

QGIS Application - Bug report #7608

Commit 3a35a53 causes segfault when loading project

2013-04-14 04:32 AM - Nyall Dawson

Status:	Closed	
Priority:	Severe/Regression	
Assignee:		
Category:	Project Loading/Saving	
Affected QGIS version:	master	Regression?: No
Operating System:		Easy fix?: No
Pull Request or Patch applied:	No	Resolution:
Crashes QGIS or corrupts data:	Yes	Copied to github as #: 16536
Description		
The project attached to #7461 causes a segfault when opened. I've tracked the crash down to commit:3a35a53d6.		

Associated revisions

Revision 6983ec39 - 2013-05-02 03:57 PM - Radim Blazek

raster block setIsNoDataExcept fix, fixes #7608

History

#1 - 2013-04-14 04:50 AM - Giovanni Manghi

- Category set to Project Loading/Saving
- Priority changed from Normal to Severe/Regression
- Target version set to Version 2.0.0

#2 - 2013-04-20 11:59 AM - Jürgen Fischer

- Resolution set to fixed

fixed in commit:261dfbf56.

#3 - 2013-04-21 02:41 AM - Nyall Dawson

Only part of this is fixed -- the project loads now. But zooming/panning around the map still causes a segfault.

It's actually unrelated to the project. Adding the raster image alone to a new project also causes segfaults when zooming in and out.

#4 - 2013-04-26 02:07 AM - Matthias Kuhn

A similar issue seems to be resolved: #7659

Does your problem persist?

#5 - 2013-04-28 02:39 PM - Nyall Dawson

- Resolution deleted (fixed)

I'm still seeing it. If I add the bo5.tiff file to a new project in epsg:4326 then I don't see any crashes. Setting the project to epsg:3148 and panning/zooming quickly crashes qgis.

#6 - 2013-04-28 10:04 PM - Mathieu Pellerin - nIRV

I'm also able to reproduce crash. Steps:

1. Add the bo5.tiff raster into a new project
2. Change the project's CRS to epsg:3148 (on the fly re-projection must be enabled)
3. Zoom in and out quickly (make sure you zoom in and out > and < than raster 100% ratio)

It won't take 10 sec for QGIS to crash.

#7 - 2013-04-29 02:05 PM - Nyall Dawson

With latest master (27c5b93fd7) I'm getting an instant segfault when reprojecting the raster - no zooming or panning required.

#8 - 2013-04-29 07:06 PM - Mathieu Pellerin - nIRV

Nyall, over here, I still have to zoom in and out a couple of times for it to segfault using windows osgeo4w build 6e90ba3.

This issue is reproducible 100% of the times I've tried. Is this on Radim's radar or should we alert him over mailing list?

#9 - 2013-04-30 09:02 PM - Nathan Woodrow

Confirmed here to.

I needed to zoom in and out really fast with the mouse wheel.

#10 - 2013-04-30 09:17 PM - Larry Shaffer

- *File 7608_raster_crash-report.txt added*

I got it to crash once, but not again. Zooming gets really slow when zooming in beyond 1:1, but returns to normal once zooming out past 1:1 again.

Could not get it to crash when only loading the raster in a clean project.

Crash report attached. Tested on Mac OS X 10.7.5

#11 - 2013-04-30 10:03 PM - Nyall Dawson

Larry - when you loaded the raster in a clean project did you set it to reproject? I'm only seeing the crash with reprojection enabled.

#12 - 2013-05-02 02:58 AM - Radim Blazek

Unfortunately I cannot reproduce it. Can you attach a small raster + project to reproduce it?

What data type it is? Does the raster have no data value? Does it happen if map canvas is fully covered by raster, i.e. no need to use no data.

#13 - 2013-05-02 03:08 AM - Mathieu Pellerin - nIRV

- File test-blend.zip added

Radim, try with the project in this attached zip file. I can reproduce this crash 100% of time on my windows machine.

#14 - 2013-05-02 03:13 AM - Mathieu Pellerin - nIRV

The raster in the above attached project is a geotiff that was created by QGIS' heatmap feature.

It's data type is: Float32 - Thirty two bit floating point

It's no data value is: -9999

The crash does seem to happen "more" when zoomed out map canvas show all of raster.

#15 - 2013-05-02 03:14 AM - Giovanni Manghi

nirvn - wrote:

Radim, try with the project in this attached zip file. I can reproduce this crash 100% of time on my windows machine.

on linux too, by zooming really quick

gio@sibirica ~ \$ qgis

Warning: loading of qt translation failed [/usr/share/qt4/translations/qt_en_US]

Debug: Enable back buffering: false

Warning: Creating Warped VRT.

