

QGIS Application - Bug report #11394

Crash while loading a map composer with a scale bar

2014-10-12 10:40 AM - marisn -

Status:	Closed	
Priority:	High	
Assignee:		
Category:	Map Composer/Printing	
Affected QGIS version:	master	Regression?: No
Operating System:		Easy fix?: No
Pull Request or Patch supplied:		Resolution: worksforme
Crashes QGIS or corrupts data:		Copied to github as #: 19677
Description		
Steps to reproduce: Create a new project and a map composer. Add a map and scale bar. Save project. Close and open project. Observe how scale bar is not rendered. Try to select objects in area of scale bar - crash! QGIS versija 2.5.0-Master QGIS koda revīzija c9cfdfa Program received signal SIGSEGV, Segmentation fault. 0x00007ffff4d863ba in QgsComposerScaleBar::update (this=0x48e9ab0) at /home/maris/soft/qgis_trunk/src/core/composer/qgscomposerscalebar.cpp:410 410 if (mStyle->name() != "Numeric") (gdb) bt #0 0x00007ffff4d863ba in QgsComposerScaleBar::update (this=0x48e9ab0) at /home/maris/soft/qgis_trunk/src/core/composer/qgscomposerscalebar.cpp:410 #1 0x00000000007ad896 in QgsComposerScaleBarWidget::on_mMapComboBox_activated (this=this@entry=0x3c804f0, text=...) at /home/maris/soft/qgis_trunk/src/app/composer/qgscomposerscalebarwidget.cpp:173 #2 0x00000000007adcd7 in QgsComposerScaleBarWidget::refreshMapComboBox (this=this@entry=0x3c804f0) at /home/maris/soft/qgis_trunk/src/app/composer/qgscomposerscalebarwidget.cpp:117 #3 0x00000000007ade01 in QgsComposerScaleBarWidget::showEvent (this=0x3c804f0, event=0x7fffffb810) at /home/maris/soft/qgis_trunk/src/app/composer/qgscomposerscalebarwidget.cpp:128 #4 0x00007ffff2d977e5 in QWidget::event(QEvent*) () from /usr/lib64/qt4/libQtGui.so.4 #5 0x00007ffff2d4866c in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/lib64/qt4/libQtGui.so.4 #6 0x00007ffff2d4ebf0 in QApplication::notify(QObject*, QEvent*) () from /usr/lib64/qt4/libQtGui.so.4 #7 0x00007ffff4b25b1b in QgsApplication::notify (this=0x7fffffd380, receiver=0x3c804f0, event=0x7fffffb810) at /home/maris/soft/qgis_trunk/src/core/qgsapplication.cpp:243 #8 0x00007ffff397d04d in QCoreApplication::notifyInternal(QObject*, QEvent*) () from /usr/lib64/qt4/libQtCore.so.4 #9 0x00007ffff2d94f4f in QWidgetPrivate::show_helper() () from /usr/lib64/qt4/libQtGui.so.4 #10 0x00007ffff2d96bf4 in QWidget::setVisible(bool) () from /usr/lib64/qt4/libQtGui.so.4 #11 0x00007ffff3102643 in QDockWidgetLayout::setWidgetForRole(QDockWidgetLayout::Role, QWidget*) () from /usr/lib64/qt4/libQtGui.so.4 #12 0x000000000083dbb1 in QgsComposer::qt_static_metacall (_o=0x7fffffb2c0, _c=QMetaObject::InvokeMetaMethod, _id=15827040, _a=0x1) at /home/maris/soft/qgis_trunk/build/src/app/composer/moc_qgscomposer.cxx:383 #13 0x00007ffff3990cba in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/lib64/qt4/libQtCore.so.4 #14 0x00007ffff454afaf in QgsComposerView::selectedItemChanged (this=this@entry=0x3c3c560, _t1=0x48e9ab0)		

