QGIS Application - Bug report #14188
QGIS crashes when removing vertex of a multipart geometry
2016-01-28 10:41 AM - Salvatore Larosa

Status: Closed
Priority: Severe/Regression
Assignee: Sandro Santilli
Category: Digitising
Affected QGIS version: master
Operating System: El Capitan OSX, Debian, Ubuntu 64bit
Pull Request or Patch supplied: No
Crashes QGIS or corrupts data: Yes

Description
The crash occurs when removing vertices of a multipart geometry.
The multipart geometry was created with the Merge selected features tool.

Stacktrace:

Program received signal SIGSEGV, Segmentation fault.
QgsGeometry::QgsGeometry (this=0x14126e250, other=...) at /Users/larosa/dev/QGIS/src/core/geometry/qgsgeometry.cpp:82
82    {
(gdb) bt
#0  QgsGeometry::QgsGeometry (this=0x14126e250, other=...) at /Users/larosa/dev/QGIS/src/core/geometry/qgsgeometry.cpp:82
#1  0x000000010041ddac in QgsSelectedFeature::updateGeometry (this=0x11853dfd0, geom=<optimized out>) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsselectedfeature.cpp:81
#2  0x000000010041f6f6 in QgsSelectedFeature::createVertexMap (this=0x14126e250) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsselectedfeature.cpp:416
#3  0x000000010041d866 in QgsSelectedFeature::replaceVertexMap (this=0x14126e250) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsselectedfeature.cpp:381
#4  QgsSelectedFeature::setSelectedFeature (this=0x14126e250, featureId=3013, vlayer=0x0, canvas=0x11853dfd0)
    at /Users/larosa/dev/QGIS/src/app/nodetool/qgsselectedfeature.cpp:114
#5  0x00000001004199b4 in QgsMapToolNodeTool::canvasPressEvent (this=0x0, e=<optimized out>) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsmaptoolnodetool.cpp:238
#6  0x0000000100e09c81 in QgsMapCanvas::mousePressEvent (this=0x14126e250, e=0x11853dfd0) at /Users/larosa/dev/QGIS/src/gui/qgsmapcanvas.cpp:1307
#7  0x00000001002a99b4 in QgMapToolNodeTool::canvasPressEvent (this=0x0, e=<optimized out>) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsmaptoolnodetool.cpp:238
#8  0x00000001002a9c94 in QWidget::event(QEvent*) () from /usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore
#9  0x000000010041b975 in QFrame::event(QEvent*) () from /usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore
#10 0x000000010041c5b9 in QAbstractScrollArea::viewportEvent(QEvent*) () from /usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore
#11 0x00000001002a80b6 in QGraphicsView::viewportEvent(QEvent*) () from /usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore
#12 0x00000001002a8273 in QAbstractScrollAreaFilter::eventFilter(QObject*, QEvent*) () from /usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore
#13 0x00000001002a02b6 in QCoreApplicationPrivate::sendThroughObjectEventFilters(QObject*, QEvent*) () from /usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore
#14 0x0000000100276754 in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore

Do not dereference null pointer on QgsSelectedFeature::updateGeometry

Fixes #14188

History

#1 - 2016-01-29 04:52 AM - Martin Dobias

Tried with multipolygon, multilinestring and multipoint - deleting vertices one by one until the geometries are completely gone - but I am unable to replicate the problem. Would you mind sharing the data where you get the crash?

#2 - 2016-01-29 04:52 AM - Martin Dobias

- Status changed from Open to Feedback

#3 - 2016-01-29 05:27 AM - Salvatore Larosa

- File test_crash.tar.gz added

I attached a small part of my shapefile. Anyway, you should before using the merge selected features tool on the shapefile and merging to the big polygon then you use the node tool (while the geometry is selected) to remove the vertices.

Sometime it crashes just if I remove a couple of vertices and sometimes I have to remove a lot of vertices before crashing.

