QGIS Application - Bug report #120
Click a shape in a shapefile, QGIS crashes

2006-05-18 10:53 PM - acarr-sasktel-net -

Status:	Closed		
Priority:	Low		
Assignee:	Marco Hugentobler		
Category:	Data Provider		
Affected QGIS version:		**Regression?:**	No
Operating System:	Fedora	**Easy fix?:**	No
Pull Request or Patch supplied:		**Resolution:**	fixed
Crashes QGIS or corrupts data:		**Copied to github as #:**	10179

Description

Computer: Fedora Core 5, 64bit
QGIS from svn, May 12ish
proj and GEOS from repository, GDAL locally compiled, all 64 bit.
QT4 from source
Compilation of QGIS using GCC 3.x, but some libraries used GCC4 (the default).
Steps:
1) Load QGIS
2) Add Vector Layer (choose a shapefile - doesn't seem to matter which, although I was only using polygons...), layer shows on screen.
3) Choose the identify tool, Click on a shape.
4) QGIS crashes:

*** glibc detected *** qgis: munmap_chunk(): invalid pointer: 0x0000000000ba4b50 ***

h7. Backtrace:

/lib64/libc.so.6(+libc_free+0x17a)[0x395d66da1a]
/usr/lib64/libgeos.so.2(_ZN4geos16TopologyLocationD0Ev+0x39)[0x36666931a9]
/usr/lib64/libgeos.so.2(_ZN4geos5LabelD0Ev+0x21)[0x366668de21]
/usr/lib64/libgeos.so.2(_ZN4geos7EdgeEndD2Ev+0x21)[0x3666687011]
/usr/lib64/libgeos.so.2(_ZN4geos13EdgeEndBundleD0Ev+0x75)[0x36666bf295]
/usr/lib64/libgeos.so.2(_ZN4geos17EdgeEndBundleStarD0Ev+0x37)[0x36666bf897]
/usr/lib64/libgeos.so.2(_ZN4geos4NodeD2Ev+0x2e)[0x366668f98e]
/usr/lib64/libgeos.so.2(_ZN4geos10RelateNodeD0Ev+0x17)[0x36666c1157]
/usr/lib64/libgeos.so.2(_ZN4geos7NodeMapD0Ev+0x35)[0x366668fe15]
/usr/lib64/libgeos.so.2(_ZN4geos14RelateComputerD1Ev+0x2e)[0x36666c06ee]
/usr/lib64/libgeos.so.2(_ZN4geos8RelateOpD1Ev+0x28)[0x36666c1878]
/usr/lib64/libgeos.so.2(_ZN4geos8RelateOp6relateEPKNS_8GeometryES3_+0x2f)[0x3666 6c199f]
/usr/lib64/libgeos.so.2(_ZNK4geos8Geometry6relateEPKS0_+0x57)[0x3666668497]
/usr/lib64/libgeos.so.2(_ZNK4geos8Geometry10intersectsEPKS0_+0x70)[0x3666666e00]
/usr/lib/qgis/ogrprovider.so(_ZN14QgsOgrProvider14getNextFeatureEb+0x1cc)[0x2aaa b13d811c]
/usr/lib/libqgis_gui.so.0(_ZN18QgsMapToolIdentify19identifyVectorLayerEP14QgsVec
torLayerRK8QgsPoint+0x34d)[0x2aaaaad3a47d]
/usr/lib/libqgis_gui.so.0(_ZN18QgsMapToolIdentify18canvasReleaseEventEP11QMouseE vent+0x9a)[0x2aaaaad3979a]
/usr/lib/libqgis_gui.so.0(_ZN12QgsMapCanvas25contentsMouseReleaseEventEP11QMouse Event+0x3c)[0x2aaaaad200ec]
/usr/local/Trolltech/Qt-4.1.2/lib/libQt3Support.so.4(_ZN12Q3ScrollView25viewport
[[MouseReleaseEventEP]]11QMouseEvent+0x69)[0x2aaaab846cc9]
/usr/local/Trolltech/Qt-4.1.2/lib/libQt3Support.so.4(_ZN12Q3ScrollView11eventFil
terEP7QObjectP6QEvent+0x200)[0x2aaaab848110]
/usr/local/Trolltech/Qt-4.1.2/lib/libQtGui.so.4(_ZN19QApplicationPrivate13notify

