

QGIS Application - Bug report #1485

crashes when playing with symbology - GDAL issue

2009-01-13 04:24 PM - Ilija Milicevic -

Status:	Closed	
Priority:	Low	
Assignee:	nobody -	
Category:	Symbology	
Affected QGIS version:		Regression?: No
Operating System:	Linux	Easy fix?: No
Pull Request or Patch supplied:		Resolution: wontfix
Crashes QGIS or corrupts data:		Copied to github as #: 11545
Description		
When I open the dataset, change the symbology to graduated and try to create 5 classes, it crashes on me. This does not happen on regular XP machines, XP running under virtualization, Hardy64 (as tested by wildintellect). Link to the dataset: http://projects.atlas.ca.gov/frs/download.php/615/cnty24k97_2.zip Link to the strace output: http://rafb.net/p/CEwcw022.html		

History

#1 - 2009-01-16 06:31 PM - Alex Mandel

I can verify this issue on Intrepid 32bit, and believe it revolves around dbf field types.

When you try to run the classify function on a column N,19 qgis crashes columns of type N,9 works fine. (As reported via [[OpenOffice]])

Looking at [dbf documentation](#) N field should be less than 18 chars, which makes me think the fields are being misidentified and should be floating point, F.

Applies to polygon layer symbology

- Graduated Symbol or
- continuous on a polygon

#2 - 2009-02-10 10:00 AM - matter -

I get buffer overloads when classifying graduated symbology on any shapefile now, and it is impeding my work! Running Intrepid 64 bit. I did not have this problem in Hardy.

What is the next step in solving this?

Here's my overflow from one such crash: (As dumped to the terminal)

```
*** buffer overflow detected ***: /usr/bin/qgis.bin terminated
```

h7. Backtrace:

```
/lib/libc.so.6(+fortify_fail+0x37)[0x7fb9e591b887]
/lib/libc.so.6[0x7fb9e5919750]
/lib/libc.so.6[0x7fb9e5918d8b]
/lib/libc.so.6(+snprintf_chk+0x7b)[0x7fb9e5918c5b]
/usr/lib/libgdal1.5.0.so.1(_ZN10OGRFeature16GetFieldAsStringEi+0x346)[0x7fb9e69903f6]
/usr/lib/libgdal1.5.0.so.1(_ZN21OGRGenSQLResultsLayer14PrepareSummaryEv+0x111)[0x7fb9e690bbb1]
/usr/lib/libgdal1.5.0.so.1(_ZN21OGRGenSQLResultsLayer10GetFeatureEi+0xbd)[0x7fb9e690be5d]
```