#4 - 2016-01-31 03:50 AM - Salvatore Larosa
Step to reproduce with the attached dataset:

- load the shapefile and start editing
- select features 10102 and 3009 (gid)
- use merge selected features tool
- select node tool and click over the feature merged (might crash here)
- click again over the feature (not over the nodes)
- QGIS crashes

#5 - 2016-01-31 09:59 AM - Giovanni Manghi
- Status changed from Feedback to Open

certified here on Ubuntu 14.04.

#6 - 2016-02-01 07:38 AM - Sandro Santilli
- Assignee set to Sandro Santilli

I'm taking this, please let me know if anyone else is already working on a fix (assign to yourself if so, thanks)

#7 - 2016-02-01 07:44 AM - Sandro Santilli
- Operating System changed from El Capitan OSX, Debian to El Capitan OSX, Debian, Ubuntu 64bit

I could reproduce here

#8 - 2016-02-01 07:52 AM - Sandro Santilli

Valgrind detects a first memory error during merge:

src/core/qgsmaprendererparalleljob.cpp: 211: (renderingFinished) [51ms] PARALLEL finished
src/gui/qgsmapcanvas.cpp: 708: (renderJobFinished) [0ms] CANVAS finish! 1
src/gui/qgsmapcanvas.cpp: 1251: (keyReleaseEvent) [542ms] keyRelease event
src/gui/qgsmapcanvas.cpp: 1273: (keyReleaseEvent) [0ms] Ignoring key release: 16777249
==14453== Conditional jump or move depends on uninitialised value(s)
==14453== at 0x7838D15: QProgressDialog::setValue(int) (in /usr/lib/x86_64-linux-gnu/libQtGui.so.4.8.6)
==14453== by 0x4F9263D: QgisApp::unionGeometries(QgsVectorLayer const*, QList<QgsFeature>&, bool&) (qgisapp.cpp:5947)
==14453== by 0x4F9577C: QgisApp::mergeSelectedFeatures() (qgisapp.cpp:6492)
==14453== by 0x53930AD: QgisApp::qt_static_metacall(QObject*, QMetaObject const*, int, void**) (moc_qgisapp.cxx:887)
==14453== by 0x6E52879: QMetaObject::activate(QObject*, QMetaObject const*, int, void**) (in /usr/lib/x86_64-linux-gnu/libQtCore.so.4.8.6)
==14453== by 0x7369A61: QAction::triggered(bool) (in /usr/lib/x86_64-linux-gnu/libQtGui.so.4.8.6)
==14453== by 0x736B432: QAction::activate(QAction::ActionEvent) (in /usr/lib/x86_64-linux-gnu/libQtGui.so.4.8.6)
==14453== by 0x7372B91: ??? (in /usr/lib/x86_64-linux-gnu/libQtGui.so.4.8.6)
==14453== by 0x7722CBB: QAbstractButton::mouseReleaseEvent(QMouseEvent*) (in /usr/lib/x86_64-libQtGui.so.4.8.6)
==14453== by 0x7F9A9C9: QToolButton::mouseReleaseEvent(QMouseEvent*) (in /usr/lib/x86_64-libQtGui.so.4.8.6)
==14453== by 0x736F519: QWidget::event(QEvent*) (in /usr/lib/x86_64-libQtGui.so.4.8.6)
==14453== by 0x736FE2B: QApplicationPrivate::notify_helper(QObject*, QEvent*) (in /usr/lib/x86_64-linux-gnu/libQtGui.so.4.8.6)
And then the attempt to dereference NULL pointer in "updateGeometry":

