QGIS Application - Bug report #12416
QGIS 2.8.1 crash opening FileGDB (openGDB-Driver)

2015-03-20 02:00 AM - Flo Ju

Status:	Closed		
Priority:	High		
Assignee:	Sandro Santilli		
Category:	Data Provider/OGR		
Affected QGIS version:	master	**Regression?:**	No
Operating System:	Windows , Linux	**Easy fix?:**	No
Pull Request or Patch supplied:	Yes	**Resolution:**	fixed/implemented
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	20588

Description

Opening a FileGDB in QGIS 2.8.1. (Win 7 x64) causes a crash of the application. With QGIS 2.4. no problems.
Crash-Dump attached.

Associated revisions

Revision bc4d16e8 - 2016-01-27 04:28 PM - Sandro Santilli

Check WKB boundaries while simplifying for rendering

Fixes crash on simplifying mixed-dimension collections.
Closes #12416

Revision 87887e43 - 2016-02-01 01:22 PM - Sandro Santilli

Add test for unexpected WKB input in simplification

Closes #12416

History

#1 - 2015-03-22 03:08 AM - Giovanni Manghi

- Crashes QGIS or corrupts data changed from No to Yes

- Status changed from Open to Feedback

I cannot confirm (qgis 2.8.1 on Win 7 64bit). I tested using the file geodatabases downloaded from here.

http://gapanalysis.usgs.gov/padus/data/download/

Please attach a sample of the data that causes the crash.

#2 - 2015-03-22 11:30 PM - Flo Ju

- File Trecks.gdb.zip added

As an attachement the GDB-File (zipped) - QGIS 2.8.1 crashes on Win-Server VM and Win7 64Bit when opening the layer Trecks_3D

#3 - 2015-03-23 01:07 AM - Giovanni Manghi

Flo Ju wrote:

> *As an attachement the GDB-File (zipped) - QGIS 2.8.1 crashes on Win-Server VM and Win7 64Bit when opening the layer Trecks_3D*

it opens just fine here.

#4 - 2015-03-23 11:32 PM - Flo Ju

We tried it on different systems: Win7 64Bit SP1 (3 different systems) and Win 2008 Server VM --> always the same crash. If I open the same GDB in QGIS 2.8.1. (with openGDB-Driver) on a Linux-system it works fine.

#5 - 2015-03-24 02:06 AM - Giovanni Manghi

Flo Ju wrote:

> *We tried it on different systems: Win7 64Bit SP1 (3 different systems) and Win 2008 Server VM --> always the same crash. If I open the same GDB in QGIS 2.8.1. (with openGDB-Driver) on a Linux-system it works fine.*

could you try see if ogrinfo works against this problematic layer? use the osgeo4w shell, to be sure you are using the same gdal/ogr installation qgis uses. Thanks.

#6 - 2015-03-24 03:24 AM - Flo Ju

Hi! OGR on command-line is 11.1.2 - the version used in QGIS 2.8.1 is the same (QGIS-Info). Tried to convert a Feature Layer from the GDB with ogr2ogr to a SHP and it worked fine.

#7 - 2015-03-25 12:36 AM - Giovanni Manghi

Flo Ju wrote:

> *Hi! OGR on command-line is 11.1.2 - the version used in QGIS 2.8.1 is the same (QGIS-Info). Tried to convert a Feature Layer from the GDB with ogr2ogr to a SHP and it worked fine.*

I'm out of ideas. The system you tested do share something that can differ from a "common" installation? cheers.

#8 - 2015-10-18 04:31 AM - Jürgen Fischer

- Category changed from Vectors to Data Provider/OGR

#9 - 2015-12-20 03:16 AM - Giovanni Manghi

I have also tested some very large filegdb dataset linked here #11746-6 with no issues whatsoever.

I suggest to close this ticket as probable local issue.

#10 - 2015-12-20 05:11 PM - clifford snow

Giovanni Manghi wrote:

> *I have also tested some very large filegdb dataset linked here*
>
> *#11746-6*
>
> *with no issues whatsoever.*
>
> *I suggest to close this ticket as probable local issue.*

I was just looking for an open ticket on this subject. QGIS closes unexpectedly when attempting to open a 124Mb Filegdb file [1]. QGIS seems to finish rendering the ways just before crashing. I'm running 1.12-1 lyon on a macbook pro with 16gb of memory.

org2ogr is able to convert to a shapefile which QGIS loads successfully.

[1] https://fortress.wa.gov/dnr/adminsa/gisdata/datadownload/state_roads.zip

#11 - 2015-12-21 01:30 AM - Giovanni Manghi

> *I was just looking for an open ticket on this subject. QGIS closes unexpectedly when attempting to open a 124Mb Filegdb file [1]. QGIS seems to finish rendering the ways just before crashing. I'm running 1.12-1 lyon on a macbook pro with 16gb of memory.*
>
> *org2ogr is able to convert to a shapefile which QGIS loads successfully.*
>
> *[1] https://fortress.wa.gov/dnr/adminsa/gisdata/datadownload/state_roads.zip*

and again no problems whatsoever in my Windows 7 testing machine with QGIS master, ltr and 2.12...

