

QGIS Application - Bug report #2903

Segmentation Fault in 1.4, ubuntu karmic binaries

2010-07-23 01:19 AM - alobo -

Status: Closed	
Priority: Low	
Assignee: Jürgen Fischer	
Category: Vectors	
Affected QGIS version:	Regression?: No
Operating System: All	Easy fix?: No
Pull Request or Patch supplied:	Resolution: fixed
Crashes QGIS or corrupts data:	Copied to github as #: 12963

Description

QGIS 1.4 (ubuntu Karmic binary) crashed while I was running plugin points2one. The problem is that QGIS crashes now as soon as I open any shape layer, all I get in the terminal is: Segmentation Fault. I have tried uninstalling the plugin, no improvement.

Before opening any vector layer, the last lines in the console are:

```
Warning: QObject::connect: Incompatible sender/receiver arguments
[[QgsProject]]::writeProject(QDomDocument&) -->
[[QgisApp]]::projectChanged(QDomDocument)
```

I've tried reinstalling qgis (and the rest of related packages) via Synaptic, same problem.

Output with gdb:

```
alobo@delia:~$ gdb qgis.bin
GNU gdb (GDB) 7.0-ubuntu
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /usr/bin/qgis.bin...(no debugging symbols found)...done.
(gdb) run
Starting program: /usr/bin/qgis.bin
[Thread debugging using libthread_db enabled]
[New Thread 0x7fffe233a910 (LWP 9132)]
[Thread 0x7fffe233a910 (LWP 9132) exited]
Python support ENABLED :-)
/home/alobo/.qgis/python/plugins/imgboundary/+init+.py:38: [[DeprecationWarning]]: [[BaseException]].message has been
deprecated as of Python 2.6
  sMsg = "Error import Module \'osgeo\' from package \'gdal-Python-1.5.4-4\'"
\
Message: %s" % e.message
```

```
Loaded : Plugin Installer (package: plugin_installer)
Warning: QObject::connect: Incompatible sender/receiver arguments
    [[QgsProject]]::writeProject(QDomDocument&) --> [[QgisApp]]::projectChanged(QDomDocument)
[New Thread 0x7fffe233a910 (LWP 9138)]
[New Thread 0x7ffc7fff910 (LWP 9139)]
[New Thread 0x7ffc75f9910 (LWP 9140)]
[New Thread 0x7ffc6df8910 (LWP 9141)]
[Thread 0x7fffe233a910 (LWP 9138) exited]
[Thread 0x7ffc7fff910 (LWP 9139) exited]
[Thread 0x7ffc6df8910 (LWP 9141) exited]

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff6c178ed in QTextCodec::toUnicode(char const*) const () from /usr/lib/libQtCore.so.4
```

Associated revisions

Revision 707522e8 - 2010-11-02 06:42 PM - Jürgen Fischer

fix #2903

git-svn-id: <http://svn.osgeo.org/qgis/trunk/qgis@14490> c8812cc2-4d05-0410-92ff-de0c093fc19c

Revision 83421bfb - 2010-11-02 06:42 PM - Jürgen Fischer

fix #2903

git-svn-id: <http://svn.osgeo.org/qgis/trunk@14490> c8812cc2-4d05-0410-92ff-de0c093fc19c

History

#1 - 2010-07-23 01:22 AM - Jürgen Fischer

#2 - 2010-07-23 01:45 AM - aloba -

Replying to [comment:2 jef]:

Here:

```
GNU gdb (GDB) 7.0-ubuntu
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /usr/bin/qgis.bin...(no debugging symbols found)...done.
(gdb) run
```

```

Starting program: /usr/bin/qgis.bin
[Thread debugging using libthread_db enabled]
[New Thread 0x7fffe233a910 (LWP 9237)]
[Thread 0x7fffe233a910 (LWP 9237) exited]
Python support ENABLED :- )
/home/alobo/.qgis/python/plugins/imgboundary/+init+.py:38: [[DeprecationWarning]]: [[BaseException]].message has been deprecated as of
Python 2.6
  sMsg = "Error import Module \\osgeo\\ from package \\gdal-Python-1.5.4-4\\"
\
Message: %s" % e.message
Loaded : Plugin Installer (package: plugin_installer)
Warning: QObject::connect: Incompatible sender/receiver arguments
  [[QgsProject]]::writeProject(QDomDocument&) --> [[QgisApp]]::projectChanged(QDomDocument)
[New Thread 0x7fffe233a910 (LWP 9243)]
[New Thread 0x7ffc7fff910 (LWP 9244)]
[Thread 0x7fffe233a910 (LWP 9243) exited]

Program received signal SIGBUS, Bus error.
0x00007ffff6c178ed in QTextCodec::toUnicode(char const*) const () from /usr/lib/libQtCore.so.4
(gdb) bt
#0 0x00007ffff6c178ed in QTextCodec::toUnicode(char const*) const () from /usr/lib/libQtCore.so.4
#3905 0x00007ffdf2e7871 in [[QgsOgrProvider]]::loadFields() () from /usr/lib/qgis/libogrprovider.so
#3906 0x00007ffdf2ed362 in [[QgsOgrProvider]]::setSubsetString(QString) () from /usr/lib/qgis/libogrprovider.so
#3907 0x00007ffdf2f2eeb in [[QgsOgrProvider]]::QgsOgrProvider(QString const&) () from /usr/lib/qgis/libogrprovider.so
#3908 0x00007ffdf2f42f9 in classFactory () from /usr/lib/qgis/libogrprovider.so
#3909 0x00007ffff7742d26 in [[QgsProviderRegistry]]::getProvider(QString const&, QString const&) () from /usr/lib/libqgis_core.so.1.4.0
#3910 0x00007ffff776d9fd in [[QgsVectorLayer]]::setDataProvider(QString const&) () from /usr/lib/libqgis_core.so.1.4.0
#3911 0x00007ffff776e195 in [[QgsVectorLayer]]::readXml(QDomNode&) () from /usr/lib/libqgis_core.so.1.4.0
#3912 0x00007ffff7725f85 in [[QgsMapLayer]]::readXML(QDomNode&) () from /usr/lib/libqgis_core.so.1.4.0
#3913 0x00007ffff773243b in [[QgsProject]]::_getMapLayers(QDomDocument const&) () from /usr/lib/libqgis_core.so.1.4.0
#10 0x00007ffff7738e29 in [[QgsProject]]::read() () from /usr/lib/libqgis_core.so.1.4.0
#3914 0x00000000004c996d in [[QgisApp]]::fileOpen() ()
#3915 0x000000000069ae0d in [[QgisApp]]::qt_metacall(QMetaObject::Call, int, void**) ()
#3916 0x00007ffff6bfeddc in QMetaObject::activate(QObject*, int, int, void**) () from /usr/lib/libQtCore.so.4
#3917 0x00007ffff608c0a7 in QAction::triggered(bool) () from /usr/lib/libQtGui.so.4
#3918 0x00007ffff608d4ef in QAction::activate(QAction::ActionEvent) () from /usr/lib/libQtGui.so.4
#3919 0x00007ffff6479ecd in ?? () from /usr/lib/libQtGui.so.4
#3920 0x00007ffff647fdea in ?? () from /usr/lib/libQtGui.so.4
#3921 0x00007ffff60e09c0 in QWidget::event(QEvent*) () from /usr/lib/libQtGui.so.4
#3922 0x00007ffff64825ab in QMenu::event(QEvent*) () from /usr/lib/libQtGui.so.4
#3923 0x00007ffff6091efc in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/lib/libQtGui.so.4
#3924 0x00007ffff6099011 in QApplication::notify(QObject*, QEvent*) () from /usr/lib/libQtGui.so.4
#3925 0x00007ffff76ef0db in [[QgsApplication]]::notify(QObject*, QEvent*) () from /usr/lib/libqgis_core.so.1.4.0
#3926 0x00007ffff6be9c2c in QCoreApplication::notifyInternal(QObject*, QEvent*) () from /usr/lib/libQtCore.so.4
#3927 0x00007ffff60988e0 in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget*, QWidget**,
QPointer<QWidget>&) () from /usr/lib/libQtGui.so.4
#3928 0x00007ffff60fee2e in ?? () from /usr/lib/libQtGui.so.4
#3929 0x00007ffff60fdaa9 in QApplication::x11ProcessEvent(_XEvent*) () from /usr/lib/libQtGui.so.4
#3930 0x00007ffff6126d0c in ?? () from /usr/lib/libQtGui.so.4
#3931 0x00007ffff21c7bce in g_main_context_dispatch () from /lib/libglib-2.0.so.0
#3932 0x00007ffff21cb598 in ?? () from /lib/libglib-2.0.so.0
#3933 0x00007ffff21cb6c0 in g_main_context_iteration () from /lib/libglib-2.0.so.0
#3934 0x00007ffff6c121a6 in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4

```

```
#3935 0x00007ffff61264be in ?? () from /usr/lib/libQtGui.so.4
#3936 0x00007ffff6be8532 in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#3937 0x00007ffff6be8904 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#3938 0x00007ffff6beaab9 in QCoreApplication::exec() () from /usr/lib/libQtCore.so.4
#36 0x00000000004adc28 in main ()
(gdb)
```