Warning: QMetaObject::connectSlotsByName: No matching signal for on_mLineWidthSpinBox_valueChanged(double)

```
- glibc detected */usr/bin/qgis.bin: double free or corruption (!prev): 0x0000000006577940 *===== Backtrace: =====
/lib/x86_64-linux-gnu/libc.so.6(+0x7eb96)[0x7fe7f0752b96]
/usr/lib/libqgis_core.so.1.9.0(_ZN14QgsRasterBlockD1Ev+0x1f)[0x7fe7f43ea86f]
/usr/lib/libqgis_core.so.1.9.0(_ZN14QgsRasterBlockD0Ev+0x9)[0x7fe7f43ea8d9]
/usr/lib/libqgis_core.so.1.9.0(_ZN25QgsSingleBandGrayRenderer5blockEiRK12QgsRectangleii+0x4a2)[0x7fe7f4423772]
/usr/lib/libqgis_core.so.1.9.0(_ZN27QgsBrightnessContrastFilter5blockEiRK12QgsRectangleii+0x60)[0x7fe7f4425d50]
/usr/lib/libqgis_core.so.1.9.0(_ZN22QgsHueSaturationFilter5blockEiRK12QgsRectangleii+0x64)[0x7fe7f4426b34]
/usr/lib/libqgis_core.so.1.9.0(_ZN23QgsRasterResampleFilter5blockEiRK12QgsRectangleii+0x1c4)[0x7fe7f44186a4]
/usr/lib/libqgis_core.so.1.9.0(_ZN18QgsRasterProjector5blockEiRK12QgsRectangleii+0x10d)[0x7fe7f43f4ffd]
/usr/lib/libqgis_core.so.1.9.0(_ZN17QgsRasterIterator18readNextRasterPartEiRiS0_PP14QgsRasterBlockS0_S0_+0x199)[0x7fe7f43fcca9]
/usr/lib/libqgis_core.so.1.9.0(_ZN15QgsRasterDrawer4drawEP8QPainterP17QgsRasterViewPortPK13QgsMapToPixel+0x9d)[0x7fe7f440fcfd]
/usr/lib/libqgis_core.so.1.9.0(_ZN14QgsRasterLayer4drawEP8QPainterP17QgsRasterViewPortPK13QgsMapToPixel+0x95)[0x7fe7f43fd9c5]
/usr/lib/libqgis_core.so.1.9.0(_ZN14QgsRasterLayer4drawER16QgsRenderContext+0x46c)[0x7fe7f440447c]
/usr/lib/libqgis_core.so.1.9.0(_ZN14QgsMapRenderer6renderEP8QPainterPd+0xf9f)[0x7fe7f42b0a7f]
/usr/lib/libqgis_gui.so.1.9.0(_ZN15QgsMapCanvasMap6renderEv+0x103)[0x7fe7f3cf9963]
/usr/lib/libqgis_gui.so.1.9.0(_ZN12QgsMapCanvas7refreshEv+0x51d)[0x7fe7f3cf47bd]
/usr/lib/libqgis_gui.so.1.9.0(_ZN12QgsMapCanvas10wheelEventEP11QWheelEvent+0x1d9)[0x7fe7f3cf7dd9]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN7QWidget5eventEP6QEvent+0xec4)[0x7fe7f26f6984]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN6QFrame5eventEP6QEvent+0x26)[0x7fe7f2ab63b6]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN13QGraphicsView13viewportEventEP6QEvent+0x7b)[0x7fe7f2ce0b2b]
```

```

/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN23QCoreApplicationPrivate29sendThroughObjectEventFiltersEP7QObjectP6QEvent+0x88)[0x7fe7f33230
8]

/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN19QApplicationPrivate13notify_helperEP7QObjectP6QEvent+0x7f)[0x7fe7f26a585f]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN12QApplication6notifyEP7QObjectP6QEvent+0x970)[0x7fe7f26aaf70]
/usr/lib/libqgis_core.so.1.9.0(_ZN14QgsApplication6notifyEP7QObjectP6QEvent+0x96)[0x7fe7f4217c26]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN16QCoreApplication14notifyInternalEP7QObjectP6QEvent+0x8c)[0x7fe7f3322e9c]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x238932)[0x7fe7f2712932]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x24be6d)[0x7fe7f2725e6d]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN12QApplication15x11ProcessEventEP7_XEvent+0xdce)[0x7fe7f2724bae]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x2740d2)[0x7fe7f274e0d2]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_dispatch+0x133)[0x7fe7ef236d53]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(+0x480a0)[0x7fe7ef2370a0]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_iteration+0x34)[0x7fe7ef237164]