```

at /home/maris/soft/qgis_trunk/build/src/gui/moc_qgscomposerview.cxx:118
#15 0x00007ffff4468d73 in QgsComposerView::endMarqueeSelect (this=this@entry=0x3c3c560, e=e@entry=0x7fffffc300)
    at /home/maris/soft/qgis_trunk/src/gui/qgscomposerview.cpp:566
#16 0x00007ffff446cb03 in QgsComposerView::mouseReleaseEvent (this=0x3c3c560, e=0x7fffffc300)
    at /home/maris/soft/qgis_trunk/src/gui/qgscomposerview.cpp:693
#17 0x00007ffff2d97a4a in QWidget::event(QEvent*) () from /usr/lib64/qt4/libQtGui.so.4
#18 0x00007ffff31145fe in QFrame::event(QEvent*) () from /usr/lib64/qt4/libQtGui.so.4
#19 0x00007ffff331f5e9 in QGraphicsView::viewportEvent(QEvent*) () from /usr/lib64/qt4/libQtGui.so.4
#20 0x00007ffff397d1b6 in QCoreApplicationPrivate::sendThroughObjectEventFilters(QObject*, QEvent*) ()
---Type <return> to continue, or q <return> to quit---
    from /usr/lib64/qt4/libQtCore.so.4
#21 0x00007ffff2d4864c in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/lib64/qt4/libQtGui.so.4
#22 0x00007ffff2d4ed2d in QApplication::notify(QObject*, QEvent*) () from /usr/lib64/qt4/libQtGui.so.4
#23 0x00007ffff4b25b1b in QgsApplication::notify (this=0x7fffffd380, receiver=0x2d48b80, event=0x7fffffc300)
    at /home/maris/soft/qgis_trunk/src/core/qgsapplication.cpp:243
#24 0x00007ffff397d04d in QCoreApplication::notifyInternal(QObject*, QEvent*) () from /usr/lib64/qt4/libQtCore.so.4
#25 0x00007ffff2d4e4e3 in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget*, QWidget**,
    QPointer<QWidget>&, bool) () from /usr/lib64/qt4/libQtGui.so.4
#26 0x00007ffff2dbf59b in QETWidget::translateMouseEvent(_XEvent const*) () from /usr/lib64/qt4/libQtGui.so.4
#27 0x00007ffff2dbe00c in QApplication::x11ProcessEvent(_XEvent*) () from /usr/lib64/qt4/libQtGui.so.4
#28 0x00007ffff2de4bc2 in x11EventSourceDispatch(_GSource*, int (*)(void*), void*) () from /usr/lib64/qt4/libQtGui.so.4
#29 0x00007ffff0fd3934 in g_main_context_dispatch () from /usr/lib64/libglib-2.0.so.0
#30 0x00007ffff0fd3b78 in g_main_context_iterate.isra () from /usr/lib64/libglib-2.0.so.0
#31 0x00007ffff0fd3c1c in g_main_context_iteration () from /usr/lib64/libglib-2.0.so.0
#32 0x00007ffff39a9b9e in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) ()
    from /usr/lib64/qt4/libQtCore.so.4
#33 0x00007ffff2de4c76 in QGuiEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) ()
    from /usr/lib64/qt4/libQtGui.so.4
#34 0x00007ffff397bc9f in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) ()
    from /usr/lib64/qt4/libQtCore.so.4
#35 0x00007ffff397bf95 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib64/qt4/libQtCore.so.4
#36 0x00007ffff39810a9 in QCoreApplication::exec() () from /usr/lib64/qt4/libQtCore.so.4
#37 0x00000000004fc7c4 in main (argc=1, argv=<optimized out>) at /home/maris/soft/qgis_trunk/src/app/main.cpp:1017

