QGIS Application - Bug report #17365
regression: QGIS crash while handling geometry in provided dataset

2017-10-31 06:31 AM - Mathieu Pellerin - nIRV

Status:	Closed		
Priority:	High		
Assignee:	Nyall Dawson		
Category:	Geometry		
Affected QGIS version:	master	**Regression?:**	Yes
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	25262

Description

QGIS simply dies when trying to open the attached geojson dataset.

Steps to reproduce

1. Create a new project, and add the "counties" layer from the attached us.json dataset
2. **boom** QGIS dies

GDB where output

```
0x00007ffff66e5c92 in QgsCurve::asQPolygonF (this=0x0) at
/home/webmaster/dev/cpp/QGIS/src/core/geometry/qgscurve.cpp:181
181     const int nb = numPoints();
(gdb) where
#0  0x00007ffff66e5c92 in QgsCurve::asQPolygonF() const (this=0x0) at
/home/webmaster/dev/cpp/QGIS/src/core/geometry/qgscurve.cpp:181
#1  0x00007ffff5f89c2e in QgsSymbol::_getPolygonRing(QgsRenderContext&, QgsCurve const&, bool) (context=..., curve=...,
clipToExtent=true)
    at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgssymbol.cpp:148
#2  0x00007ffff5f89e8f in QgsSymbol::_getPolygon(QPolygonF&, QList<QPolygonF>&, QgsRenderContext&, QgsPolygon
const&, bool) (pts=..., holes=..., context=...,
    polygon=..., clipToExtent=true) at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgssymbol.cpp:179
#3  0x00007ffff5f8eeac in QgsSymbol::renderFeature(QgsFeature const&, QgsRenderContext&, int, bool, bool, int, int)
(this=0x555559831470,
    feature=..., context=..., layer=-1, selected=false, drawVertexMarker=false, currentVertexMarkerType=1,
currentVertexMarkerSize=3)
    at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgssymbol.cpp:917
#4  0x00007ffff5f21ea4 in QgsFeatureRenderer::renderFeatureWithSymbol(QgsFeature&, QgsSymbol*, QgsRenderContext&,
int, bool, bool) (this=0x5555589e02c0, feature=..., symbol=0x555559831470, context=..., layer=-1, selected=false,
drawVertexMarker=false) at /home/webmaster/dev/cpp/QGIS/src/core/symbology/qgsrenderer.cpp:109
#5  0x00007ffff5f21e3a in QgsFeatureRenderer::renderFeature(QgsFeature&, QgsRenderContext&, int, bool, bool)
(this=0x5555589e02c0, feature=..., context=..., layer=-1, selected=false, drawVertexMarker=false) at
/home/webmaster/dev/cpp/QGIS/src/core/symbology/qgsrenderer.cpp:103
#6  0x00007ffff64c1b66 in QgsVectorLayerRenderer::drawRenderer(QgsFeatureIterator&) (this=0x55555b6b7800, fit=...)
    at /home/webmaster/dev/cpp/QGIS/src/core/qgsvectorlayerrenderer.cpp:283
#7  0x00007ffff64c1478 in QgsVectorLayerRenderer::render() (this=0x55555b6b7800) at
/home/webmaster/dev/cpp/QGIS/src/core/qgsvectorlayerrenderer.cpp:247
#8  0x00007ffff62c2af1 in QgsMapRendererParallelJob::renderLayerStatic(LayerRenderJob&) (job=...)
    at /home/webmaster/dev/cpp/QGIS/src/core/qgsmaprendererparalleljob.cpp:256
#9  0x00007ffff62c426c in QtConcurrent::FunctionWrapper1<void, LayerRenderJob&>::operator()(LayerRenderJob&)
(this=0x55555b21fe88, u=...)
    at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentfunctionwrappers.h:83
```

```
#10 0x00007ffff62c3fa5 in QtConcurrent::MapKernel<QList<LayerRenderJob>::iterator, QtConcurrent::FunctionWrapper1<void, LayerRenderJob&> >::runIteration(QList<LayerRenderJob>::iterator, int, void*) (this=0x55555b21fe50, it=...) at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentmapkernel.h:69
#11 0x00007ffff62c4044 in QtConcurrent::MapKernel<QList<LayerRenderJob>::iterator, QtConcurrent::FunctionWrapper1<void, LayerRenderJob&> >::runIterations(QList<LayerRenderJob>::iterator, int, int, void*) (this=0x55555b21fe50, sequenceBeginIterator=..., beginIndex=0, endIndex=1)
    at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentmapkernel.h:78
#12 0x00007ffff62c4514 in QtConcurrent::IterateKernel<QList<LayerRenderJob>::iterator, void>::forThreadFunction() (this=0x55555b21fe50)
    at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentiteratekernel.h:256
#13 0x00007ffff62c41d6 in QtConcurrent::IterateKernel<QList<LayerRenderJob>::iterator, void>::threadFunction() (this=0x55555b21fe50)
    at /usr/include/x86_64-linux-gnu/qt5/QtConcurrent/qtconcurrentiteratekernel.h:218
#14 0x00007fffebd31bfd in QtConcurrent::ThreadEngineBase::run() () at /usr/lib/x86_64-linux-gnu/libQt5Concurrent.so.5
#15 0x00007ffff44c0581 in  () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#16 0x00007ffff44c429d in  () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#17 0x00007fffeac8c7fc in start_thread (arg=0x7fff3164f700) at pthread_create.c:465
```

Associated revisions

Revision eea155d6 - 2017-11-01 11:48 AM - Nyall Dawson

Fix crash when attempting to render multipolygon with missing exterior ring

This commit fixes a possible crash when the vector layer renderer
attempts to render a multipolygon containing a polygon without
an exterior ring.

The underlying cause of the creation of this invalid geometry is deeper,
but this commit hardens the renderer and makes it more robust for
handling bad geometries.

Fixes #17365

Revision f4d3152e - 2017-11-01 11:48 AM - Nyall Dawson

[ogr] Also discard features with empty geometries
when feature request specifies a filter rect

OGR sometimes returns a feature with empty geometry (e.g.
a multipolygon with a polygon child with no rings) even when
OGR_L_SetSpatialFilterRect has been set for the layer.

Refs #17365

History

#1 - 2017-10-31 06:45 AM - Mathieu Pellerin - nIRV

This patch fixes the crasher, however I do not know if it's the right way to handle this:

https://github.com/nirvn/QGIS/commit/97a58ba2594fdb1f32fe5aef16eec458d0fbdf6c

#2 - 2017-10-31 07:38 AM - Mathieu Pellerin - nIRV

I get a crash under linux (ubuntu 17.10) running gdal 2.2.1, as well as under windows (osgeo4w QGIS dev) running gdal 2.2.2.

#3 - 2017-10-31 11:48 PM - Nyall Dawson

- Assignee set to Nyall Dawson

#4 - 2017-10-31 11:48 PM - Nyall Dawson

PR at https://github.com/qgis/QGIS/pull/5501

#5 - 2017-11-01 11:48 AM - Nyall Dawson

- % Done changed from 0 to 100

- Status changed from Open to Closed

Applied in changeset commit:qgis|eea155d6e28bbe3d66dd32e972d7c0472bbf3af4.

Files

us.json	641 KB	2017-10-31	Mathieu Pellerin - nIRV