

QGIS Application - Bug report #6877

qgis_expressiontest failure in testsuite

2012-12-14 09:15 AM - Sandro Santilli

Status:	Closed	
Priority:	Normal	
Assignee:		
Category:		
Affected QGIS version:	master	Regression?: No
Operating System:		Easy fix?: No
Pull Request or Patch supplied:		Resolution:
Crashes QGIS or corrupts data:		Copied to github as #: 16006
Description		
I've run it through valgrind: <pre>==26967== Conditional jump or move depends on uninitialised value(s) ==26967== at 0x57D05B9: fcnMonth(QList<QVariant> const&, QgsFeature*, QgsExpression*) (qgsexpression.cpp:634) ==26967== by 0x57E4D8D: QgsExpression::StaticFunction::func(QList<QVariant> const&, QgsFeature*, QgsExpression*) (qgsexpression.h:269) ==26967== by 0x57E07F5: QgsExpression::NodeFunction::eval(QgsExpression*, QgsFeature*) (qgsexpression.cpp:2210) ==26967== by 0x57D9D17: QgsExpression::evaluate(QgsFeature*) (qgsexpression.cpp:1298) ==26967== by 0x41411C: TestQgsExpression::evaluation() (testqgsexpression.cpp:329) ==26967== by 0x40CCCC: TestQgsExpression::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) (moc_testqgsexpression.cxx:88) ==26967== by 0x4FB4F00: QMetaMethod::invoke(QObject*, Qt::ConnectionType, QGenericReturnArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument) const (in /usr/lib/x86_64-linux-gnu/libQtCore.so.4.8.1) ==26967== by 0x4FB720F: QMetaObject::invokeMethod(QObject*, char const*, Qt::ConnectionType, QGenericReturnArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument) (in /usr/lib/x86_64-linux-gnu/libQtCore.so.4.8.1) ==26967== by 0x5310214: ??? (in /usr/lib/x86_64-linux-gnu/libQtTest.so.4.8.1) ==26967== by 0x531123C: QTest::qExec(QObject*, int, char**) (in /usr/lib/x86_64-linux-gnu/libQtTest.so.4.8.1) ==26967== by 0x40CBAC: main (testqgsexpression.cpp:745) ==26967== ==26967== Conditional jump or move depends on uninitialised value(s) ==26967== at 0x57D048D: fcnYear(QList<QVariant> const&, QgsFeature*, QgsExpression*) (qgsexpression.cpp:619) ==26967== by 0x57E4D8D: QgsExpression::StaticFunction::func(QList<QVariant> const&, QgsFeature*, QgsExpression*) (qgsexpression.h:269) ==26967== by 0x57E07F5: QgsExpression::NodeFunction::eval(QgsExpression*, QgsFeature*) (qgsexpression.cpp:2210) ==26967== by 0x57D9D17: QgsExpression::evaluate(QgsFeature*) (qgsexpression.cpp:1298) ==26967== by 0x41411C: TestQgsExpression::evaluation() (testqgsexpression.cpp:329) ==26967== by 0x40CCCC: TestQgsExpression::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) (moc_testqgsexpression.cxx:88) ==26967== by 0x4FB4F00: QMetaMethod::invoke(QObject*, Qt::ConnectionType, QGenericReturnArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument) const (in /usr/lib/x86_64-linux-gnu/libQtCore.so.4.8.1) ==26967== by 0x4FB720F: QMetaObject::invokeMethod(QObject*, char const*, Qt::ConnectionType, QGenericReturnArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument,</pre>		

QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument) (in /usr/lib/x86_64-linux-gnu/libQtCore.so.4.8.1)

Associated revisions

Revision bd00b0f3 - 2012-12-14 06:24 PM - Sandro Santilli

Initialize all members in Interval constructor.

Fixes memory conditional jumps depending on uninitialized values
and as a consequence the unstable results from qgis_expressiontest

Closes #6877

History

#1 - 2012-12-14 09:16 AM - Sandro Santilli

And this other:

```
==26967== Conditional jump or move depends on uninitialised value(s)
==26967== at 0x57CE377: getInterval(QVariant const&, QgsExpression*, bool) (qgsexpression.cpp:322)
==26967== by 0x57D01AD: fcnToInterval(QList<QVariant> const&, QgsFeature*, QgsExpression*) (qgsexpression.cpp:589)
==26967== by 0x57E4D8D: QgsExpression::StaticFunction::func(QList<QVariant> const&, QgsFeature*, QgsExpression*)
(qgsexpression.h:269)
==26967== by 0x57E07F5: QgsExpression::NodeFunction::eval(QgsExpression*, QgsFeature*) (qgsexpression.cpp:2210)
==26967== by 0x57D9D17: QgsExpression::evaluate(QgsFeature*) (qgsexpression.cpp:1298)
==26967== by 0x41411C: TestQgsExpression::evaluation() (testqgsexpression.cpp:329)
==26967== by 0x40CCCC: TestQgsExpression::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) (moc_testqgsexpression.cxx:88)
==26967== by 0x4FB4F00: QMetaMethod::invoke(QObject*, Qt::ConnectionType, QGenericReturnArgument, QGenericArgument,
QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument,
QGenericArgument, QGenericArgument) const (in /usr/lib/x86_64-linux-gnu/libQtCore.so.4.8.1)
==26967== by 0x4FB720F: QMetaObject::invokeMethod(QObject*, char const*, Qt::ConnectionType, QGenericReturnArgument,
QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument, QGenericArgument,
QGenericArgument, QGenericArgument, QGenericArgument) (in /usr/lib/x86_64-linux-gnu/libQtCore.so.4.8.1)
==26967== by 0x5310214: ??? (in /usr/lib/x86_64-linux-gnu/libQtTest.so.4.8.1)
==26967== by 0x531123C: QTest::qExec(QObject*, int, char**) (in /usr/lib/x86_64-linux-gnu/libQtTest.so.4.8.1)
==26967== by 0x40CBAC: main (testqgsexpression.cpp:745)
==26967==
```

#2 - 2012-12-14 09:19 AM - Sandro Santilli

Indeed the Interval::mValid is not initialized in the constructor

#3 - 2012-12-14 09:26 AM - Sandro Santilli

- Status changed from Open to Closed

Fixed in changeset commit:"bd00b0f3f61849bc9dbf8771a32c4c360c95a644".