```

```

#0 0x00007ffff4d863ba in QgsComposerScaleBar::update (this=0x48e9ab0)
    at /home/maris/soft/qgis_trunk/src/core/composer/qgscomposerscalebar.cpp:410
No locals.

```

```

#1 0x00000000007ad896 in QgsComposerScaleBarWidget::on_mMapComboBox_activated (this=this@entry=0x3c804f0,
    text=...)

```

```

    at /home/maris/soft/qgis_trunk/src/app/composer/qgscomposerscalebarwidget.cpp:173
    conversionOk = true
    textSplit = {<QList<QString>> = {{p = {static shared_null = {ref = {_q_value = 13453}, alloc = 0, begin = 0,
        end = 0, sharable = 1, array = {0x0}}, d = 0x4732360}, d = 0x4732360}}, <No data fields>}}
    idString = {static null = {<No data fields>}, static shared_null = {ref = {_q_value = 73222}, alloc = 0,
        size = 0, data = 0xda865a <QString::shared_null+26>, clean = 0, simpletext = 0, righttoleft = 0,
        asciiCache = 0, capacity = 0, reserved = 0, array = {0}}, static shared_empty = {ref = {_q_value = 712},
        alloc = 0, size = 0, data = 0x7ffff3ce18fa <QString::shared_empty+26>, clean = 0, simpletext = 0,
        righttoleft = 0, asciiCache = 0, capacity = 0, reserved = 0, array = {0}}, d = 0x3cb81b0,
        static codecForCStrings = 0x0}
    id = <optimized out>
    composerMap = 0x3d554f0

```

```
#2 0x0000000007adcd7 in QgsComposerScaleBarWidget::refreshMapComboBox (this=this@entry=0x3c804f0)
at /home/maris/soft/qgis_trunk/src/app/composer/qgscomposerscalebarwidget.cpp:117
    saveCurrentComboText = {static null = {<No data fields>}, static shared_null = {ref = {_q_value = 73222},
    alloc = 0, size = 0, data = 0xda865a <QString::shared_null+26>, clean = 0, simpletext = 0, righttoleft = 0,
    asciiCache = 0, capacity = 0, reserved = 0, array = {0}}, static shared_empty = {ref = {_q_value = 712},
    alloc = 0, size = 0, data = 0xffff3ce18fa <QString::shared_empty+26>, clean = 0, simpletext = 0,
    righttoleft = 0, asciiCache = 0, capacity = 0, reserved = 0, array = {0}},
    d = 0xda8640 <QString::shared_null>, static codecForCStrings = 0x0}
#3 0x00000000007ade01 in QgsComposerScaleBarWidget::showEvent (this=0x3c804f0, event=0x7fffffb810)
at /home/maris/soft/qgis_trunk/src/app/composer/qgscomposerscalebarwidget.cpp:128
No locals.
#4 0x00007ffff2d977e5 in QWidget::event(QEvent*) () from /usr/lib64/qt4/libQtGui.so.4
```

Associated revisions

Revision 9f063df8 - 2014-10-13 01:53 PM - Nyal Dawson

[composer] Fix possible crash in scale bar update (refs #11394)