#3 - 2010-07-23 02:57 AM - Jürgen Fischer

Replying to [comment:3 alobo]:


Here:

```
<pre>
GNU gdb (GDB) 7.0-ubuntu
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /usr/bin/qgis.bin...(no debugging symbols found)...done.
(gdb) run
Starting program: /usr/bin/qgis.bin
[Thread debugging using libthread_db enabled]
[New Thread 0x7fffe233a910 (LWP 9237)]
[Thread 0x7fffe233a910 (LWP 9237) exited]
Python support ENABLED :-)
/home/alobo/.qgis/python/plugins/imgboundary/+init+.py:38: [[DeprecationWarning]]: [[BaseException]].message has been deprecated as of
Python 2.6
  sMsg = "Error import Module \\osgeo\\" from package \\gdal-Python-1.5.4-4\\"
\
Message: %s" % e.message
Loaded : Plugin Installer (package: plugin_installer)
Warning: QObject::connect: Incompatible sender/receiver arguments
  [[QgsProject]]::writeProject(QDomDocument&) --> [[QgisApp]]::projectChanged(QDomDocument)
[New Thread 0x7fffe233a910 (LWP 9243)]
[New Thread 0x7fffc7fff910 (LWP 9244)]
```

[Thread 0x7ffe233a910 (LWP 9243) exited]

Program received signal SIGBUS, Bus error.

0x00007ffff6c178ed in QTextCodec::toUnicode(char const*) const () from /usr/lib/libQtCore.so.4

(gdb) bt

```
#0 0x00007ffff6c178ed in QTextCodec::toUnicode(char const*) const () from /usr/lib/libQtCore.so.4
#3905 0x00007ffff2e7871 in [[QgsOgrProvider]]::loadFields() () from /usr/lib/qgis/libogrprovider.so
#3906 0x00007ffff2ed362 in [[QgsOgrProvider]]::setSubsetString(QString) () from /usr/lib/qgis/libogrprovider.so
#3907 0x00007ffff2f2eeb in [[QgsOgrProvider]]::QgsOgrProvider(QString const&) () from /usr/lib/qgis/libogrprovider.so
#3908 0x00007ffff2f42f9 in classFactory () from /usr/lib/qgis/libogrprovider.so
#3909 0x00007ffff7742d26 in [[QgsProviderRegistry]]::getProvider(QString const&, QString const&) () from /usr/lib/libqgis_core.so.1.4.0
#3910 0x00007ffff776d9fd in [[QgsVectorLayer]]::setDataProvider(QString const&) () from /usr/lib/libqgis_core.so.1.4.0
#3911 0x00007ffff776e195 in [[QgsVectorLayer]]::readXml(QDomNode&) () from /usr/lib/libqgis_core.so.1.4.0
#3912 0x00007ffff7725f85 in [[QgsMapLayer]]::readXML(QDomNode&) () from /usr/lib/libqgis_core.so.1.4.0
#3913 0x00007ffff773243b in [[QgsProject]]::_getMapLayers(QDomDocument const&) () from /usr/lib/libqgis_core.so.1.4.0
#10 0x00007ffff7738e29 in [[QgsProject]]::read() () from /usr/lib/libqgis_core.so.1.4.0
#3914 0x00000000004c996d in [[QgisApp]]::fileOpen() ()
#3915 0x000000000069ae0d in [[QgisApp]]::qt_metacall(QMetaObject::Call, int, void**) ()
#3916 0x00007ffff6bfeddc in QMetaObject::activate(QObject*, int, int, void**) () from /usr/lib/libQtCore.so.4
#3917 0x00007ffff608c0a7 in QAction::triggered(bool) () from /usr/lib/libQtGui.so.4
#3918 0x00007ffff608d4ef in QAction::activate(QAction::ActionEvent) () from /usr/lib/libQtGui.so.4
#3919 0x00007ffff6479ecd in ?? () from /usr/lib/libQtGui.so.4
#3920 0x00007ffff647fdea in ?? () from /usr/lib/libQtGui.so.4
#3921 0x00007ffff60e09c0 in QWidget::event(QEvent*) () from /usr/lib/libQtGui.so.4
#3922 0x00007ffff64825ab in QMenu::event(QEvent*) () from /usr/lib/libQtGui.so.4
#3923 0x00007ffff6091efc in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/lib/libQtGui.so.4
#3924 0x00007ffff6099011 in QApplication::notify(QObject*, QEvent*) () from /usr/lib/libQtGui.so.4
#3925 0x00007ffff6ef0db in [[QgsApplication]]::notify(QObject*, QEvent*) () from /usr/lib/libqgis_core.so.1.4.0
#3926 0x00007ffff6be9c2c in QCoreApplication::notifyInternal(QObject*, QEvent*) () from /usr/lib/libQtCore.so.4
#3927 0x00007ffff60988e0 in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget*, QWidget**,
QPointer<QWidget>&) () from /usr/lib/libQtGui.so.4
#3928 0x00007ffff60fee2e in ?? () from /usr/lib/libQtGui.so.4
#3929 0x00007ffff60fdaa9 in QApplication::x11ProcessEvent(_XEvent*) () from /usr/lib/libQtGui.so.4
#3930 0x00007ffff6126d0c in ?? () from /usr/lib/libQtGui.so.4
#3931 0x00007ffff21c7bce in g_main_context_dispatch () from /lib/libglib-2.0.so.0
#3932 0x00007ffff21cb598 in ?? () from /lib/libglib-2.0.so.0
#3933 0x00007ffff21cb6c0 in g_main_context_iteration () from /lib/libglib-2.0.so.0
#3934 0x00007ffff6c121a6 in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#3935 0x00007ffff61264be in ?? () from /usr/lib/libQtGui.so.4
#3936 0x00007ffff6be8532 in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#3937 0x00007ffff6be8904 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#3938 0x00007ffff6beaab9 in QCoreApplication::exec() () from /usr/lib/libQtCore.so.4
#36 0x00000000004adc28 in main ()
(gdb)
</pre>
```