/usr/lib/qgis/libogrprovider.so(_ZN14QgsOgrProvider12minimumValueEi+0x4ea)[0x7fb9d465d8ca]
/usr/bin/qgis.bin(_ZN24QgsGraduatedSymbolDialog20adjustClassificationEv+0x17ff)[0x4cd8ff]
/usr/bin/qgis.bin(_ZN24QgsGraduatedSymbolDialog11qt_metacallEN11QMetaObject4CallEiPPv+0xc0)[0x5d2720]
/usr/lib/libQtCore.so.4(_ZN11QMetaObject8activateEP7QObjectiiPPv+0x244)[0x7fb9e8a62134]
/usr/lib/libQtGui.so.4(_ZN15QAbstractButton7clickedEb+0x37)[0x7fb9e84f6787]
/usr/lib/libQtGui.so.4[0x7fb9e827a8db]
/usr/lib/libQtGui.so.4[0x7fb9e827c4a2]
/usr/lib/libQtGui.so.4(_ZN15QAbstractButton17mouseReleaseEventEP11QMouseEvent+0x85)[0x7fb9e827c6f5]
/usr/lib/libQtGui.so.4(_ZN7QWidget5eventEP6QEvent+0x9b9)[0x7fb9e7fc2329]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate13notify_helperEP7QObjectP6QEvent+0xbd)[0x7fb9e7f6fc3d]
/usr/lib/libQtGui.so.4(_ZN12QApplication6notifyEP7QObjectP6QEvent+0x90a)[0x7fb9e7f7822a]
/usr/lib/libqgis_core.so.1.0(_ZN14QgsApplication6notifyEP7QObjectP6QEvent+0x18)[0x7fb9e8d9bad8]
/usr/lib/libQtCore.so.4(_ZN16QCoreApplication14notifyInternalEP7QObjectP6QEvent+0xd1)[0x7fb9e8a4dd61]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate14sendMouseEventEP7QWidgetP11QMouseEventS1_S1_PS1_R8QPointerIS0_E+0x108)[0x7fb9e7f775c8][
b9e7f775c8]
/usr/lib/libQtGui.so.4[0x7fb9e7fdbbe9]
/usr/lib/libQtGui.so.4(_ZN12QApplication15x11ProcessEventEP7_XEvent+0x8c7)[0x7fb9e7fda607]
/usr/lib/libQtGui.so.4[0x7fb9e80022c4]
/usr/lib/libglib-2.0.so.0(g_main_context_dispatch+0x23b)[0x7fb9e4b4ad3b]
/usr/lib/libglib-2.0.so.0[0x7fb9e4b4e50d]
/usr/lib/libglib-2.0.so.0(g_main_context_iteration+0x6b)[0x7fb9e4b4e6cb]
/usr/lib/libQtCore.so.4(_ZN20QEventDispatcherGlib13processEventsE6QFlagsIN10QEventLoop17ProcessEventsFlagEE+0x4f)[0x7fb9e8a7615f][
usr/lib/libQ
]
/usr/lib/libQtGui.so.4[0x7fb9e8001a6f]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop13processEventsE6QFlagsINS_17ProcessEventsFlagEE+0x32)[0x7fb9e8a4c682]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop4execE6QFlagsINS_17ProcessEventsFlagEE+0xcd)[0x7fb9e8a4c80d]
/usr/lib/libQtGui.so.4(_ZN7QDialog4execEv+0xc5)[0x7fb9e8389065]
/usr/bin/qgis.bin(_ZN9QgsLegend25legendLayerShowPropertiesEv+0x11a)[0x59f8fa]
/usr/bin/qgis.bin(_ZN9QgsLegend11qt_metacallEN11QMetaObject4CallEiPPv+0x11d)[0x5d594d]
/usr/lib/libQtCore.so.4(_ZN11QMetaObject8activateEP7QObjectiiPPv+0x244)[0x7fb9e8a62134]
/usr/lib/libQtGui.so.4(_ZN7QAction9triggeredEb+0x37)[0x7fb9e7f69f57]
/usr/lib/libQtGui.so.4(_ZN7QAction8activateENS_11ActionEventE+0xb0)[0x7fb9e7f6a720]
/usr/lib/libQtGui.so.4[0x7fb9e83031ad]
/usr/lib/libQtGui.so.4(_ZN7QWidget5eventEP6QEvent+0x9b9)[0x7fb9e7fc2329]
/usr/lib/libQtGui.so.4(_ZN5QMenu5eventEP6QEvent+0xeb)[0x7fb9e830598b]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate13notify_helperEP7QObjectP6QEvent+0xbd)[0x7fb9e7f6fc3d]
/usr/lib/libQtGui.so.4(_ZN12QApplication6notifyEP7QObjectP6QEvent+0x90a)[0x7fb9e7f7822a]
/usr/lib/libqgis_core.so.1.0(_ZN14QgsApplication6notifyEP7QObjectP6QEvent+0x18)[0x7fb9e8d9bad8]
/usr/lib/libQtCore.so.4(_ZN16QCoreApplication14notifyInternalEP7QObjectP6QEvent+0xd1)[0x7fb9e8a4dd61]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate14sendMouseEventEP7QWidgetP11QMouseEventS1_S1_PS1_R8QPointerIS0_E+0x108)[0x7fb9e7f775c8][
b9e7f775c8]
/usr/lib/libQtGui.so.4[0x7fb9e7fdbda4]
/usr/lib/libQtGui.so.4(_ZN12QApplication15x11ProcessEventEP7_XEvent+0x8c7)[0x7fb9e7fda607]
/usr/lib/libQtGui.so.4[0x7fb9e80022c4]
/usr/lib/libglib-2.0.so.0(g_main_context_dispatch+0x23b)[0x7fb9e4b4ad3b]
/usr/lib/libglib-2.0.so.0[0x7fb9e4b4e50d]
/usr/lib/libglib-2.0.so.0(g_main_context_iteration+0x6b)[0x7fb9e4b4e6cb]
/usr/lib/libQtCore.so.4(_ZN20QEventDispatcherGlib13processEventsE6QFlagsIN10QEventLoop17ProcessEventsFlagEE+0x4f)[0x7fb9e8a7615f][
usr/lib/libQ
]
/usr/lib/libQtGui.so.4[0x7fb9e8001a6f]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop13processEventsE6QFlagsINS_17ProcessEventsFlagEE+0x32)[0x7fb9e8a4c682]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop4execE6QFlagsINS_17ProcessEventsFlagEE+0xcd)[0x7fb9e8a4c80d]
/usr/lib/libQtGui.so.4(_ZN5QMenu4execERK6QPointP7QAction+0x75)[0x7fb9e83057e5]

```

/usr/bin/qgis.bin(_ZN9QgsLegend21handleRightClickEventEP15QTreeWidgetItemRK6QPoint+0x406)[0x5a18f6]
/usr/bin/qgis.bin(_ZN9QgsLegend15mousePressEventEP11QMouseEvent+0x86)[0x5a1cf6]
/usr/lib/libQtGui.so.4(_ZN7QWidget5eventEP6QEvent+0x99f)[0x7fb9e7fc230f]
/usr/lib/libQtGui.so.4(_ZN17QAbstractItemView13viewportEventEP6QEvent+0x3ed)[0x7fb9e83e78fd]
/usr/lib/libQtGui.so.4(_ZN9QTreeView13viewportEventEP6QEvent+0x250)[0x7fb9e841c530]
/usr/lib/libQtCore.so.4(_ZN23QCoreApplicationPrivate29sendThroughObjectEventFiltersEP7QObjectP6QEvent+0x88)[0x7fb9e8a4d038]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate13notify_helperEP7QObjectP6QEvent+0x8c)[0x7fb9e7f6fc0c]