History

#1 - 2014-10-12 10:53 AM - marisn -

Valgrind output doesn't give anything more:

```
src/core/qgscoordinatereferencesystem.cpp: 992: (setMapUnits) Projection has linear units of metre
src/core/qgsdistancearea.cpp: 212: (setEllipsoid) setEllipsoid: a=6.37814e+06, b=6.35675e+06, 1/f=298.257
src/core/qgscoordinatereferencesystem.cpp: 522: (createFromProj4) proj4: +proj=longlat +ellps=WGS84 +no_defs
src/core/qgscoordinatereferencesystem.cpp: 552: (createFromProj4) proj string supplied has no +a argument
src/core/qgscoordinatereferencesystem.cpp: 719: (getRecord) running query: select * from tbl_srs where parameters='+proj=longlat
+ellps=WGS84 +no_defs' order by deprecated
src/core/qgscoordinatereferencesystem.cpp: 740: (getRecord) trying system srs.db
src/core/qgscoordinatereferencesystem.cpp: 751: (getRecord) Multiple records found in srs.db
src/core/qgscoordinatereferencesystem.cpp: 762: (getRecord) trying user qgis.db
src/core/qgscoordinatereferencesystem.cpp: 803: (getRecord) failed : select * from tbl_srs where parameters='+proj=longlat +ellps=WGS84
+no_defs' order by deprecated
src/core/qgscoordinatereferencesystem.cpp: 810: (getRecord) retrieved: select * from tbl_srs where parameters='+proj=longlat +ellps=WGS84
+no_defs' order by deprecated
src/core/qgscoordinatereferencesystem.cpp: 719: (getRecord) running query: SELECT * FROM tbl_srs WHERE '||parameters||' LIKE '%
+proj=longlat %' AND '||parameters||' LIKE '% +ellps=WGS84 %' AND '||parameters||' LIKE '% +no_defs %' order by deprecated
src/core/qgscoordinatereferencesystem.cpp: 740: (getRecord) trying system srs.db
src/core/qgscoordinatereferencesystem.cpp: 751: (getRecord) Multiple records found in srs.db
src/core/qgscoordinatereferencesystem.cpp: 762: (getRecord) trying user qgis.db
src/core/qgscoordinatereferencesystem.cpp: 803: (getRecord) failed : SELECT * FROM tbl_srs WHERE '||parameters||' LIKE '% +proj=longlat
%' AND '||parameters||' LIKE '% +ellps=WGS84 %' AND '||parameters||' LIKE '% +no_defs %' order by deprecated
src/core/qgscoordinatereferencesystem.cpp: 810: (getRecord) retrieved: SELECT * FROM tbl_srs WHERE '||parameters||' LIKE '%
+proj=longlat %' AND '||parameters||' LIKE '% +ellps=WGS84 %' AND '||parameters||' LIKE '% +no_defs %' order by deprecated
src/core/qgscoordinatereferencesystem.cpp: 682: (createFromProj4) globbing search for srsid from this proj string
src/core/qgscoordinatereferencesystem.cpp: 1030: (findMatchingProj) entered.
src/core/qgscoordinatereferencesystem.cpp: 1072: (findMatchingProj) -----> MATCH FOUND in srs.db srsid: 3239
src/core/qgscoordinatereferencesystem.cpp: 685: (createFromProj4) globbing search for srsid returned srsid: 3239
==19228== Invalid read of size 8
```

```

==19228== at 0x7F023BA: QgsComposerScaleBar::update() (qgscomposerscalebar.cpp:410)
==19228== by 0x7AD895: QgsComposerScaleBarWidget::on_mMapComboBox_activated(QString const&)
(qgscomposerscalebarwidget.cpp:173)
==19228== by 0x7ADCD6: QgsComposerScaleBarWidget::refreshMapComboBox() (qgscomposerscalebarwidget.cpp:117)
==19228== by 0x7ADE00: QgsComposerScaleBarWidget::showEvent(QShowEvent*) (qgscomposerscalebarwidget.cpp:128)
==19228== by 0x96207E4: QWidget::event(QEvent*) (in /usr/lib64/qt4/libQtGui.so.4.8.5)
==19228== by 0x95D166B: QApplicationPrivate::notify_helper(QObject*, QEvent*) (in /usr/lib64/qt4/libQtGui.so.4.8.5)
==19228== by 0x95D7BEF: QApplication::notify(QObject*, QEvent*) (in /usr/lib64/qt4/libQtGui.so.4.8.5)
==19228== by 0x7CA1B1A: QgsApplication::notify(QObject*, QEvent*) (qgsapplication.cpp:243)
==19228== by 0x90A404C: QCoreApplication::notifyInternal(QObject*, QEvent*) (in /usr/lib64/qt4/libQtCore.so.4.8.5)
==19228== by 0x961DF4E: QWidgetPrivate::show_helper() (in /usr/lib64/qt4/libQtGui.so.4.8.5)
==19228== by 0x961FBF3: QWidget::setVisible(bool) (in /usr/lib64/qt4/libQtGui.so.4.8.5)
==19228== by 0x998B642: QDockWidgetLayout::setWidgetForRole(QDockWidgetLayout::Role, QWidget*) (in /usr/lib64/qt4/libQtGui.so.4.8.5)
==19228== Address 0x0 is not stack'd, malloc'd or (recently) free'd
==19228==
QGIS died on signal 11[Current thread is 1 (process 19228)]

```

#2 - 2014-10-12 12:40 PM - Giovanni Manghi

- Status changed from Open to Feedback

Cannot confirm on QGIS master on Ubuntu 14.04. Please attach a project (and sample data). Cheers!