/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN20QEventDispatcherGlib13processEventsE6QFlagsIN10QEventLoop17ProcessEventFlagEE+0x6f)[0x7f
7f33523bf]

/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x273d5e)[0x7fe7f274dd5e]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN10QEventLoop13processEventsE6QFlagsINS_17ProcessEventFlagEE+0x32)[0x7fe7f3321c82]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN10QEventLoop4execE6QFlagsINS_17ProcessEventFlagEE+0xf7)[0x7fe7f3321ed7]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN16QCoreApplication4execEv+0x87)[0x7fe7f3326f67]
/usr/bin/qgis.bin(main+0x21fe)[0x4e1ade]
/lib/x86_64-linux-gnu/libc.so.6(_libc_start_main+0xed)[0x7fe7f06f576d]

/usr/bin/qgis.bin[0x4e5861]===== Memory map: =====
00400000-00a26000 r-xp 00000000 08:03 1053927 /usr/bin/qgis.bin
00c26000-00c28000 r--p 00626000 08:03 1053927 /usr/bin/qgis.bin
00c28000-00c30000 rw-p 00628000 08:03 1053927 /usr/bin/qgis.bin
00c30000-00c33000 rw-p 00000000 00:00 0
01273000-081a4000 rw-p 00000000 00:00 0 [heap]
7fe7baffd000-7fe7bb4a7000 rw-s 00000000 00:04 1015817 /SYSV00000000 (deleted)
7fe7bb4a7000-7fe7bb4b9000 r-xp 00000000 08:03 1442830 /usr/lib/x86_64-linux-gnu/pkcs11/gnome-keyring-pkcs11.so
7fe7bb4b9000-7fe7bb6b8000 ---p 00012000 08:03 1442830 /usr/lib/x86_64-linux-gnu/pkcs11/gnome-keyring-pkcs11.so
7fe7bb6b8000-7fe7bb6ba000 r--p 00011000 08:03 1442830 /usr/lib/x86_64-linux-gnu/pkcs11/gnome-keyring-pkcs11.so
7fe7bb6ba000-7fe7bb6bb000 rw-p 00013000 08:03 1442830 /usr/lib/x86_64-linux-gnu/pkcs11/gnome-keyring-pkcs11.so
7fe7bb6bb000-7fe7bb8c9000 rw-p 00000000 00:00 0
7fe7bb8c9000-7fe7bbdfa000 rw-s 00000000 00:04 884743 /SYSV00000000 (deleted)
7fe7bbdfa000-7fe7bbdfef000 r-xp 00000000 08:03 1442328 /usr/lib/x86_64-linux-gnu/gdk-pixbuf-2.0/2.10.0/loaders/libpixbufloader-png.so
7fe7bbdfef000-7fe7bbffef000 ---p 00004000 08:03 1442328 /usr/lib/x86_64-linux-gnu/gdk-pixbuf-2.0/2.10.0/loaders/libpixbufloader-png.so
7fe7bbffef000-7fe7bbffff000 r--p 00004000 08:03 1442328 /usr/lib/x86_64-linux-gnu/gdk-pixbuf-2.0/2.10.0/loaders/libpixbufloader-png.so
7fe7bbffff000-7fe7bc000000 rw-p 00005000 08:03 1442328 /usr/lib/x86_64-linux-gnu/gdk-pixbuf-2.0/2.10.0/loaders/libpixbufloader-png.so
7fe7bc000000-7fe7bc021000 rw-p 00000000 00:00 0
7fe7bc021000-7fe7c0000000 ---p 00000000 00:00 0
7fe7c0067000-7fe7c00b7000 r-xp 00000000 08:03 1050564 /usr/lib/x86_64-linux-gnu/libcups.so.2
7fe7c00b7000-7fe7c02b6000 ---p 00050000 08:03 1050564 /usr/lib/x86_64-linux-gnu/libcups.so.2
7fe7c02b6000-7fe7c02ba000 r--p 0004f000 08:03 1050564 /usr/lib/x86_64-linux-gnu/libcups.so.2
7fe7c02ba000-7fe7c02bb000 rw-p 00053000 08:03 1050564 /usr/lib/x86_64-linux-gnu/libcups.so.2
7fe7c02bb000-7fe7c02c2000 r-xp 00000000 08:03 5123791 /lib/x86_64-linux-gnu/libnss_dns-2.15.so
7fe7c02c2000-7fe7c04c1000 ---p 00007000 08:03 5123791 /lib/x86_64-linux-gnu/libnss_dns-2.15.so
7fe7c04c1000-7fe7c04c2000 r--p 00006000 08:03 5123791 /lib/x86_64-linux-gnu/libnss_dns-2.15.so
7fe7c04c2000-7fe7c04c3000 rw-p 00007000 08:03 5123791 /lib/x86_64-linux-gnu/libnss_dns-2.15.so
7fe7c04c3000-7fe7c04c5000 r-xp 00000000 08:03 5111861 /lib/libnss_mdns4_minimal.so.2
7fe7c04c5000-7fe7c06c4000 ---p 00002000 08:03 5111861 /lib/libnss_mdns4_minimal.so.2
7fe7c06c4000-7fe7c06c5000 r--p 00001000 08:03 5111861 /lib/libnss_mdns4_minimal.so.2
7fe7c06c5000-7fe7c06c6000 rw-p 00002000 08:03 5111861 /lib/libnss_mdns4_minimal.so.2