```

h7. Memory map:

00400000-00640000 r-xp 00000000 fe:01 443872	/usr/bin/qgis.bin
00840000-00841000 r--p 00240000 fe:01 443872	/usr/bin/qgis.bin
00841000-00847000 rw-p 00241000 fe:01 443872	/usr/bin/qgis.bin
00847000-00848000 rw-p 00847000 00:00 0	
00e57000-06b0c000 rw-p 00e57000 00:00 0	[heap]
404bf000-404c0000 ---p 404bf000 00:00 0	
404c0000-40cc0000 rw-p 404c0000 00:00 0	
40cc0000-40cc1000 ---p 40cc0000 00:00 0	
40cc1000-414c1000 rw-p 40cc1000 00:00 0	
41a08000-41a09000 ---p 41a08000 00:00 0	
41a09000-42209000 rw-p 41a09000 00:00 0	
7fb9c8000000-7fb9c80ce000 rw-p 7fb9c8000000 00:00 0	
7fb9c80ce000-7fb9cc000000 ---p 7fb9c80ce000 00:00 0	
7fb9cff0a000-7fb9cff70000 rw-p 7fb9cff0a000 00:00 0	
7fb9cff70000-7fb9cff78000 r-xp 00000000 fe:01 482816	/usr/lib/gdal15plugins/gdal_GRASS.so
7fb9cff78000-7fb9d0178000 ---p 00008000 fe:01 482816	/usr/lib/gdal15plugins/gdal_GRASS.so
7fb9d0178000-7fb9d0179000 r--p 00008000 fe:01 482816	/usr/lib/gdal15plugins/gdal_GRASS.so
7fb9d0179000-7fb9d017a000 rw-p 00009000 fe:01 482816	/usr/lib/gdal15plugins/gdal_GRASS.so
7fb9d017a000-7fb9d017e000 r-xp 00000000 fe:01 114584	/usr/lib/python2.5/lib-dynload/zlib.so
7fb9d017e000-7fb9d037d000 ---p 00004000 fe:01 114584	/usr/lib/python2.5/lib-dynload/zlib.so
7fb9d037d000-7fb9d037e000 r--p 00003000 fe:01 114584	/usr/lib/python2.5/lib-dynload/zlib.so
7fb9d037e000-7fb9d0380000 rw-p 00004000 fe:01 114584	/usr/lib/python2.5/lib-dynload/zlib.so
7fb9d0380000-7fb9d0384000 r-xp 00000000 fe:01 114560	/usr/lib/python2.5/lib-dynload/cStringIO.so
7fb9d0384000-7fb9d0583000 ---p 00004000 fe:01 114560	/usr/lib/python2.5/lib-dynload/cStringIO.so
7fb9d0583000-7fb9d0584000 r--p 00003000 fe:01 114560	/usr/lib/python2.5/lib-dynload/cStringIO.so
7fb9d0584000-7fb9d0586000 rw-p 00004000 fe:01 114560	/usr/lib/python2.5/lib-dynload/cStringIO.so
7fb9d0586000-7fb9d058b000 r-xp 00000000 fe:01 114563	/usr/lib/python2.5/lib-dynload/binascii.so
7fb9d058b000-7fb9d078a000 ---p 00005000 fe:01 114563	/usr/lib/python2.5/lib-dynload/binascii.so
7fb9d078a000-7fb9d078b000 r--p 00004000 fe:01 114563	/usr/lib/python2.5/lib-dynload/binascii.so
7fb9d078b000-7fb9d078c000 rw-p 00005000 fe:01 114563	/usr/lib/python2.5/lib-dynload/binascii.so
7fb9d078c000-7fb9d0793000 r-xp 00000000 fe:01 114559	/usr/lib/python2.5/lib-dynload/_struct.so
7fb9d0793000-7fb9d0992000 ---p 00007000 fe:01 114559	/usr/lib/python2.5/lib-dynload/_struct.so
7fb9d0992000-7fb9d0993000 r--p 00006000 fe:01 114559	/usr/lib/python2.5/lib-dynload/_struct.so
7fb9d0993000-7fb9d0995000 rw-p 00007000 fe:01 114559	/usr/lib/python2.5/lib-dynload/_struct.so
7fb9d0995000-7fb9d0a00000 r-xp 00000000 fe:01 361918	/usr/lib/python2.5/site-packages/PyQt4/QtNetwork.so
7fb9d0a00000-7fb9d0c00000 ---p 0006b000 fe:01 361918	/usr/lib/python2.5/site-packages/PyQt4/QtNetwork.so
7fb9d0c00000-7fb9d0c02000 r--p 0006bAborted	

This bug is likely related to other similar issues caused by gdal 1.5 on ubuntu. Timlinux suggests trying gdal 1.6 (not available on ppa yet) to resolve it.