#3 - 2014-10-12 01:21 PM - Nyal Dawson

I can't reproduce this either, on Windows 7 64 bit.

#4 - 2014-10-12 03:20 PM - marisn -

- File *qgis_missing_scale_bar.jpeg* added
 - File *comp_crash.zip* added

On my Gentoo ~AMD64 Linux system I can crash it always. Could be some configuration switches / GCC flags to blame?

Attachment contains a project and data file to make QGIS crash.

Unzip attachment; Open project in QGIS; Go to "Print composer"; Use select tool to select the lowest square. If necessary, try to move the invisible scale bar, that will appear as a selected rectangle inside the drawn rectangle. CRASH.

#5 - 2014-10-13 12:23 AM - Giovanni Manghi

marisn - wrote:

On my Gentoo ~AMD64 Linux system I can crash it always. Could be some configuration switches / GCC flags to blame?

Attachment contains a project and data file to make QGIS crash.

Unzip attachment; Open project in QGIS; Go to "Print composer"; Use select tool to select the lowest square. If necessary, try to move the invisible

| scale bar, that will appear as a selected rectangle inside the drawn rectangle. CRASH.

tested with your project here on master/ubuntu 14.04, it works all as expected and no crash.

#6 - 2014-10-13 03:24 AM - marisn -

Seems that the crash is related to something specific on my system / my GCC / compilation parameters.

I managed to work around the issue. Following code change makes the problem to disappear. I am not certain if it fixes the root cause, still it allows me to load a project with a scale bar in composer.

```
diff --git a/src/core/composer/qgscomposerscalebar.cpp b/src/core/composer/qgscomposerscalebar.cpp
index b76e3f8..f2ceee1 100644
--- a/src/core/composer/qgscomposerscalebar.cpp
+++ b/src/core/composer/qgscomposerscalebar.cpp
@@ -407,7 +407,7 @@ void QgsComposerScaleBar::adjustBoxSize()
void QgsComposerScaleBar::update()
{
    //Don't adjust box size for numeric scale bars:
-   if ( mStyle->name() != "Numeric" )
+   if ( mStyle && mStyle->name() != "Numeric" )
    {
        adjustBoxSize();
    }
```