#4 - 2010-07-23 03:01 AM - Jürgen Fischer

Replying to [comment:3 alobo]:

```
> #0 0x00007ffff6c178ed in QTextCodec::toUnicode(char const*) const () from /usr/lib/libQtCore.so.4
> #3905 0x00007ffff2e7871 in [[QgsOgrProvider]]::loadFields() () from /usr/lib/qgis/libogrprovider.so
> #3906 0x00007ffff2ed362 in [[QgsOgrProvider]]::setSubsetString(QString) () from /usr/lib/qgis/libogrprovider.so
```

> #3907 0x00007ffdf2f2eeb in [[QgsOgrProvider]]::QgsOgrProvider(QString const&) () from /usr/lib/qgis/libogrprovider.so

Which encoding is selected in the 'add vector layer' dialog? And does that also happen, when you disable third party plugins? Anything special (eg. non-ascii characters in column names) in your shapefiles?

#5 - 2010-07-23 03:54 AM - alobo -

Seems to be solved: The problem occurred with any vector layer and the reason was that actually no encoding was selected by default, the box was empty. Once UTF8 is selected, vector layers and projects open normally (UTF8 keeps selected as default).

Actually, I do not know how to make that box empty again to double check. I think that plugin points2one made that happen at crashing and from then on I could not open any vector layer again.

Do you want me to do any further test using gdb to fully clarify the issue?

Thanks!

Agus

#6 - 2010-07-30 05:17 AM - Giovanni Manghi

this ticket can be closed?

#7 - 2010-08-01 11:42 AM - alobo -

Yes, I think so. The problem is caused by plugin points2one leaving the encoding box empty by default.

Agus

#8 - 2010-08-01 11:43 AM - alobo -

- Status changed from Open to Closed

- Resolution set to invalid

#9 - 2010-11-02 09:37 AM - marisn -

- Status changed from Closed to Feedback

- Resolution deleted (invalid)

Remind me - how it's NOT a bug?!? How "Add vector" dialog can turn into state where it offers no encoding that leads to crash at first place?!?

Work flow:

Create a new Shapefile with "Points2One" without specifying encoding (I had no attribute data and thus left it blank);

After crash, QGIS still has this empty encoding option active by default and it causes crash on any shapefile.

#10 - 2010-11-02 10:23 AM - alobo -

I'm away of the machine where I had the problem and cannot verify until Wedn.5/11/2010, but I bet this was again the problem, as I was actually running points2one just before the crash.

I understand I could have been wrong when I said that the ticket could be closed, but the fact is that this is an error in a plugin and this track does not follow errors on python plugins.

Nevertheless, as the consequence is very serious for the user and very hard for him/her to make the actual link to the plugin:

1. Could the author of points2one be asked to check the plugin and eventually do not keep it in the official repository until is fixed? Or at least, could a warning message be added to the plugin?
2. Could QGIS be made more robust to the fact that there is an empty space in the encoding field?

Agus

#11 - 2010-11-02 10:43 AM - Jürgen Fischer

crash fixed in commit:83421bfb (SVN r14491).

#12 - 2011-03-02 06:39 AM - Paolo Cavallini

- *Resolution set to fixed*

- *Status changed from Feedback to Closed*

It should be fixed. Please check against 1.6 or trunk, and reopen if still valid.