Ticket may be a duplicate.

#4 - 2009-02-17 02:28 PM - Jürgen Fischer

- Status changed from Open to Closed
- Resolution set to fixed

Looks like the backported unstable package in our ppa also solves the issue.

https://launchpad.net/%7Eggis/+archive/ppa/+files/libgdal1-1.5.0_1.5.4-2~intrepid3_amd64.deb

#5 - 2009-03-27 02:24 AM - dolf -

- Resolution deleted (fixed)
- Status changed from Closed to Feedback

I already had the above version of libgdal installed on Ubuntu Intrepid Ibex but downloaded and installed the above version just to be safe. The problem still exists with me. When classifying using unique values there is no problem, but when using a graduated color, qgis crashes.

I was classifying the counties of california with the attached dataset.

I am running the following system:

Ubuntu Intrepid Ibex 8.10 with 2.6.27-11-generic #3905 SMP x86_64 GNU/Linux

libgdal1-1.5.0	1.5.4-2~intrepid3	Geospatial Data Abstraction Library
libgdal1-1.5.0-grass	1.5.2-1	GRASS extension for the Geospatial Data Abstraction Library
gdal-bin	1.5.4-2~intrepid3	Geospatial Data Abstraction Library - Utility programs
qgis	1.0.1-1~intrepid1	Geographic Information System (GIS)
qgis-common	1.0.1-1~intrepid1	Quantum GIS - architecture-independent data
qgis-plugin-grass	1.0.1-1~intrepid1	GRASS plugin for Quantum GIS
qgis-plugin-grass-common	1.0.1-1~intrepid1	GRASS plugin for Quantum GIS - architecture-independent data
grass	6.2.3-2.1	Geographic Resources Analysis Support System

The following is the dump:

Python support ENABLED :-)

