 2.0 (And there is no more data type QVariant in PyQt...) And as it seems, it's easy to work around in 1.8.

Please reopen if this is still an issue.