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=<optimized out>, vlayer=<optimized out>,
canvas=0x11853df0)
at /Users/larosa/dev/QGIS/src/app/nodetool/qgsselectedfeature.cpp:114
#5 0x000000010041d69f in QgsMapToolNodeTool::canvasPressEvent (this=0x0, e=<optimized out>)
at /Users/larosa/dev/QGIS/src/app/nodetool/qgsmaptoolnodetool.cpp:238
#6 0x00000001004199b4 in QgsMapCanvas::mousePressEvent (this=0x14126e250, e=0x11853dfd0) at
/Users/larosa/dev/QGIS/src/app/nodetool/qgsmapcanvas.cpp:238
#7 0x0000000100e09c81 in QgsMapCanvas::mousePressEvent (this=0x14126e250, e=0x11853dfd0) at
/Users/larosa/dev/QGIS/src/gui/qgsmapcanvas.cpp:238
#8 0x00000001027a9c94 in QWidget::event(QEvent*) () from /usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#9 0x0000000102b26273 in QAbstractScrollAreaFilter::eventFilter(QObject*, QEvent*) () from
/usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#10 0x0000000102c80fb6 in QGraphicsView::viewportEvent(QEvent*) () from
/usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#11 0x0000000102c80fb6 in QGraphicsView::viewportEvent(QEvent*) () from
/usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#12 0x0000000102b26273 in QAbstractScrollAreaFilter::eventFilter(QObject*, QEvent*) () from
/usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#13 0x0000000102d4d26eb in QCoreApplicationPrivate::sendThroughObjectEventFilters(QObject*, QEvent*) () from
/usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore
#14 0x000000010276754e in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from
/usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore
#15 0x00000000102768ed4 in QApplication::notify(QObject*, QEvent*) () from
/usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#16 0x0000000010193f590 in QgsApplication::notify (this=0x7fff5fbff430, receiver=0x1448a9c20, event=0x7fff5fbfe628)
at/Users/larosa/dev/QGIS/src/core/qgsapplication.cpp:281
#17 0x000000001024d246 in QCoreApplication::notifyInternal(QObject*, QEvent*) () from
/usr/local/opt/qt/lib/QtCore.framework/Versions/4/QtCore
#18 0x00000000102767e0b in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget*, QWidget**, QPointer<QWidget>&, bool) ()
from/usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#19 0x00000000102720143 in qt_mac_handleMouseEvent(NSEvent*, QEvent::Type, Qt::MouseButton, QWidget*, bool) ()
from/usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#20 0x00007fff96348d1d in -[NSWindow _handleMouseDownEvent:isDelayedEvent:] () from
/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit
#21 0x00007fff96349fad in -[NSWindow _reallySendEvent:isDelayedEvent:] () from
/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit
#22 0x00007fff95ca2735 in -[NSApplication sendEvent:] () from /System/Library/Frameworks/AppKit.framework/Versions/C/AppKit
#23 0x000000001027186c3 in -[QCocoaWindow sendEvent:] () from /usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#24 0x0000000010f59ec49 in -[NSApplication sendEvent:] () from
/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit
#25 0x0000000010271cb68 in -[QNSApplication sendEvent:] () from /usr/local/opt/qt/lib/QtGui.framework/Versions/4/QtGui
#26 0x0000000010f59bd203a in -[NSApplication run] () from /System/Library/Frameworks/AppKit.framework/Versions/C/AppKit

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 0x736B432: QAction::activate(QAction::ActionEvent) (in /usr/lib/x86_64-linux-gnu/libQtGui.so.4.8.6)
==14453== by 0x7722B91: ??? (in /usr/lib/x86_64-linux-gnu/libQtGui.so.4.8.6)
==14453== by 0x77722CBB: QAbstractButton::mouseReleaseEvent(QMouseEvent*) (in /usr/lib/x86_64-linux-gnu/libQtGui.so.4.8.6)
==14453== by 0x77D9A9C: QToolBar::mouseReleaseEvent(QMouseEvent*) (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)
```

2021-08-01 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: (updateGeometry) [1ms] Entering.
```

```
src/app/nodetool/qgsselectedfeature.cpp: 114: (updateGeometry) [1ms] Entering.
```

```
`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  0x0000000010041ae60 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
```

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  0x000000001004a1aae0 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
```

2021-08-01
Salvatore: same steps, to reproduce?

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>