*** buffer overflow detected ***: /usr/bin/qgis.bin terminated

h7. Backtrace:

```
/lib/libc.so.6(+fortify_fail+0x37)[0x7fb3188bf887]
/lib/libc.so.6[0x7fb3188bd750]
/lib/libc.so.6[0x7fb3188bcd8b]
/lib/libc.so.6(+snprintf_chk+0x7b)[0x7fb3188bcc5b]
/usr/lib/libgdal1.5.0.so.1(_ZN10OGRFeature16GetFieldAsStringEi+0x346)[0x7fb319937566]
/usr/lib/libgdal1.5.0.so.1(_ZN21OGRGenSQLResultsLayer14PrepareSummaryEv+0x111)[0x7fb3198b2931]
/usr/lib/libgdal1.5.0.so.1(_ZN21OGRGenSQLResultsLayer10GetFeatureEi+0xbd)[0x7fb3198b2bdd]
/usr/lib/qgis/libogrprovider.so(_ZN14QgsOgrProvider12minimumValueEi+0x4ea)[0x7fb304cf78ba]
/usr/bin/qgis.bin(_ZN24QgsGraduatedSymbolDialog20adjustClassificationEv+0x17ff)[0x4cdaeef]
```

```

/usr/bin/qgis.bin(_ZN24QgsGraduatedSymbolDialog11qt_metacallEN11QMetaObject4CallEiPPv+0xc0)[0x5d28c0]
/usr/lib/libQtCore.so.4(_ZN11QMetaObject8activateEP7QObjectiiPPv+0x244)[0x7fb31ba09134]
/usr/lib/libQtGui.so.4(_ZN15QAbstractButton7clickedEb+0x37)[0x7fb31b49d797]
/usr/lib/libQtGui.so.4[0x7fb31b2218db]
/usr/lib/libQtGui.so.4[0x7fb31b2234a2]
/usr/lib/libQtGui.so.4(_ZN15QAbstractButton17mouseReleaseEventEP11QMouseEvent+0x85)[0x7fb31b2236f5]
/usr/lib/libQtGui.so.4(_ZN7QWidget5eventEP6QEvent+0x9b9)[0x7fb31af69329]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate13notify_helperEP7QObjectP6QEvent+0xbd)[0x7fb31af16c3d]
/usr/lib/libQtGui.so.4(_ZN12QApplication6notifyEP7QObjectP6QEvent+0x90a)[0x7fb31af1f22a]
/usr/lib/libqgis_core.so.1.0(_ZN14QgsApplication6notifyEP7QObjectP6QEvent+0x18)[0x7fb31bd42a08]
/usr/lib/libQtCore.so.4(_ZN16QCoreApplication14notifyInternalEP7QObjectP6QEvent+0xd1)[0x7fb31b9f4d61]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate14sendMouseEventEP7QWidgetP11QMouseEventS1_S1_PS1_R8QPointerIS0_E+0x108)[0x7fb31af1e5c8]
b31af1e5c8]
/usr/lib/libQtGui.so.4[0x7fb31af82be9]
/usr/lib/libQtGui.so.4(_ZN12QApplication15x11ProcessEventEP7_XEvent+0x8c7)[0x7fb31af81607]
/usr/lib/libQtGui.so.4[0x7fb31afa92c4]
/usr/lib/libglib-2.0.so.0(g_main_context_dispatch+0x23b)[0x7fb317aeed5b]
/usr/lib/libglib-2.0.so.0[0x7fb317af252d]
/usr/lib/libglib-2.0.so.0(g_main_context_iteration+0x6b)[0x7fb317af26eb]
/usr/lib/libQtCore.so.4(_ZN20QEventDispatcherGlib13processEventsE6QFlagsIN10QEventLoop17ProcessEventFlagEE+0x4f)[0x7fb31ba1d15f]
usr/lib/
f]
/usr/lib/libQtGui.so.4[0x7fb31afa8a6f]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop13processEventsE6QFlagsINS_17ProcessEventFlagEE+0x32)[0x7fb31b9f3682]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop4execE6QFlagsINS_17ProcessEventFlagEE+0xcd)[0x7fb31b9f380d]
/usr/lib/libQtGui.so.4(_ZN7QDialog4execEv+0xc5)[0x7fb31b330065]
/usr/bin/qgis.bin(_ZN9QgsLegend25legendLayerShowPropertiesEv+0x11a)[0x59fa9a]
/usr/lib/libQtGui.so.4(_ZN7QWidget5eventEP6QEvent+0x80c)[0x7fb31af6917c]
/usr/lib/libQtGui.so.4(_ZN17QAbstractItemView13viewportEventEP6QEvent+0x3ed)[0x7fb31b38e8fd]
/usr/lib/libQtGui.so.4(_ZN9QTreeView13viewportEventEP6QEvent+0x250)[0x7fb31b3c3530]
/usr/lib/libQtCore.so.4(_ZN23QCoreApplicationPrivate29sendThroughObjectEventFiltersEP7QObjectP6QEvent+0x88)[0x7fb31b9f4038]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate13notify_helperEP7QObjectP6QEvent+0x8c)[0x7fb31af16c0c]
/usr/lib/libQtGui.so.4(_ZN12QApplication6notifyEP7QObjectP6QEvent+0x90a)[0x7fb31af1f22a]
/usr/lib/libqgis_core.so.1.0(_ZN14QgsApplication6notifyEP7QObjectP6QEvent+0x18)[0x7fb31bd42a08]
/usr/lib/libQtCore.so.4(_ZN16QCoreApplication14notifyInternalEP7QObjectP6QEvent+0xd1)[0x7fb31b9f4d61]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate14sendMouseEventEP7QWidgetP11QMouseEventS1_S1_PS1_R8QPointerIS0_E+0x108)[0x7fb31af1e5c8]
b31af1e5c8]
/usr/lib/libQtGui.so.4[0x7fb31af82be9]
/usr/lib/libQtGui.so.4(_ZN12QApplication15x11ProcessEventEP7_XEvent+0x8c7)[0x7fb31af81607]
/usr/lib/libQtGui.so.4[0x7fb31afa92c4]
/usr/lib/libglib-2.0.so.0(g_main_context_dispatch+0x23b)[0x7fb317aeed5b]
/usr/lib/libglib-2.0.so.0[0x7fb317af252d]
/usr/lib/libglib-2.0.so.0(g_main_context_iteration+0x6b)[0x7fb317af26eb]
/usr/lib/libQtCore.so.4(_ZN20QEventDispatcherGlib13processEventsE6QFlagsIN10QEventLoop17ProcessEventFlagEE+0x4f)[0x7fb31ba1d15f]
usr/lib/libQ
f]
/usr/lib/libQtGui.so.4[0x7fb31afa8a6f]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop13processEventsE6QFlagsINS_17ProcessEventFlagEE+0x32)[0x7fb31b9f3682]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop4execE6QFlagsINS_17ProcessEventFlagEE+0xcd)[0x7fb31b9f380d]
/usr/lib/libQtCore.so.4(_ZN16QCoreApplication4execEv+0xbd)[0x7fb31b9f5cbd]
/usr/bin/qgis.bin(main+0x1ba8)[0x46d448]
/lib/libc.so.6(+libc_start_main+0xe6)[0x7fb3187de466]
/usr/bin/qgis.bin[0x46b3e9]

```

h7. Memory map:

