QGIS Application - Bug report #13958
Overflow on primary key with negative values; crashes QGIS when editing

2015-12-07 09:04 PM - Mike Taves

Status:	Closed		
Priority:	Severe/Regression		
Assignee:	Sandro Santilli		
Category:	Data Provider		
Affected QGIS version:	master	**Regression?:**	No
Operating System:	Windows 7, Ubuntu 14.04 64bit	**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	fixed/implemented
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	21973

Description

This is a recent issue with QGIS 2.12.1-Lyon (commit:16760fd) on Windows 7 via OSGeo4W x64. I can reproduce the behaviour with any version of PostGIS, but have not tested other data providers.

Create a simple PostGIS table:

```
CREATE table my_lines(gid integer primary key, col integer);
SELECT AddGeometryColumn('my_lines', 'geom', 4326, 'MULTILINESTRING', 2);

INSERT INTO my_lines(gid, col, geom)
SELECT -1, 2, 'SRID=4326;MULTILINESTRING((0 0, 1 1))';
```

Note that the primary key has a negative value -1, which should be completely fine and previous versions of QGIS were OK with this.

This table can be added to QGIS, which shows the simple geometry on the main canvas normally, and the Layer properties correctly describes both gid and col fields as int4.

However, the attribute table shows the values of gid and col as ERROR, and clicking the feature with the Identify Features tool show gid of 4294967295, which is the overflow version of an unsigned integer value -1. Perhaps the primary key was internally cast in QGIS to unsigned long?

Editing the layer, e.g. with the Node tool, crashes QGIS when the geometry is clicked. A minidump is written the a temporary location, and is available on request.

Associated revisions

Revision 2bd7f446 - 2016-02-16 05:40 PM - Sandro Santilli

Fix signed 32bit integer overflow in PostgreSQL provider

Fixes #13958
Includes test for signed integer attributes

History

#1 - 2016-02-09 03:19 AM - Sandro Santilli

- Crashes QGIS or corrupts data changed from Yes to No

- Status changed from Open to In Progress

- Assignee set to Sandro Santilli

- Operating System changed from Windows 7 to Windows 7, Ubuntu 14.04 64bit

Confirmed with current master (2.14.0dev, 964ae1f) on Linux 64bit -- but it doesn't cause crash or corruption, right ?

#2 - 2016-02-09 03:21 AM - Sandro Santilli

- Affected QGIS version changed from 2.12.0 to master

- Target version changed from Future Release - High Priority to Version 2.14

#3 - 2016-02-09 03:46 AM - Sandro Santilli

Mike what's the latest version still working, to help bisect ?

#4 - 2016-02-09 04:03 AM - Sandro Santilli

final-2_12_0 is already bogus

#5 - 2016-02-09 06:11 AM - Sandro Santilli

final-2_10_1 is already broken

#6 - 2016-02-09 06:13 AM - Sandro Santilli

Actually, 2.8.4-Wien also has the same behavior.
What does it mean, Mike, that this is "a recent issue" ?

#7 - 2016-02-09 06:16 AM - Sandro Santilli

- Priority changed from High to Severe/Regression

- Crashes QGIS or corrupts data changed from No to Yes

Oops, sorry but I completely overlooked the crash part ! But confirm 2.8.4-Wien and final-2_10_1 are affected by it.
Will re-check with master and report back.

#8 - 2016-02-09 06:36 AM - Sandro Santilli

- Status changed from In Progress to Closed

- Resolution set to fixed/implemented

Ok, master (ded1ebb) does not crash for me, so this seems to be fixed (the crash).
Feel free to file another one for the ERROR/ERROR indication, which is also a bug but not blocker.

#9 - 2016-02-09 06:40 AM - Sandro Santilli

- Status changed from Closed to Reopened

Wait, reopening. It still crashes, only later (need to close to crash).

Before closing, this is logged:

> ERROR: 1 geometries not changed.
>
> Provider errors:
>
> PostGIS error while changing geometry values: ERROR: value "4294967295" is out of range for type integer

On closing, crash:

```
(gdb) bt
#0  0x00007f3f9ade4441 in QBrush::~QBrush() () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#1  0x00007f3f9bec4138 in QgsSimpleMarkerSymbolLayerV2::~QgsSimpleMarkerSymbolLayerV2 (this=0x2550460, __in_chrg=<optimized
out>)
    at /usr/src/qgis/qgis-master/src/core/symbology-ng/qgsmarkersymbollayerv2.h:34
#2  0x00007f3f9bec41f2 in QgsSimpleMarkerSymbolLayerV2::~QgsSimpleMarkerSymbolLayerV2 (this=0x2550460, __in_chrg=<optimized out>)
    at /usr/src/qgis/qgis-master/src/core/symbology-ng/qgsmarkersymbollayerv2.h:34
#3  0x00007f3f9bf2945b in qDeleteAll<QList<QgsSymbolLayerV2*>::const_iterator> (begin=..., end=...) at
/usr/include/qt4/QtCore/qalgorithms.h:322
#4  0x00007f3f9bf28ea1 in qDeleteAll<QList<QgsSymbolLayerV2*> > (c=...) at /usr/include/qt4/QtCore/qalgorithms.h:330
#5  0x00007f3f9bf1e09e in QgsSymbolV2::~QgsSymbolV2 (this=0x7f3f01def440 <QgsCategorizedSymbolRendererV2::sSkipRender>,
__in_chrg=<optimized out>)
    at /usr/src/qgis/qgis-master/src/core/symbology-ng/qgssymbolv2.cpp:241
#6  0x00007f3f9bf295c0 in QgsMarkerSymbolV2::~QgsMarkerSymbolV2 (this=0x7f3f01def440
<QgsCategorizedSymbolRendererV2::sSkipRender>,
    __in_chrg=<optimized out>) at /usr/src/qgis/qgis-master/src/core/symbology-ng/qgssymbolv2.h:415
#7  0x00007f3f9a267259 in __run_exit_handlers (status=0, listp=0x7f3f9a5e96c8 <__exit_funcs>, run_list_atexit=run_list_atexit@entry=true)
    at exit.c:82
#8  0x00007f3f9a2672a5 in __GI_exit (status=<optimized out>) at exit.c:104
#9  0x00007f3f9a24cecc in __libc_start_main (main=0x405aa7 <main(int, char**)>, argc=2, argv=0x7fff6d67c1c8, init=<optimized out>,
    fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fff6d67c1b8) at libc-start.c:321
#10 0x00000000004051a9 in _start ()
```