I also noticed that there are a lot of logging related stack traces reported while Composer is open. They happen without and with aforementioned code change. No idea if could be related or just harmless chatter.

```
Warning: QPainter::setCompositionMode: Blend modes not supported on device
Stacktrace (piped through c++filt):
/home/maris/soft/qgis_bin/bin/qgis[0x50209e]
/home/maris/soft/qgis_bin/bin/qgis(myMessageOutput(QtMsgType, char const*)+0x14f)[0x50252f]
/usr/lib64/qt4/libQtCore.so.4(qt_message_output(QtMsgType, char const*)+0x16)[0x8f9a756]
/usr/lib64/qt4/libQtCore.so.4(+0x70929)[0x8f9a929]
/usr/lib64/qt4/libQtCore.so.4(qWarning(char const*, ...)+0x94)[0x8f9ab74]
/home/maris/soft/qgis_bin/lib/libqgis_core.so.2.5.0(QgsComposerMouseHandles::drawSelectedItemBounds(QPainter*)+0x59)[0x7eac6e9]
/usr/lib64/qt4/libQtGui.so.4(+0x780e57)[0x9b8ae57]
/usr/lib64/qt4/libQtGui.so.4(+0x781c15)[0x9b8bc15]
/usr/lib64/qt4/libQtGui.so.4(+0x7822c6)[0x9b8c2c6]
/usr/lib64/qt4/libQtGui.so.4(QGraphicsView::paintEvent(QPaintEvent*)+0x4de)[0x9ba97de]
/home/maris/soft/qgis_bin/lib/libqgis_gui.so.2.5.0(QgsComposerView::paintEvent(QPaintEvent*)+0x15)[0x860f9d5]
/usr/lib64/qt4/libQtGui.so.4(QWidget::event(QEvent*)+0x8b0)[0x9620830]
/usr/lib64/qt4/libQtGui.so.4(QFrame::event(QEvent*)+0x1e)[0x999d5fe]
/usr/lib64/qt4/libQtGui.so.4(QGraphicsView::viewportEvent(QEvent*)+0x179)[0x9ba85e9]
/usr/lib64/qt4/libQtCore.so.4(QCoreApplicationPrivate::sendThroughObjectEventFilters(QObject*, QEvent*)+0x86)[0x90a41b6]
/usr/lib64/qt4/libQtGui.so.4(QApplicationPrivate::notify_helper(QObject*, QEvent*)+0x6c)[0x95d164c]
/usr/lib64/qt4/libQtGui.so.4(QApplication::notify(QObject*, QEvent*)+0x270)[0x95d7bf0]
/home/maris/soft/qgis_bin/lib/libqgis_core.so.2.5.0(QgsApplication::notify(QObject*, QEvent*)+0x5b)[0x7ca1d1b]
/usr/lib64/qt4/libQtCore.so.4(QCoreApplication::notifyInternal(QObject*, QEvent*)+0x6d)[0x90a404d]
```

```
/usr/lib64/qt4/libQtGui.so.4(QWidgetPrivate::drawWidget(QPaintDevice*, QRegion const&, QPoint const&, int, QPainter*,
QWidgetBackingStore*)+0x571)[0x961af51]
src/core/qgsmessagelog.cpp: 45: (logMessage) 2014-10-13T11:50:44 Qt[1] QPainter::setCompositionMode: Blend modes not supported on
device
```

#7 - 2014-10-13 04:56 AM - Nyal Dawson

marisn: I've pushed that change- thanks. But it looks like there's something quite strange with your install. Those "Blend modes not supported on device" log messages definitely aren't normal. Can you let me know:

- your Qt version
- your graphics card and what driver you are using
- kernel/xorg/mesa version

#8 - 2014-10-13 10:34 AM - marisn -

Nyal Dawson wrote:

```
marisn: I've pushed that change- thanks. But it looks like there's something quite strange with your install. Those "Blend modes not supported on
device" log messages definitely aren't normal. Can you let me know:
- your Qt version
- your graphics card and what driver you are using
- kernel/xorg/mesa version
```

```
dev-qt/qtcore-4.8.5-r2:4
Chipset: "NVIDIA NV98"
AIGLX: reverting to software rendering
GLX: Initialized DRISWRAST GL provider for screen 0
Module nouveau: vendor="X.Org Foundation"
compiled for 1.16.1, module version = 1.0.10
ABI class: X.Org Video Driver, version 18.0
X.Org X Server 1.16.1
Kernel 3.17.0-gentoo
media-libs/mesa-10.3.0
```

I don't have a hardware acceleration as Nouveau wasn't playing nice with my chip and acceleration on suspend/resume etc.

#9 - 2014-10-18 04:29 PM - Nyal Dawson

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

```
I don't have a hardware acceleration as Nouveau wasn't playing nice with my chip and acceleration on suspend/resume etc.
```

I suspect that's your problem. I'm going to close this issue as it looks like a local issue -- please reopen if you can reproduce this on a different workstation.

Files

rm_scalebar_crash.qgs	12.7 KB	2014-10-12	marisn -
comp_crash.zip	8.85 KB	2014-10-12	marisn -
qgis_missing_scale_bar.jpeg	101 KB	2014-10-12	marisn -