Can you please guys try a fresh installation? uninstall, remove .qgis, clean config, re-install.

#12 - 2015-12-28 03:06 AM - Giovanni Manghi

- Status changed from Feedback to Open

Flo Ju wrote:

> *As an attachement the GDB-File (zipped) - QGIS 2.8.1 crashes on Win-Server VM and Win7 64Bit when opening the layer Trecks_3D*

you are right, if using the **open** driver qgis crashes (but gdal/ogr is ok).

I also replicated with other datasets, but not all.

And if using the **closed** driver I never got a crash with any dataset.

#13 - 2015-12-28 03:06 AM - Giovanni Manghi

- Affected QGIS version changed from 2.8.1 to master

#14 - 2016-01-19 09:09 AM - Sandro Santilli

- Operating System changed from Windows to Windows , Linux

- OS version changed from Win 7 x64 to Win 7 x64, Ubuntu 14.04 64bit

I **can** reproduce under Ubuntu 14.04 64bit with GDAL trunk (2.1.0dev) and OpenFileGDB.
`ogrinfo -al` works fine.

#15 - 2016-01-19 09:11 AM - Sandro Santilli

```
#0  __memcpy_sse2_unaligned () at ../sysdeps/x86_64/multiarch/memcpy-sse2-unaligned.S:158
#1  0x00007f1d0386184e in QgsMapToPixelSimplifier::simplifyWkbGeometry (simplifyFlags=3, wkbType=QGis::WKBLineString,
    sourceWkb=0x7f1c5023809b "\\325V\\354/|\\237@\\340u\\236\\232\\001\\255\\026A\\300\\233\\234\\352\\333H\\tA",
sourceWkbSize=68191865,
    targetWkb=0x7f1c501d54ab "\\265\\246yG\f@", targetWkbSize=@0x7f1c56de0350: 9, envelope=..., map2pixelTol=1224.0509582740297,
writeHeader=true,
    isaLinearRing=false) at /usr/src/qgis/qgis-master/src/core/qgsmaptopixelgeometrysimplifier.cpp:276
#2  0x00007f1d03861f42 in QgsMapToPixelSimplifier::simplifyWkbGeometry (simplifyFlags=3, wkbType=QGis::WKBMultiLineString,
    sourceWkb=0x7f1c501c6112 "@\\252\\366?Pg\\bA", sourceWkbSize=25371, targetWkb=0x7f1c501d54a2 "@",
targetWkbSize=@0x7f1c56de0448: 10370,
    envelope=..., map2pixelTol=34.986439634150109, writeHeader=true, isaLinearRing=false)
    at /usr/src/qgis/qgis-master/src/core/qgsmaptopixelgeometrysimplifier.cpp:408
#3  0x00007f1d03862209 in QgsMapToPixelSimplifier::simplifyGeometry (geometry=0x7f1c50186300, simplifyFlags=3,
tolerance=34.986439634150109)
    at /usr/src/qgis/qgis-master/src/core/qgsmaptopixelgeometrysimplifier.cpp:460
#4  0x00007f1d038622ea in QgsMapToPixelSimplifier::simplifyGeometry (this=0x7f1c50196ec0, geometry=0x7f1c50186300)
    at /usr/src/qgis/qgis-master/src/core/qgsmaptopixelgeometrysimplifier.cpp:475
#5  0x00007f1d037e5507 in QgsAbstractFeatureIterator::simplify (this=0x7f1c5000ede0, feature=...)
    at /usr/src/qgis/qgis-master/src/core/qgsfeatureiterator.cpp:216
#6  0x00007f1d037e4c1c in QgsAbstractFeatureIterator::nextFeature (this=0x7f1c5000ede0, f=...)
    at /usr/src/qgis/qgis-master/src/core/qgsfeatureiterator.cpp:85
```

#16 - 2016-01-19 09:13 AM - Sandro Santilli

- Status changed from Open to In Progress

- Assignee set to Sandro Santilli

#17 - 2016-01-19 09:21 AM - Sandro Santilli

- File valgrind.txt added

There are a couple of these errors before the crash:

```
==10779== Thread 11 Thread (pooled):
==10779== Invalid read of size 8
==10779==    at 0x659F71E: QgsMapToPixelSimplifier::simplifyWkbGeometry(int, QGis::WkbType, unsigned char const*, int, unsigned char*,
int&, QgsRectangle const&, double, bool, bool) (qgsmaptopixelgeometrysimplifier.cpp:264)
```

