QGIS Application - Bug report #1511
Buffer overload when classifying ArcGIS created shapefiles

2009-01-25 12:24 PM - matter -

Status:	Closed		
Priority:	Low		
Assignee:	nobody -		
Category:	Symbology		
Affected QGIS version:		**Regression?:**	No
Operating System:	Debian	**Easy fix?:**	No
Pull Request or Patch supplied:		**Resolution:**	duplicate
Crashes QGIS or corrupts data:		**Copied to github as #:**	11571

Description

On several shapefiles that I have tried to import the system is hard-crashing while trying to classify the values in a gradated symbol scheme. One of the shapefiles was exported from Datamine, and would not import to QGIS, so it was imported to [[ArcGIS]] first, and then exported another shapefile to be imported into QGIS. The other files were a QGIS-generated shapefile that was taken to [[ArcGIS]], edited, and re-imported to QGIS. New projects were created, and the data was tweaked to be smaller, yet QGIS crashed every time. One of the offending shapefiles is attached.

Upon crashing, this was 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(_ZN21OGRGenSQLResultsLayer10GetFeatureEl+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)[
_E+0x108)[0x7fb9e7f775c8]
/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)[0x7fb9e8a7
0x7fb9e8a7615f]
/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)[
_E+0x108)[0x7fb9e7f775c8]
/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)[0x7fb9e8a7
0x7fb9e8a7615f]
/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]?/us
a4d038]
/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
```

History

#1 - 2009-01-25 12:32 PM - matter -

Bug may be related to #1485

#2 - 2009-02-10 09:56 AM - matter -

- Resolution set to duplicate

- Status changed from Open to Closed

Yes, this is the same bug as #1485. Can someone please delete this so it can be concentrated into one bugtrack?

#3 - 2009-08-22 01:01 AM - Anonymous

Milestone Version 1.0.1 deleted

Files

ArcGISeditedShapefile.zip	2.09 KB	2009-01-25	matter -