00400000-00641000 r-xp 00000000 08:02 582425	/usr/bin/qgis.bin
00840000-00841000 r--p 00240000 08:02 582425	/usr/bin/qgis.bin
00841000-00847000 rw-p 00241000 08:02 582425	/usr/bin/qgis.bin
00847000-00848000 rw-p 00847000 00:00 0	
01524000-027e6000 rw-p 01524000 00:00 0	[heap]
402d1000-402d2000 ---p 402d1000 00:00 0	
402d2000-40ad2000 rw-p 402d2000 00:00 0	
40ad2000-40ad3000 ---p 40ad2000 00:00 0	
40ad3000-412d3000 rw-p 40ad3000 00:00 0	
4191d000-4191e000 ---p 4191d000 00:00 0	
4191e000-4211e000 rw-p 4191e000 00:00 0	
7fb3012a6000-7fb3012ae000 r-xp 00000000 08:02 1441882	/usr/lib/gdal15plugins/gdal_GRASS.so
7fb3012ae000-7fb3014ae000 ---p 00008000 08:02 1441882	/usr/lib/gdal15plugins/gdal_GRASS.so
7fb3014ae000-7fb3014af000 r--p 00008000 08:02 1441882	/usr/lib/gdal15plugins/gdal_GRASS.so
7fb3014af000-7fb3014b0000 rw-p 00009000 08:02 1441882	/usr/lib/gdal15plugins/gdal_GRASS.so
7fb3014b0000-7fb301528000 r-xp 00000000 08:02 1098047	/usr/lib/python2.5/site-packages/qgis/gui.so
7fb301528000-7fb301728000 ---p 00078000 08:02 1098047	/usr/lib/python2.5/site-packages/qgis/gui.so
7fb301728000-7fb30172b000 r--p 00078000 08:02 1098047	/usr/lib/python2.5/site-packages/qgis/gui.so
7fb30172b000-7fb301736000 rw-p 0007b000 08:02 1098047	/usr/lib/python2.5/site-packages/qgis/gui.so
7fb301736000-7fb301774000 r-xp 00000000 08:02 1262013	/usr/lib/python2.5/site-packages/PyQt4/QtXml.so
7fb301774000-7fb301973000 ---p 0003e000 08:02 1262013	/usr/lib/python2.5/site-packages/PyQt4/QtXml.so
7fb301973000-7fb301975000 r--p 0003d000 08:02 1262013	/usr/lib/python2.5/site-packages/PyQt4/QtXml.so
7fb301975000-7fb30197c000 rw-p 0003f000 08:02 1262013	/usr/lib/python2.5/site-packages/PyQt4/QtXml.so
7fb30197c000-7fb301a29000 r-xp 00000000 08:02 950293	/usr/lib/python2.5/site-packages/qgis/core.so
7fb301a29000-7fb301c28000 ---p 000ad000 08:02 950293	/usr/lib/python2.5/site-packages/qgis/core.so
7fb301c28000-7fb301c2c000 r--p 000ac000 08:02 950293	/usr/lib/python2.5/site-packages/qgis/core.so
7fb301c2c000-7fb301c40000 rw-p 000b0000 0Aborted	

#6 - 2009-03-27 02:37 AM - dolf -

The dataset was too large to upload. It is the california dataset on <http://www.plantsciences.ucdavis.edu/plant/qgislabs.htm> where I was classifying the countries layer.

#7 - 2009-04-26 01:20 PM - Giovanni Manghi

Don't know if it is related but every time I try to classify using a column that is of "real" type qgis crashes.

- buffer overflow detected ***: /usr/bin/qgis.bin terminated

h7. Backtrace:

```

/lib/tls/i686/cmov/libc.so.6(+fortify_fail+0x48)[0xb697e6d8]
/lib/tls/i686/cmov/libc.so.6[0xb697c800]
/lib/tls/i686/cmov/libc.so.6[0xb697c107]
/lib/tls/i686/cmov/libc.so.6(+snprintf_chk+0x34)[0xb697bffa]
/usr/lib/libgdal1.5.0.so.1(_ZN10OGRFeature16GetFieldAsStringEi+0x36f)[0xb6f4b98f]
/usr/lib/libgdal1.5.0.so.1(_ZN21OGRGenSQLResultsLayer14PrepareSummaryEv+0x10b)[0xb6eb47bb]
/usr/lib/libgdal1.5.0.so.1(_ZN21OGRGenSQLResultsLayer10GetFeatureEi+0xda)[0xb6eb4a8a]