_helperEP7QObjectP6QEvent+0xb6)[0x2aaaac12c736]
/usr/local/Trolltech/Qt-4.1.2/lib/libQtGui.so.4(_ZN12QApplication6notifyEP7QObje ctP6QEvent+0x524)[0x2aaaac12dee4]
/usr/local/Trolltech/Qt-4.1.2/lib/libQtGui.so.4[0x2aaaac17b5b2]
/usr/local/Trolltech/Qt-4.1.2/lib/libQtGui.so.4(_ZN12QApplication15x11ProcessEve ntEP7_XEvent+0x981)[0x2aaaac17a751]
/usr/local/Trolltech/Qt-4.1.2/lib/libQtGui.so.4[0x2aaaac18a98d]
/usr/local/Trolltech/Qt-4.1.2/lib/libQtCore.so.4(_ZN10QEventLoop13processEventsE
6QFlagsINS_17ProcessEventsFlagEE+0x30)[0x2aaaac833e50]
/usr/local/Trolltech/Qt-4.1.2/lib/libQtCore.so.4(_ZN10QEventLoop4execE6QFlagsINS
_17ProcessEventsFlagEE+0xa7)[0x2aaaac834157]
/usr/local/Trolltech/Qt-4.1.2/lib/libQtCore.so.4(_ZN16QCoreApplication4execEv+0x bb)[0x2aaaac8362bb]
qgis(main+0x17ab)[0x404d9b]
/lib64/libc.so.6(+libc_start_main+0xf4)[0x395d61d084]
qgis[0x4031a9]

h7. Memory map:

00400000-00408000 r-xp 00000000 08:01 4537304 /usr/bi n/qgis
00508000-00509000 rw-p 00008000 08:01 4537304 /usr/bi n/qgis
00509000-00bcb000 rw-p 00509000 00:00 0 [heap]
3666000000-3666008000 r-xp 00000000 08:01 794150 /usr/li b64/libgif.so.4.1.3
3666008000-3666108000 ---p 00008000 08:01 794150 /usr/li b64/libgif.so.4.1.3
3666108000-3666109000 rw-p 00008000 08:01 794150 /usr/li b64/libgif.so.4.1.3
3666200000-366621f000 r-xp 00000000 08:01 795733 /usr/li b64/libpq.so.4.1
366621f000-366631f000 ---p 0001f000 08:01 795733 /usr/li b64/libpq.so.4.1
366631f000-3666321000 rw-p 0001f000 08:01 795733 /usr/li b64/libpq.so.4.1
3666400000-3666457000 r-xp 00000000 08:01 791192 /usr/li b64/libsqlite3.so.0.8.6
3666457000-3666557000 ---p 00057000 08:01 791192 /usr/li b64/libsqlite3.so.0.8.6
3666557000-3666559000 rw-p 00057000 08:01 791192 /usr/li b64/libsqlite3.so.0.8.6
3666600000-3666706000 r-xp 00000000 08:01 794950 /usr/li b64/libgeos.so.2.2.1
3666706000-3666806000 ---p 00106000 08:01 794950 /usr/li b64/libgeos.so.2.2.1
3666806000-366680f000 rw-p 00106000 08:01 794950 /usr/li b64/libgeos.so.2.2.1
3666f00000-3666f6800Aborted

History

#1 - 2006-05-18 11:50 PM - Marco Hugentobler

My feeling is that this is a 64-bit problem in [[QgsGeometry]]::geosGeometry()

#2 - 2006-08-16 07:16 AM - Tim Sutton

I have had the same problem before on 32 bit platform. I believe its an issue with GEOS. Which exact version of GEOS was QGIS compiled against?

#3 - 2006-08-16 11:52 AM - acarr-sasktel-net -

- Resolution set to fixed

- Status changed from Open to Closed

RPM version. rpm -q returns:
geos-2.2.1-4.fc5

Obviously, I have the devel package, too, same version.

Could it be derived from a compiler mismatch? I had to use the gcc-compat compiler for QGIS, because the main FC5 compiler failed.

I believe there is a patch floating around. I will retest with the GCC 4 compiler and the current libraries.

It seems to be working now, although I'm not sure on the details of why. The two possibilities which present themselves are:

1) Compiler issues between the RPM library (GCC 4.1) and QGiS (GCC 3.x). I can now compile in GCC 4.1, so I have, and it works.

2) Some change within QGIS which has corrected the problem by itself.

Thanks for looking into it.

Angus Carr.

#4 - 2009-08-22 12:46 AM - Anonymous

Milestone Version 0.8 deleted