

QGIS Application - Bug report #7835

Opening WMS layer properties crashes QGIS

2013-05-15 09:51 AM - Anita Graser

Status:	Closed	
Priority:	Severe/Regression	
Assignee:		
Category:	Web Services clients/WMS	
Affected QGIS version:	master	Regression?: No
Operating System:		Easy fix?: No
Pull Request or Patch supplied:	No	Resolution:
Crashes QGIS or corrupts data:	Yes	Copied to github as #: 16717
Description		
Tested with today's nightly on Win 7 and different layers from http://data.wien.gv.at/daten/wms		

Associated revisions

Revision ce49b666 - 2013-05-17 11:09 PM - Larry Shaffer

Fix #7835, opening WMS layer properties causes crash

History

#1 - 2013-05-16 03:59 AM - Giovanni Manghi

confirmed here

gio@sibirica ~ \$ qgis

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

Fatal: QGIS died on signal 11

Stacktrace (run through c++filt):

```
/usr/bin/qgis.bin(Z15myMessageOutput9QtMsgTypePKc+0xac)[0x4e766c]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_Z17qt_message_output9QtMsgTypePKc+0x2e)[0x7f6078b9d41e]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(+0x718bf)[0x7f6078b9d8bf]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_Z6qFatalPKcz+0x94)[0x7f6078b9da64]
/lib/x86_64-linux-gnu/libc.so.6(+0x364a0)[0x7f607608e4a0]
/usr/lib/libqgis_gui.so.1.9.0(_ZN20QgsOptionsDialogBase20restoreOptionsBaseUiEv+0x3de)[0x7f607969a59e]
/usr/bin/qgis.bin(_ZN24QgsRasterLayerPropertiesC1EP11QgsMapLayerP12QgsMapCanvasP7QWidget6QFlagsIN2Qt10WindowTypeEE+0x1d31)[0xb9081]
/usr/bin/qgis.bin(_ZN7QgisApp19showLayerPropertiesEP11QgsMapLayer+0x281)[0x512771]
/usr/bin/qgis.bin(_ZN9QgsLegend21mouseDoubleClickEventEP11QMouseEvent+0x87)[0x74bd17]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN7QWidget5eventEP6QEvent+0x69e)[0x7f607807a15e]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN6QFrame5eventEP6QEvent+0x26)[0x7f607843a3b6]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN17QAbstractItemView13viewportEventEP6QEvent+0x3eb)[0x7f607854e89b]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN9QTreeView13viewportEventEP6QEvent+0x135)[0x7f60785964b5]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN23QCoreApplicationPrivate29sendThroughObjectEventFiltersEP7QObjectP6QEvent+0x88)[0x7f6078ca708]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN19QApplicationPrivate13notify_helperEP7QObjectP6QEvent+0x7f)[0x7f607802985f]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN12QApplication6notifyEP7QObjectP6QEvent+0xabf)[0x7f607802f0bf]
/usr/lib/libqgis_core.so.1.9.0(_ZN14QgsApplication6notifyEP7QObjectP6QEvent+0x96)[0x7f6079b9c9a6]
```

```

/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN16QCoreApplication14notifyInternalEP7QObjectP6QEvent+0x8c)[0x7f6078ca6e9c]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN19QApplicationPrivate14sendMouseEventEP7QWidgetP11QMouseEventS1_S1_PS1_R8QPointerIS0_Eb0x172)[0x7f607802a862]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x24bbf5)[0x7f60780a9bf5]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(_ZN12QApplication15x11ProcessEventEP7_XEvent+0xdce)[0x7f60780a8bae]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x2740d2)[0x7f60780d20d2]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_dispatch+0x133)[0x7f6074bbad53]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(+0x480a0)[0x7f6074bbb0a0]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_iteration+0x34)[0x7f6074bbb164]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN20QEventDispatcherGlib13processEventsE6QFlagsIN10QEventLoop17ProcessEventsFlagEE+0x6f)[0x7f078cd63bf]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x273d5e)[0x7f60780d1d5e]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN10QEventLoop13processEventsE6QFlagsINS_17ProcessEventsFlagEE+0x32)[0x7f6078ca5c82]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN10QEventLoop4execE6QFlagsINS_17ProcessEventsFlagEE+0xf7)[0x7f6078ca5ed7]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(_ZN16QCoreApplication4execEv+0x87)[0x7f6078caaf67]
/usr/bin/qgis.bin(main+0x229e)[0x4e361e]
/lib/x86_64-linux-gnu/libc.so.6(_libc_start_main+0xed)[0x7f607607976d]
/usr/bin/qgis.bin[0x4e7411]
Aborted (core dumped)

```

#2 - 2013-05-16 04:03 AM - Anita Graser

- Crashes QGIS or corrupts data changed from No to Yes

#3 - 2013-05-16 09:00 AM - Radim Blazek

- Status changed from Open to Feedback

Works for me on Debian and Win XP.

It seems to crash in QgsOptionsDialogBase::restoreOptionsBaseUi where I see some really dangerous code:

```

int curIdx = settings.value( QString( "/Windows/%1/tab" ) ).arg( mOptsKey ), 0 ).toInt();
if ( !mOptStackedWidget->widget( curIdx )->isEnabled()

```

It means that if in settings was stored higher index than how many widgets are present, mOptStackedWidget->widget(curIdx) returns null and it must crash.

Could you please try to open regular local raster (tif), open its properties, select "General" widget (tab), close properties, try to open properties of wms layer.

#4 - 2013-05-16 09:14 AM - Giovanni Manghi

Could you please try to open regular local raster (tif), open its properties, select "General" widget (tab), close properties, try to open properties of wms layer.

does not crash

#5 - 2013-05-16 11:44 AM - Larry Shaffer

- File 7835_options-tab-out-of-range_patch.diff added

Thank you Radim for contacting me about this,

Yes, my mistake. I got the logic expression shortcuting in the wrong order for that conditional. Please try attached patch (works fine here).

#6 - 2013-05-17 02:09 PM - Larry Shaffer

- Status changed from Feedback to Closed

Fixed in changeset commit:"ce49b66673c66c5c4aab84a62e7b471e85fedf71".

Files

7835_options-tab-out-of-range_patch.diff	1.13 KB	2013-05-16	Larry Shaffer
--	---------	------------	---------------