QGIS Application - Bug report #14462
QGIS crash on typing "$x_at" in expression.

2016-03-11 11:10 AM - barryrowlingson -

Status:	Closed		
Priority:	High		
Assignee:			
Category:	Expressions		
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 #:**	22440

Description

Start QGIS (2.14 LTS), open any shapefile.

Go to "Select by expression" and type $x_at (as is, no quote marks) in the expression box. QGIS immediately crashes with an ASSERT failure:

Fatal: ASSERT failure in QList<T>::at: "index out of range", file /usr/include/qt4/QtCore/qlist.h, line 469
Stacktrace (piped through c++filt):
Aborted
/usr/bin/qgis.bin[0x40a440]
/usr/bin/qgis.bin[0x40a548]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(qt_message_output(QtMsgType, char const*)+0x21)[0x7f5c62a59bb1]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(+0x70ff9)[0x7f5c62a59ff9]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(qFatal(char const*, ...)+0x94)[0x7f5c62a5a804]
/usr/lib/libqgis_core.so.2.14.0(+0x3305a6)[0x7f5c631fe5a6]
/usr/lib/libqgis_core.so.2.14.0(+0x3308c4)[0x7f5c631fe8c4]
/usr/lib/libqgis_core.so.2.14.0(+0x3333c7)[0x7f5c632013c7]
/usr/lib/libqgis_core.so.2.14.0(QgsExpression::NodeFunction::eval(QgsExpression*, QgsExpressionContext const*)+0x1f3)[0x7f5c631fa163]
/usr/lib/libqgis_core.so.2.14.0(QgsExpression::evaluate(QgsExpressionContext const*)+0x5b)[0x7f5c631c36cb]
/usr/lib/libqgis_gui.so.2.14.0(QgsExpressionBuilderWidget::on_txtExpressionString_textChanged()+0x226)[0x7f5c63cb7df6]
/usr/lib/libqgis_gui.so.2.14.0(QgsExpressionBuilderWidget::qt_metacall(QMetaObject::Call, int, void**)+0x33)[0x7f5c63d7e943]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QMetaObject::activate(QObject*, QMetaObject const*, int, void**)+0x4d8)[0x7f5c62b7aa78]
/usr/lib/libqscintilla2.so.11(QsciScintilla::handleModified(int, int, char const*, int, int, int, int, int, int)+0x40)[0x7f5c5d77add0]
/usr/lib/libqscintilla2.so.11(+0x2818bc)[0x7f5c5d9838bc]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QMetaObject::activate(QObject*, QMetaObject const*, int, void**)+0x2da)[0x7f5c62b7a87a]
/usr/lib/libqscintilla2.so.11(QsciScintillaBase::SCN_MODIFIED(int, int, char const*, int, int, int, int, int, int, int)+0xbc)[0x7f5c5d98471c]
/usr/lib/libqscintilla2.so.11(QsciScintillaQt::NotifyParent(SCNotification)+0x544)[0x7f5c5d7ad444]
/usr/lib/libqscintilla2.so.11(Editor::NotifyModified(Document*, DocModification, void*)+0x500)[0x7f5c5d963ca0]
/usr/lib/libqscintilla2.so.11(Document::NotifyModified(DocModification)+0xaf)[0x7f5c5d949b8f]
/usr/lib/libqscintilla2.so.11(Document::InsertString(int, char const*, int)+0x1dd)[0x7f5c5d94a5ed]
/usr/lib/libqscintilla2.so.11(Editor::AddCharUTF(char*, unsigned int, bool)+0x230)[0x7f5c5d965a10]
/usr/lib/libqscintilla2.so.11(ScintillaBase::AddCharUTF(char*, unsigned int, bool)+0x42)[0x7f5c5d97d592]
/usr/lib/libqscintilla2.so.11(QsciScintillaBase::keyPressEvent(QKeyEvent*)+0x193)[0x7f5c5d782b63]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QWidget::event(QEvent*)+0x994)[0x7f5c61f4f3e4]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QFrame::event(QEvent*)+0x1e)[0x7f5c622f104e]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QAbstractScrollArea::event(QEvent*)+0x2bb)[0x7f5c6236d4ab]
/usr/lib/libqscintilla2.so.11(QsciScintilla::event(QEvent*)+0x22)[0x7f5c5d780e22]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QApplicationPrivate::notify_helper(QObject*, QEvent*)+0x8c)[0x7f5c61effe2c]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QApplication::notify(QObject*, QEvent*)+0x14c1)[0x7f5c61f076f1]

/usr/lib/libqgis_core.so.2.14.0(QgsApplication::notify(QObject*, QEvent*)+0x5b)[0x7f5c6316739b]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QCoreApplication::notifyInternal(QObject*, QEvent*)+0x6d)[0x7f5c62b664dd]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x269027)[0x7f5c61f9f027]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x2693c9)[0x7f5c61f9f3c9]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(QApplication::x11ProcessEvent(*XEvent*)+0x6e7)[0x7f5c61f79417]*
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x26bb32)[0x7f5c61fa1b32]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_dispatch+0x254)[0x7f5c5ae0ee04]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(+0x49048)[0x7f5c5ae0f048]
/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_iteration+0x2c)[0x7f5c5ae0f0ec]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)+0x71)[0x
f5c62b937a1]
/usr/lib/x86_64-linux-gnu/libQtGui.so.4(+0x26bbe6)[0x7f5c61fa1be6]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>)+0x2f)[0x7f5c62b65
af]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>)+0x175)[0x7f5c62b653a5]
/usr/lib/x86_64-linux-gnu/libQtCore.so.4(QCoreApplication::exec()+0x89)[0x7f5c62b6ab79]
/usr/bin/qgis.bin[0x406fd7]
*/lib/x86_64-linux-gnu/libc.so.6(*__libc_start_main+0xf5)[0x7f5c61478ec5]
/usr/bin/qgis.bin[0x409d48]

Does it with $x_at in every expression box I've tried. I've run it from a fresh .qgis2 folder to eliminate plugin problems. Still does it.

QGIS About:

QGIS version
2.14.0-Essen
QGIS code revision
exported
Compiled against Qt
4.8.6
Running against Qt
4.8.6
Compiled against GDAL/OGR
1.10.1
Running against GDAL/OGR
1.10.1
Compiled against GEOS
3.4.2-CAPI-1.8.2
Running against GEOS
3.4.2-CAPI-1.8.2 r3921
PostgreSQL Client Version
9.3.4
SpatiaLite Version
4.1.1
QWT Version
5.2.3
PROJ.4 Version
480
QScintilla2 Version
2.8.1

Associated revisions

Revision 3b40e2ba - 2016-03-12 10:21 AM - Nyall Dawson

Fix broken $x_at, $y_at functions (fix #14462), add tests

Revision 35ceacc8 - 2016-03-12 10:23 AM - Nyall Dawson

Fix broken $x_at, $y_at functions (fix #14462), add tests

(cherry-picked from 3b40e2baa5b939dd4b920220e266a98cf9ef0e4c)

History

#1 - 2016-03-11 01:39 PM - Barend Kobben

Exactly same behaviour on Mac OSX (Yosemite, 10.10.5)

#2 - 2016-03-12 01:07 AM - Anita Graser

- Affected QGIS version changed from 2.14.0 to master

- Priority changed from Normal to High

Confirmed on master with today's nightly on OSGeo4W

#3 - 2016-03-12 01:21 AM - Nyall Dawson

- Status changed from Open to Closed

Fixed in changeset commit:"3b40e2baa5b939dd4b920220e266a98cf9ef0e4c".