#10 - 2016-02-09 06:41 AM - Sandro Santilli

Uff, the crash is unrelated with this bug. I'm filing a new one.

#11 - 2016-02-09 06:44 AM - Sandro Santilli

So the crash was filed as #14260 -- Mike I'll leave to you confirming that master branch does not crash on edit, and filing the separate ticket about the ERROR/ERROR and impossibility to edit the layer, if you don't mind.

#12 - 2016-02-09 08:24 AM - Sandro Santilli

- Status changed from Reopened to Closed

I cannot reproduce the crash with a clean build against commit:b9726d7285733c27d42456c115e28d5a37f3e0be, so closing this for the crash part. The rest was filed as #14262

#13 - 2016-02-10 11:35 AM - Jürgen Fischer

Negative ids are used to identify new features (see FID_AS_NEW) - so negative ids might also cause other trouble, when adding, updating and deleting features.

#14 - 2016-02-12 02:13 AM - Sandro Santilli

Uhm, I wish new features could be identifier in some other way, but as long as this is how you tell them apart, there should be checks in the provider to refuse accepting negative integers as real feature identifiers. Aren't there cases in which a field is refused as an identifier ? Like where duplicates are found ? Another case should be presence of negative integers, until that FID_IS_NEW usage changes, or the PostgreSQL provider changes the way it generates identifiers by isolating the database identifier from the qgis feature identifier (which would also allow using multiple-column identifiers or string-based ones etc.).

#15 - 2016-02-12 02:15 AM - Sandro Santilli

The general case of overflow should be probably discussed in #14262 though...

#16 - 2016-02-16 06:46 AM - Sandro Santilli

- Status changed from Closed to Reopened

I just got a segfault again, as of commit:6365eb7ee6edcd66aaee11524aba25ce892f4152

Backtrace:

```
Core was generated by `output/bin/qgis'.
Program terminated with signal SIGSEGV, Segmentation fault.
#0  0x00007f2c05f1370f in QgsMapToolNodeTool::canvasMoveEvent (this=0x261e2c0, e=0x22be3e0)
    at /usr/src/qgis/qgis-master/src/app/nodetool/qgsmaptoolnodetool.cpp:142
142         QgsAbstractGeometryV2* rbGeom = mSelectedFeature->geometry()->geometry()->clone();
Traceback (most recent call last):
  File "/usr/share/gdb/auto-load/usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.19-gdb.py", line 63, in <module>
    from libstdcxx.v6.printers import register_libstdcxx_printers
ImportError: No module named 'libstdcxx'
(gdb)
(gdb) bt
#0  0x00007f2c05f1370f in QgsMapToolNodeTool::canvasMoveEvent (this=0x261e2c0, e=0x22be3e0)
    at /usr/src/qgis/qgis-master/src/app/nodetool/qgsmaptoolnodetool.cpp:142
#1  0x00007f2c04d70335 in QgsMapCanvas::mouseMoveEvent (this=0x222b910, e=0x7fffc7ae1150)
    at /usr/src/qgis/qgis-master/src/gui/qgsmapcanvas.cpp:1515
#2  0x00007f2c01692645 in QWidget::event(QEvent*) () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#3  0x00007f2c01a3404e in QFrame::event(QEvent*) () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#4  0x00007f2c01c3f859 in QGraphicsView::viewportEvent(QEvent*) () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#5  0x00007f2c022a9646 in QCoreApplicationPrivate::sendThroughObjectEventFilters(QObject*, QEvent*) ()
   from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
```

```
#6  0x00007f2c01642e0c in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#7  0x00007f2c016495dd in QApplication::notify(QObject*, QEvent*) () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
#8  0x00007f2c02e4f472 in QgsApplication::notify (this=0x7fffc7ae2110, receiver=0x2304400, event=0x7fffc7ae1150)
    at /usr/src/qgis/qgis-master/src/core/qgsapplication.cpp:281
#9  0x00007f2c022a94dd in QCoreApplication::notifyInternal(QObject*, QEvent*) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#10 0x00007f2c01648d93 in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget*, QWidget**,
QPointer<QWidget>&, bool) ()
   from /usr/lib/x86_64-linux-gnu/libQtGui.so.4
```

The behavior with https://github.com/qgis/QGIS/pull/2777 merged becomes more weird but doesn't crash (yet)

#17 - 2016-02-16 06:49 AM - Sandro Santilli

Why isn't the QgsFeatureId class used ?
https://github.com/qgis/QGIS/blob/master/src/core/qgsfeature.h#L33
It could be extended to signal if the feature is new or existing...

#18 - 2016-02-16 07:01 AM - Sandro Santilli

I verified that always using the primary key of type "map" fixes this issue.
See commit:2dbcfb5 which is now part of https://github.com/qgis/QGIS/pull/2777

#19 - 2016-02-16 08:41 AM - Sandro Santilli

- Status changed from Reopened to Closed

Fixed in changeset commit:"2bd7f446b4dd368968f23b990262c5e8a5a83f80".