src/app/nodetool/qgsselectedfeature.cpp: 73: (updateGeometry) [1ms] Entering.
src/app/nodetool/qgsselectedfeature.cpp: 81: (updateGeometry) [0x000000010041aa60] in QgsMapToolNodeTool::updateSelectFeature(QgsMapMouseEvent*) (qgsmaptoolnodetool.cpp:469)
src/app/nodetool/qgsmapcanvas.cpp: 1354: (updateGeometry) [0x000000010041b236] in QgsMapCanvas::mousePressEvent(QMouseEvent*) (qgsmapcanvas.cpp:1354)
src/app/nodetool/qgsmapcanvas.cpp: 1386: (updateGeometry) [0x000000010041b858] in QFrame::event(QEvent*) (in /usr/lib64-linux-gnu/libQtGui.so.4.8.6)
src/app/qgsidentifyresultsdialog.cpp: 1436: (featureDeleted) [11915ms] item 10 / 11
src/app/qgsidentifyresultsdialog.cpp: 14453: Invalid read of size 8
src/app/qgsidentifyresultsdialog.cpp: 14453: at 0x683CD26: QgsGeometry::QgsGeometry(QgsGeometry const&) (qgsgeometry.cpp:83)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x5157EC6: QgsSelectedFeature::updateGeometry(QgsGeometry*) (qgsselectedfeature.cpp:81)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x5159954: QgsSelectedFeature::createVertexMap() (qgsselectedfeature.cpp:416)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x515973F: QgsSelectedFeature::replaceVertexMap() (qgsselectedfeature.cpp:381)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x515818D: QgsSelectedFeature::setSelectedFeature(long long, QgsVectorLayer*, QgsMapCanvas*) (qgsselectedfeature.cpp:114)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x515255F: QgsMapToolNodeTool::canvasReleaseEvent(QgsMapMouseEvent*) (qgsmaptoolnodetool.cpp:469)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x5C329EB: QgsMapCanvas::mouseReleaseEvent(QMouseEvent*) (qgsmapcanvas.cpp:1354)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x73BF519: QWidget::event(QEvent*) (in /usr/lib64-linux-gnu/libQtGui.so.4.8.6)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x776104D: QFrame::event(QEvent*) (in /usr/lib64-linux-gnu/libQtGui.so.4.8.6)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x796C858: QGraphicsView::viewportEvent(QEvent*) (in /usr/lib64-linux-gnu/libQtGui.so.4.8.6)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x6E3E645: QCoreApplicationPrivate::sendThroughObjectEventFilters(QObject*, QEvent*) (in /usr/lib64-linux-gnu/libQtCore.so.4.8.6)
src/app/qgsidentifyresultsdialog.cpp: 14453: by 0x736F6DE: QApplicationPrivate::notify_helper(QObject*, QEvent*) (in /usr/lib64-linux-gnu/libQtGui.so.4.8.6)
src/app/qgsidentifyresultsdialog.cpp: 14453: Address 0x0 is not stack'd, malloc'd or (recently) free'd

#9 - 2016-02-01 08:28 AM - Sandro Santilli
- Status changed from Open to In Progress
- % Done changed from 0 to 40

#10 - 2016-02-01 08:31 AM - Sandro Santilli
- Status changed from In Progress to Closed

Fixed in changeset commit:"781c9d7fc2c144b94be16c23522da8ae1ce0e63d".

#11 - 2016-02-01 08:48 AM - Salvatore Larosa
- Status changed from Closed to Reopened

Sandro thanks to take care of this, unfortunately it still crashes for me, with different stacktrace, but it crashes:

Program received signal SIGSEGV, Segmentation fault.
QgsGeometry::geometry (this=0x0) at /Users/larosa/dev/QGIS/src/core/geometry/qgsgeometry.cpp:130
130 return d->geometry;
(gdb) bt
#0 QgsGeometry::geometry (this=0x0) at /Users/larosa/dev/QGIS/src/core/geometry/qgsgeometry.cpp:130
#1 0x0000000010041aa60 in QgsMapToolNodeTool::updateSelectFeature (this=0x107e35c40, geom=...) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsmaptoolnodetool.cpp:388
#2 0x0000000010041b236 in QgsMapToolNodeTool::updateSelectFeature (this=0x107e35c40) at
Salvatore could you please try commit:24a9f491812a3a044c28a4406a24764504d792db?

Yes, I am building.....

- Status changed from Reopened to Closed

works for me, thanks

Files

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>test_crash.tar.gz</td>
<td>10.3 KB</td>
<td>2016-01-29</td>
<td>Salvatore Larosa</td>
</tr>
</tbody>
</table>