```

/usr/lib/libgdal1.5.0.so.1(_ZN21OGRGenSQLResultsLayer14GetNextFeatureEv+0xe2)[0xb6eb4692]
/usr/lib/libgdal1.5.0.so.1(OGR_L_GetNextFeature+0x21)[0xb6ee0871]
/usr/lib/qgis/libogrprovider.so(_ZN14QgsOgrProvider12uniqueValuesEiR5QListI8QVariantE+0x444)[0xb2cdac84]
/usr/bin/qgis.bin(_ZN20QgsUniqueValueDialog29changeClassificationAttributeEv+0xb3)[0x81adef3]
/usr/bin/qgis.bin(_ZN20QgsUniqueValueDialog11qt_metacallEN11QMetaObject4CallEiPPv+0x143)[0x8219d83]
/usr/lib/libQtCore.so.4(_ZN11QMetaObject8activateEP7QObjectiiPPv+0x200)[0xb7d7da60]
/usr/lib/libQtCore.so.4(_ZN11QMetaObject8activateEP7QObjectPKS_iiPPv+0x60)[0xb7d7de60]
/usr/lib/libQtGui.so.4(_ZN15QAbstractButton7clickedEb+0x51)[0xb7a47e61]
/usr/lib/libQtGui.so.4[0xb779b199]
/usr/lib/libQtGui.so.4[0xb779cd94]
/usr/lib/libQtGui.so.4(_ZN15QAbstractButton17mouseReleaseEventEP11QMouseEvent+0x96)[0xb779d026]
/usr/lib/libQtGui.so.4(_ZN7QWidget5eventEP6QEvent+0x9a2)[0xb74b1962]
/usr/lib/libQtGui.so.4(_ZN15QAbstractButton5eventEP6QEvent+0x3e)[0xb779b03e]
/usr/lib/libQtGui.so.4(_ZN11QPushButton5eventEP6QEvent+0x40)[0xb7841910]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate13notify_helperEP7QObjectP6QEvent+0xbc)[0xb74598ec]
/usr/lib/libQtGui.so.4(_ZN12QApplication6notifyEP7QObjectP6QEvent+0xa71)[0xb74620e1]
/usr/lib/libqgis_core.so.1.0(_ZN14QgsApplication6notifyEP7QObjectP6QEvent+0x33)[0xb7e9f023]
/usr/lib/libQtCore.so.4(_ZN16QCoreApplication14notifyInternalEP7QObjectP6QEvent+0xb1)[0xb7d68e61]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate14sendMouseEventEP7QWidgetP11QMouseEventS1_S1_PS1_R8QPointerIS0_E+0xde)[0xb746136e]
/usr/lib/libQtGui.so.4[0xb74cb656]
/usr/lib/libQtGui.so.4(_ZN12QApplication15x11ProcessEventEP7_XEvent+0x1625)[0xb74ca9e5]
/usr/lib/libQtGui.so.4[0xb74f47aa]
/usr/lib/libglib-2.0.so.0(g_main_context_dispatch+0x1e8)[0xb67c3718]
/usr/lib/libglib-2.0.so.0[0xb67c6dc3]
/usr/lib/libglib-2.0.so.0(g_main_context_iteration+0x71)[0xb67c6f81]
/usr/lib/libQtCore.so.4(_ZN20QEventDispatcherGlib13processEventsE6QFlagsIN10QEventLoop17ProcessEventFlagEE+0x58)[0xb7d93478]
/usr/lib/libQtGui.so.4[0xb74f3ea5]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop13processEventsE6QFlagsINS_17ProcessEventFlagEE+0x4a)[0xb7d6752a]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop4execE6QFlagsINS_17ProcessEventFlagEE+0xea)[0xb7d676ea]
/usr/lib/libQtGui.so.4(_ZN7QDialog4execEv+0xe7)[0xb78c6987]
/usr/bin/qgis.bin(_ZN9QgsLegend25legendLayerShowPropertiesEv+0x143)[0x81e4763]
/usr/lib/libQtGui.so.4(_ZN7QWidget5eventEP6QEvent+0x7f2)[0xb74b17b2]
/usr/lib/libQtGui.so.4(_ZN6QFrame5eventEP6QEvent+0x33)[0xb77e8fd3]
/usr/lib/libQtGui.so.4(_ZN19QAbstractScrollArea13viewportEventEP6QEvent+0x5f)[0xb787f7df]
/usr/lib/libQtGui.so.4(_ZN17QAbstractItemView13viewportEventEP6QEvent+0x30f)[0xb792accf]
/usr/lib/libQtGui.so.4(_ZN9QTreeView13viewportEventEP6QEvent+0x234)[0xb79629e4]
/usr/lib/libQtGui.so.4[0xb7881d85]
/usr/lib/libQtCore.so.4(_ZN23QCoreApplicationPrivate29sendThroughObjectEventFiltersEP7QObjectP6QEvent+0x9a)[0xb7d6804a]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate13notify_helperEP7QObjectP6QEvent+0x9a)[0xb74598ca]
/usr/lib/libQtGui.so.4(_ZN12QApplication6notifyEP7QObjectP6QEvent+0xa71)[0xb74620e1]
/usr/lib/libqgis_core.so.1.0(_ZN14QgsApplication6notifyEP7QObjectP6QEvent+0x33)[0xb7e9f023]
/usr/lib/libQtCore.so.4(_ZN16QCoreApplication14notifyInternalEP7QObjectP6QEvent+0xb1)[0xb7d68e61]
/usr/lib/libQtGui.so.4(_ZN19QApplicationPrivate14sendMouseEventEP7QWidgetP11QMouseEventS1_S1_PS1_R8QPointerIS0_E+0xde)[0xb746136e]
/usr/lib/libQtGui.so.4[0xb74cb656]
/usr/lib/libQtGui.so.4(_ZN12QApplication15x11ProcessEventEP7_XEvent+0x1625)[0xb74ca9e5]
/usr/lib/libQtGui.so.4[0xb74f47aa]
/usr/lib/libglib-2.0.so.0(g_main_context_dispatch+0x1e8)[0xb67c3718]
/usr/lib/libglib-2.0.so.0[0xb67c6dc3]
/usr/lib/libglib-2.0.so.0(g_main_context_iteration+0x71)[0xb67c6f81]
/usr/lib/libQtCore.so.4(_ZN20QEventDispatcherGlib13processEventsE6QFlagsIN10QEventLoop17ProcessEventFlagEE+0x58)[0xb7d93478]
/usr/lib/libQtGui.so.4[0xb74f3ea5]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop13processEventsE6QFlagsINS_17ProcessEventFlagEE+0x4a)[0xb7d6752a]
/usr/lib/libQtCore.so.4(_ZN10QEventLoop4execE6QFlagsINS_17ProcessEventFlagEE+0xea)[0xb7d676ea]

```
/usr/lib/libQtCore.so.4(_ZN16QCoreApplication4execEv+0xb5)[0xb7d69da5]
/usr/lib/libQtGui.so.4(_ZN12QApplication4execEv+0x27)[0xb7459767]
/usr/bin/qgis.bin(main+0x18ef)[0x80a4aaf]
```

