### QGIS Application - Bug report #14188
### QGIS crashes when removing vertex of a multipart geometry

2016-01-28 10:41 AM - Salvatore Larosa

<table>
<thead>
<tr>
<th>Status</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Severe/Regression</td>
</tr>
<tr>
<td>Assignee</td>
<td>Sandro Santilli</td>
</tr>
<tr>
<td>Category</td>
<td>Digitising</td>
</tr>
<tr>
<td>Affected QGIS version</td>
<td>master</td>
</tr>
<tr>
<td>Operating System</td>
<td>El Capitan OSX, Debian, Ubuntu 64bit</td>
</tr>
<tr>
<td>Pull Request or Patch supplied</td>
<td>No</td>
</tr>
<tr>
<td>Crashes QGIS or corrupts data</td>
<td>Yes</td>
</tr>
<tr>
<td>Regression?</td>
<td>No</td>
</tr>
<tr>
<td>Easy fix?</td>
<td>No</td>
</tr>
<tr>
<td>Resolution</td>
<td></td>
</tr>
<tr>
<td>Copied to github as #</td>
<td>22190</td>
</tr>
</tbody>
</table>

### 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  0x0000000010041d4ac in QgsSelectedFeature::updateGeometry (this=0x11853dfd0, geom=<optimized out>) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsselectedfeature.cpp:81
#2  0x0000000010041f666 in QgsSelectedFeature::createVertexMap (this=0x14126e250) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsselectedfeature.cpp:416
#3  0x0000000010041d666 in QgsSelectedFeature::replaceVertexMap (this=0x14126e250) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsselectedfeature.cpp:381
#4  QgsSelectedFeature::setSelectedFeature (this=0x14126e250, featureId=<optimized out>, vlayer=<optimized out>, canvas=0x11853df0) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsselectedfeature.cpp:114
#5  0x0000000010041d699 in QgsMapToolNodeTool::canvasPressEvent (this=0x0, e=<optimized out>) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsmaptoolnodetool.cpp:238
#6  0x0000000010041b9b4 in QgsMapToolNodeTool::canvasPressEvent (this=0x0, e=0x11853dfd0) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsmaptoolnodetool.cpp:238
#7  0x00000000100419c81 in QgsMapCanvas::mousePressEvent (this=0x14126e250, e=0x11853df0) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsmapcanvas.cpp:1307
#8  0x0000000010279949 in QWidget::event(QEvent*) () from /usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#9  0x00000000102ab37875 in QFrame::event(QEvent*) () from /usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#10 0x000000001025b9d9 in QAbsAbstractScrollArea::viewportEvent(QEvent*) () from /usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#11 0x00000000102c89f6 in QGraphicsView::viewportEvent(QEvent*) () from /usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#12 0x00000000102b26273 in QAbsAbstractScrollAreaFilter::eventFilter(QObject*, QEvent*) () from /usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#13 0x000000001024d6c66 in QCoreApplicationPrivate::sendThroughObjectEventFilters(QObject*, QEvent*) () from /usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore
#14 0x000000001027754e in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
```

2022-03-04
# Associated revisions

**Revision 781c9d7f - 2016-02-01 05:30 PM - Sandro Santilli**

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

confirmed 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::Call, 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 0x73BF519: QWidget::event(QEvent*) (in /usr/lib/x86_64-linux-gnu/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)
2022-03-04 3/6
```
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: (qgsselectedfeature.cpp:114)
```

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  0x0000000100014a60 in QgsMapToolNodeTool::updateSelectFeature (this=0x107e35c40, geom=...) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsmaptoolnodetool.cpp:388
#2  0x00000001004b236 in QgsMapToolNodeTool::updateSelectFeature (this=0x107e35c40) at

#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  0x0000000100014a60 in QgsMapToolNodeTool::updateSelectFeature (this=0x107e35c40, geom=...) at /Users/larosa/dev/QGIS/src/app/nodetool/qgsmaptoolnodetool.cpp:388
#2  0x00000001004b236 in QgsMapToolNodeTool::updateSelectFeature (this=0x107e35c40) at
Salvatore: same steps, to reproduce?

Oops, I can still reproduce too, maybe I reverted the actual fix before pushing ??

---

2022-03-04

#12 - 2016-02-01 08:51 AM - Sandro Santilli
Salvatore: same steps, to reproduce?

#13 - 2016-02-01 08:53 AM - Sandro Santilli
Oops, I can still reproduce too, maybe I reverted the actual fix before pushing ??
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>