

2019-02-20 01:31 PM - Martin Dobias

```
Description

Steps to reproduce:
1. make a layer editable
2. enable a digitizing tool (e.g. add polygon)
3. enable advanced digitizing
4. click on the map so that you get the click snapped to an existing feature
5. close QGIS window
6. crash

Stacktrace:

#0 0x00007f3b54d9a6c2 in __GI___waitpid (pid=32216, stat_loc=0x7ffd57b01d64, options=0) at
../sysdeps/unix/sysv/linux/waitpid.c:30
    resultvar = 18446744073709551104
    sc_cancel_oldtype = 0
#1 0x000055baf4388d10 in qgisCrash(int) (signal=11) at ../src/app/main.cpp:336
    status = 32765
    pidstr = "--pid=31571\000|\~u", '\000' <repeats 15 times>
    gdbpid = 32216
    exename = "/home/martin/qgis/git-master/build-debug/output/bin/qgis\000\035\260W\375\177\000\000
(\260W\375\177\000\000\250\004\t\000\273U\000\000\000\036\260W\375\177\000\000\000\200|x|\~uP+\260W\375\177\000\000\000
\000\004\000\000\000\000\000\000\000\240K\031\372\272U\000\000\340\260W\375\177\000\000\200\243CY;\177\000\000\001\000\0
00\000\000\000\000\000\000\000\227\351\371\272U\000\000x$\220U;\177\000\000\240\327\365\365\272U\000\000P\036\260W\37
W\375\177\000\000 (\260W\375\177\000\000\026\000\000\000\001\000\000\000\001j}\366\272U\000\000\000"...
    len = 56
#2 0x00007f3b54cf4f20 in <signal handler called> () at /lib/x86_64-linux-gnu/libc.so.6
#3 0x0000000000000000 in ()
#4 0x00007f3b59a57ff2 in std::default_delete<QgsVertexMarker>::operator()(QgsVertexMarker*) const (this=0x55baf6995b90,
__ptr=0x55bafa0f6b60) at /usr/include/c++/7/bits/unique_ptr.h:78
#5 0x00007f3b58d8c145 in std::unique_ptr<QgsVertexMarker, std::default_delete<QgsVertexMarker> >::~unique_ptr()
(this=0x55baf6995b90, __in_chrg=<optimized out>) at /usr/include/c++/7/bits/unique_ptr.h:268
    __ptr = @0x55baf6995b90: 0x55bafa0f6b60
#6 0x00007f3b58d8b840 in QgsSnapIndicator::~QgsSnapIndicator() (this=0x55baf6995b30, __in_chrg=<optimized out>) at
../src/gui/qgssnapindicator.h:32
#7 0x00007f3b59a41d78 in std::default_delete<QgsSnapIndicator>::operator()(QgsSnapIndicator*) const
(this=0x55baf6983460, __ptr=0x55baf6995b30) at /usr/include/c++/7/bits/unique_ptr.h:78
#8 0x00007f3b58aeb169 in std::unique_ptr<QgsSnapIndicator, std::default_delete<QgsSnapIndicator> >::~unique_ptr()
(this=0x55baf6983460, __in_chrg=<optimized out>) at /usr/include/c++/7/bits/unique_ptr.h:268
    __ptr = @0x55baf6983460: 0x55baf6995b30
#9 0x00007f3b58aeb6c4 in QgsAdvancedDigitizingCanvasItem::~QgsAdvancedDigitizingCanvasItem() (this=0x55baf69833e0,
```

```
__in_chrg=<optimized out>) at ../src/gui/qgsadvanceddigitizingcanvasitem.h:31
#10 0x00007f3b58aeb74c in QgsAdvancedDigitizingCanvasItem::~QgsAdvancedDigitizingCanvasItem() (this=0x55baf69833e0,
__in_chrg=<optimized out>) at ../src/gui/qgsadvanceddigitizingcanvasitem.h:31
#11 0x00007f3b58c4e973 in QgsMapCanvas::~QgsMapCanvas() (this=0x55baf6054420, __in_chrg=<optimized out>) at
../src/gui/qgsmapcanvas.cpp:251
[...]
```

My suspicion is that this is caused by <https://github.com/qgis/QGIS/commit/f002a9c43d3c8a999fbff995cc41fdc06dcb8d91> because it added holding of QgsSnapIndicator in QgsAdvancedDigitizingCanvasItem. Snap indicator object in turn holds QgsVertexMarker ... but that one can be already deleted by map canvas destructor when the adv.digitizing canvas item is deleted.

History

#1 - 2019-02-21 11:37 AM - Giovanni Manghi

possibly related to #21307

#2 - 2019-02-21 11:50 AM - Martin Dobias

These are two different issues. The crash here is triggered when closing QGIS (and it has very different backtrace)

#3 - 2019-02-21 11:54 AM - Loïc BARTOLETTI

Hmmm... you reopen a bug founded when I write the bugfix <https://github.com/qgis/QGIS/pull/8307#issue-225422152>

I haven't be able to reproduce this issue, but I thought she hadn't miraculously disappeared.

Can denis reproduce it?