h7. Memory map:

```
08048000-0827b000 r-xp 00000000 08:01 2445955 /usr/bin/qgis.bin
0827b000-0827c000 r--p 00232000 08:01 2445955 /usr/bin/qgis.bin
0827c000-0827f000 rw-p 00233000 08:01 2445955 /usr/bin/qgis.bin
0827f000-08280000 rw-p 0827f000 00:00 0
08d0d000-0b356000 rw-p 08d0d000 00:00 0 [heap]
ad2cb000-ad360000 r--p 00000000 08:01 2574075 /usr/share/fonts/truetype/ttf-dejavu/DejaVuSans.ttf
ad360000-ad370000 rw-p ad360000 00:00 0
ad37a000-ad37b000 ---p ad37a000 00:00 0
ad37b000-adb7b000 rw-p ad37b000 00:00 0
adb7b000-adb7c000 ---p adb7b000 00:00 0
adb7c000-ae7e5000 rw-p adb7c000 00:00 0
ae840000-ae8d0000 rw-p ae840000 00:00 0
ae8da000-ae8de000 r-xp 00000000 08:01 5070978 /lib/tls/i686/cmov/libnss_dns-2.8.90.so
ae8de000-ae8df000 r--p 00003000 08:01 5070978 /lib/tls/i686/cmov/libnss_dns-2.8.90.so
ae8df000-ae8e0000 rw-p 00004000 08:01 5070978 /lib/tls/i686/cmov/libnss_dns-2.8.90.so
ae8e0000-ae8e2000 r-xp 00000000 08:01 5054556 /lib/libnss_mdns4_minimal.so.2
ae8e2000-ae8e3000 rw-p 00001000 08:01 5054556 /lib/libnss_mdns4_minimal.so.2
ae8e3000-ae8f2000 r-xp 00000000 08:01 5055260 /lib/libresolv-2.8.90.so
ae8f2000-ae8f3000 r--p 0000e000 08:01 5055260 /lib/libresolv-2.8.90.so
ae8f3000-ae8f4000 rw-p 0000f000 08:01 5055260 /lib/ld.so.0
```

#8 - 2009-04-26 01:27 PM - Giovanni Manghi

I forgot to mention that this happens on ubuntu 8.10 32 bit with qgis 1.0.1 and no matter how simple if the shape file.

#9 - 2009-05-09 08:33 AM - Jürgen Fischer

see also #1679.

This still looks like an OGR bug (it works for me in trunk on Debian unstable and in OSGeo4W 1.0.2 and 1.1.0). All using GDAL 1.5.4 (as reported in the provider tab in the about box).

Please include the GDAL version and package origin.

#10 - 2009-05-10 09:37 AM - Giovanni Manghi

Seems really a gdal bug. I tested qgis 1.0.1 in the Les-ejk [[UbuntuGIS]] repository and as is compiled against gdal 1.6.0 there isn't this problem.

#11 - 2009-05-19 04:38 AM - matter -

- Status changed from Feedback to Closed
- Resolution set to wontfix

The Les-ejk repository seems to be out of date now for getting the updated version of GDAL

For info on the [[UbuntuGIS]] repository, look here:

[\[https://launchpad.net/~ubuntugis\]](https://launchpad.net/~ubuntugis)

Since this is a GDAL issue, I marked this as resolved (wontfix)

#12 - 2018-03-10 06:54 AM - trackposlaju parcelposts

This bug is likely related to other similar issues on site issue like poslaju. poslaju is an malaysian courier site, same bug repeats on poslajutracking.me . I need to solve the issues so that people in malaysia will be able to track their parcels.