```

7fe7c06c6000-7fe7c06c7000 ---p 00000000 00:00 0
7fe7c06c7000-7fe7c11c8000 rw-p 00000000 00:00 0
7fe7c11c8000-7fe7c11d6000 r-xp 00000000 08:03 1311314
7fe7c11d6000-7fe7c13d5000 ---p 0000e000 08:03 1311314
7fe7c13d5000-7fe7c13d6000 r--p 0000d000 08:03 1311314
7fe7c13d6000-7fe7c13d8000 rw-p 0000e000 08:03 1311314
7fe7c13d8000-7fe7c13e6000 r-xp 00000000 08:03 1313029
7fe7c13e6000-7fe7c15e6000 ---p 0000e000 08:03 1313029
7fe7c15e6000-7fe7c15e7000 r--p 0000e000 08:03 1313029
7fe7c15e7000-7fe7c15e8000 rw-p 0000f000 08:03 1313029
7fe7c15e8000-7fe7c1612000 r-xp 00000000 08:03 1310838
7fe7c1612000-7fe7c1811000 ---p 0002a000 08:03 1310838
7fe7c1811000-7fe7c1812000 r--p 00029000 08:03 1310838
7fe7c1812000-7fe7c1818000 rw-p 0002a000 08:03 1310838
7fe7c1818000-7fe7c185a000 r-xp 00000000 08:03 1315000
7fe7c185a000-7fe7c1a59000 ---p 00042000 08:03 1315000
7fe7c1a59000-7fe7c1a5a000 r--p 00041000 08:03 1315000
7fe7c1a5a000-7fe7c1a8f000 rw-p 00042000 08:03 1315000
7fe7c1a8f000-7fe7c1a98000 r-xp 00000000 08:03 1314986
7fe7c1a98000-7fe7c1c97000 ---p 00009000 08:03 1314986
7fe7c1c97000-7fe7c1c98000 r--p 00008000 08:03 1314986
7fe7c1c98000-7fe7c1c99000 rw-p 00009000 08:03 1314986
7fe7c1c99000-7fe7c1c9e000 r-xp 00000000 08:03 1314993
7fe7c1c9e000-7fe7c1e9e000 ---p 00005000 08:03 1314993
7fe7c1e9e000-7fe7c1e9f000 r--p 00005000 08:03 1314993
7fe7c1e9f000-7fe7c1ea0000 rw-p 00006000 08:03 1314993
7fe7c1ea0000-7fe7c1ea6000 r-xp 00000000 08:03 1314989
7fe7c1ea6000-7fe7c20a5000 ---p 00006000 08:03 1314989
7fe7c20a5000-7fe7c20a6000 r--p 00005000 08:03 1314989
7fe7c20a6000-7fe7c20a7000 rw-p 00006000 08:03 1314989
7fe7c20a7000-7fe7c20d1000 r-xp 00000000 08:03 1311977
7fe7c20d1000-7fe7c22d0000 ---p 0002a000 08:03 1311977
7fe7c22d0000-7fe7c22d1000 r--p 00029000 08:03 1311977
7fe7c22d1000-7fe7c22d3000 rw-p 0002a000 08:03 1311977
7fe7c22d3000-7fe7c22d8000 r-xp 00000000 08:03 1311951
7fe7c22d8000-7fe7c24d7000 ---p 00005000 08:03 1311951
7fe7c24d7000-7fe7c24d8000 r--p 00004000 08:03 1311951
7fe7c24d8000-7fe7c24d9000 rw-p 00005000 08:03 1311951
7fe7c24d9000-7fe7c24f1000 r-xp 00000000 08:03 1311958
7fe7c24f1000-7fe7c26f0000 ---p 00018000 08:03 1311958
7fe7c26f0000-7fe7c26f1000 r--p 00017000 08:03 1311958

