QGIS Application - Bug report #4509
Crash on SPARC when opening vector layer

2011-11-09 01:26 PM - Sam Gillingham

Status:	Closed			
Priority:	High			
Assignee:				
Category:	Vectors			
Affected QGIS version:	master	**Regression?:**	No	
Operating System:	Sparc Solaris	**Easy fix?:**	No	
Pull Request or Patch supplied:	Applied	**Resolution:**	fixed/implemented	
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	14431	

Description

QGIS crashes with "signal BUS (invalid address alignment)" on Sparc Solaris when opening a shape file. I have tracked the problem down to src/core/symbology-ng/qgsrendererv2.cpp and I attach a proposed patch. As I understand it, Sparc and other RISC processors only allow memory access on certain memory boundaries so maybe memcpy is safer than pointer casting when dealing with WKBs. It seems other parts of QGIS already do this.

I think this will likely be a problem on ARM chips also as they have a similar limitation.

I am happy to do any other testing on Sparc that may be required.

History

#1 - 2011-12-09 08:19 AM - Paolo Cavallini

- Category set to Vectors

#2 - 2011-12-16 02:10 PM - Giovanni Manghi

- Target version set to Version 1.7.4

#3 - 2011-12-23 12:05 PM - Giovanni Manghi

- Affected QGIS version set to master

- Crashes QGIS or corrupts data set to Yes

#4 - 2012-01-31 12:55 PM - Sam Gillingham

- File qgsgeometry.cpp.patch added

Found that qgsgeometry.cpp has a similar problem...

#5 - 2012-04-11 04:29 PM - Sam Gillingham

- File qgslabel.cpp.patch added

Also in qgslabel.cpp - see attached patch. Confirmed that these issues cause similar problems on Linux/ARM.

#6 - 2012-04-16 06:32 AM - Paolo Cavallini

- Target version changed from Version 1.7.4 to Version 1.8.0

#7 - 2012-04-18 05:15 PM - Sam Gillingham

- File qgsdistancearea.cpp.patch added

- File qgsgeometry.cpp.patch2 added

Found a couple of missed fixes in qgsgeometry.cpp - see new patch. Also found another file with the problem (qgsdistancearea.cpp).

#8 - 2012-09-04 11:56 AM - Paolo Cavallini

- Target version changed from Version 1.8.0 to Version 2.0.0

#9 - 2013-05-29 09:40 AM - Paolo Cavallini

Could you check that the problem is still there? If so, could Marco please revise the patch and apply it if appropriate?
Thanks

#10 - 2013-09-18 04:39 PM - Marco Bernasocchi

this is also valid for android

#11 - 2013-09-18 04:41 PM - Marco Bernasocchi

patches updated and partly applyed in https://github.com/mbernasocchi/QGIS/tree/androidFixByteAllign. I'll pull request and close this later this week.

#12 - 2014-01-30 11:43 PM - Paolo Cavallini

- Target version changed from Version 2.0.0 to Future Release - High Priority

#13 - 2014-02-09 09:18 PM - Martin Dobias

- Resolution set to fixed/implemented

- Status changed from Open to Closed

- Target version changed from Future Release - High Priority to Version 2.2

Some time ago the WKB handling has been updated to use memcpy, so it should be working now in master. Please reopen if there are any remaining issues.

Files

qgsrendererv2.cpp.patch	3.73 KB	2011-11-09	Sam Gillingham
qgsgeometry.cpp.patch	35.6 KB	2012-01-31	Sam Gillingham
qgslabel.cpp.patch	4.23 KB	2012-04-11	Sam Gillingham
qgsgeometry.cpp.patch2	37.5 KB	2012-04-18	Sam Gillingham
qgsdistancearea.cpp.patch	2.33 KB	2012-04-18	Sam Gillingham