/usr/lib/python2.7/lib-dynload/pyexpat.so
/usr/lib/python2.7/lib-dynload/pyexpat.so
/usr/lib/python2.7/lib-dynload/pyexpat.so
/usr/lib/python2.7/lib-dynload/pyexpat.so
/usr/lib/python2.7/dist-packages/mx/DateTime/mxDateTime/mxDateTime.so
/usr/lib/python2.7/dist-packages/mx/DateTime/mxDateTime/mxDateTime.so
/usr/lib/python2.7/dist-packages/mx/DateTime/mxDateTime/mxDateTime.so
/usr/lib/python2.7/dist-packages/mx/DateTime/mxDateTime/mxDateTime.so
/usr/lib/python2.7/dist-packages/psycopg2/_psycopg.so
/usr/lib/python2.7/dist-packages/psycopg2/_psycopg.so
/usr/lib/python2.7/dist-packages/psycopg2/_psycopg.so
/usr/lib/python2.7/dist-packages/psycopg2/_psycopg.so
/usr/lib/python2.7/dist-packages/numpy/random/mtrand.so
/usr/lib/python2.7/dist-packages/numpy/random/mtrand.so
/usr/lib/python2.7/dist-packages/numpy/random/mtrand.so
/usr/lib/python2.7/dist-packages/numpy/random/mtrand.so
/usr/lib/python2.7/dist-packages/numpy/fft/fftpack_lite.so
/usr/lib/python2.7/dist-packages/numpy/fft/fftpack_lite.so
/usr/lib/python2.7/dist-packages/numpy/fft/fftpack_lite.so
/usr/lib/python2.7/dist-packages/numpy/fft/fftpack_lite.so
/usr/lib/python2.7/dist-packages/numpy/linalg/lapack_lite.so
/usr/lib/python2.7/dist-packages/numpy/linalg/lapack_lite.so
/usr/lib/python2.7/dist-packages/numpy/linalg/lapack_lite.so
/usr/lib/python2.7/dist-packages/numpy/linalg/lapack_lite.so
/usr/lib/python2.7/dist-packages/numpy/lib/_compiled_base.so
/usr/lib/python2.7/dist-packages/numpy/lib/_compiled_base.so
/usr/lib/python2.7/dist-packages/numpy/lib/_compiled_base.so
/usr/lib/python2.7/dist-packages/numpy/lib/_compiled_base.so
/usr/lib/python2.7/dist-packages/numpy/core/scalarmath.so
/usr/lib/python2.7/dist-packages/numpy/core/scalarmath.so
/usr/lib/python2.7/dist-packages/numpy/core/scalarmath.so
/usr/lib/python2.7/dist-packages/numpy/core/scalarmath.so
/usr/lib/python2.7/dist-packages/numpy/core/_dotblas.so
/usr/lib/python2.7/dist-packages/numpy/core/_dotblas.so
/usr/lib/python2.7/dist-packages/numpy/core/_dotblas.so
/usr/lib/python2.7/dist-packages/numpy/core/_dotblas.so
/usr/lib/python2.7/dist-packages/numpy/core/_sort.so
/usr/lib/python2.7/dist-packages/numpy/core/_sort.so
/usr/lib/python2.7/dist-packages/numpy/core/_sort.so

#16 - 2013-05-02 03:56 AM - Radim Blazek

nirvn - wrote:

| Radim, try with the project in this attached zip file. I can reproduce this crash 100% of time on my windows machine.

Crashes here also, good. Thanks.

#17 - 2013-05-02 06:58 AM - Radim Blazek
- Status changed from Open to Closed

Fixed in changeset commit:"6983ec39b23ba8261f75b95aa5cd47eec5f5cb66".

#18 - 2013-05-02 06:59 AM - Radim Blazek

It should be fixed, we were really 1 byte out of block.

#19 - 2013-05-02 06:01 PM - Mathieu Pellerin - nIRV

Radim, that was fast :) thanks. I think that'll effectively deal with a bunch of raster related crashes I observed in last few weeks. Landsat 7 imagery with no data value for example kept crashing on me.

Files			
7608_raster_crash-report.txt	8.01 KB	2013-04-30	Larry Shaffer
test-blend.zip	2.72 MB	2013-05-02	Mathieu Pellerin - nIRV