==10779== by 0x659FF41: QgsMapToPixelSimplifier::simplifyWkbGeometry(int, QGis::WkbType, unsigned char const*, int, unsigned char*, int&, QgsRectangle const&, double, bool, bool) (qgsmaptopixelgeometrysimplifier.cpp:408)
==10779== by 0x65A0208: QgsMapToPixelSimplifier::simplifyGeometry(QgsGeometry*, int, double) (qgsmaptopixelgeometrysimplifier.cpp:460)
==10779== by 0x65A02E9: QgsMapToPixelSimplifier::simplifyGeometry(QgsGeometry*) const (qgsmaptopixelgeometrysimplifier.cpp:475)
==10779== by 0x6523506: QgsAbstractFeatureIterator::simplify(QgsFeature&) (qgsfeatureiterator.cpp:216)
==10779== by 0x6522C1B: QgsAbstractFeatureIterator::nextFeature(QgsFeature&) (qgsfeatureiterator.cpp:85)
==10779== by 0x642C02D: QgsFeatureIterator::nextFeature(QgsFeature&) (qgsfeatureiterator.h:234)
==10779== by 0x66AC8D4: QgsVectorLayerFeatureIterator::fetchFeature(QgsFeature&) (qgsvectorlayerfeatureiterator.cpp:237)
==10779== by 0x6522BCE: QgsAbstractFeatureIterator::nextFeature(QgsFeature&) (qgsfeatureiterator.cpp:76)
==10779== by 0x642C02D: QgsFeatureIterator::nextFeature(QgsFeature&) (qgsfeatureiterator.h:234)
==10779== by 0x66BE693: QgsVectorLayerRenderer::drawRendererV2(QgsFeatureIterator&) (qgsvectorlayerrenderer.cpp:290)
==10779== by 0x66BDBE3: QgsVectorLayerRenderer::render() (qgsvectorlayerrenderer.cpp:252)
==10779== Address 0x93f63e3b is 0 bytes after a block of size 25,371 alloc'd
==10779== at 0x4C2B7AA: operator new[](unsigned long) (vg_replace_malloc.c:392)
==10779== by 0x83A75015: QgsOgrFeatureIterator::readFeature(void*, QgsFeature&) (qgsogrfeatureiterator.cpp:340)
==10779== by 0x83A7474D: QgsOgrFeatureIterator::fetchFeature(QgsFeature&) (qgsogrfeatureiterator.cpp:215)
==10779== by 0x6522BCE: QgsAbstractFeatureIterator::nextFeature(QgsFeature&) (qgsfeatureiterator.cpp:76)
==10779== by 0x642C02D: QgsFeatureIterator::nextFeature(QgsFeature&) (qgsfeatureiterator.h:234)
==10779== by 0x66AC8D4: QgsVectorLayerFeatureIterator::fetchFeature(QgsFeature&) (qgsvectorlayerfeatureiterator.cpp:237)
==10779== by 0x6522BCE: QgsAbstractFeatureIterator::nextFeature(QgsFeature&) (qgsfeatureiterator.cpp:76)
==10779== by 0x642C02D: QgsFeatureIterator::nextFeature(QgsFeature&) (qgsfeatureiterator.h:234)
==10779== by 0x66BE693: QgsVectorLayerRenderer::drawRendererV2(QgsFeatureIterator&) (qgsvectorlayerrenderer.cpp:290)
==10779== by 0x66BDBE3: QgsVectorLayerRenderer::render() (qgsvectorlayerrenderer.cpp:252)
==10779== by 0x659696B: QgsMapRendererParallelJob::renderLayerStatic(LayerRenderJob&) (qgsmaprendererparalleljob.cpp:234)
==10779== by 0x6597CDF: QtConcurrent::FunctionWrapper1<void, LayerRenderJob&>::operator()(LayerRenderJob&) (qtconcurrentfunctionwrappers.h:86)
==10779==

Full valgrind log is atached

#18 - 2016-01-25 02:46 AM - Sandro Santilli

The crash only happens when the offending layer is the first one on the map. Crash also occurs by loading the "Tracks" layer.

#19 - 2016-01-25 05:02 AM - Even Rouault

The root cause is a bug in the OpenFileGDB driver (https://trac.osgeo.org/gdal/ticket/6332) that results in inconsistant WKB export, that QGIS crashes on.

#20 - 2016-01-25 05:15 AM - Sandro Santilli

Thanks Even.
Still I think QGIS should check before reading past the end of the buffer.
I'll look into that in the evening.

#21 - 2016-01-25 08:41 AM - Sandro Santilli

My take on boundary checking is here: https://github.com/qgis/QGIS/pull/2721
At the time of writing this comment, the code checks just enough to not fail in this case.
It's to be noted that the main QGIS WKB parser has no problem with the "malformed" WKB, only the WKB parser used inside the QgsMapToPixelSimplifier class, which for some reason acts on the WKB format (maybe it should just really stop doing that).

#22 - 2016-01-25 08:41 AM - Sandro Santilli

- Pull Request or Patch supplied changed from No to Yes

#23 - 2016-01-25 09:14 AM - Sandro Santilli

I'm taking back the "main QGIS WKB parser has no problem with the malformed WKB" as that's very unlikely as the QgsGeometry::fromWkb() method does not even **use** the passed WKB size argument to check against reading past the input end (is implemented by QgsAbstractGeometryV2::fromWkb not even taking that size parameter)

#24 - 2016-01-25 09:23 AM - Sandro Santilli

The other possibility is that QGIS centralized WKB parser simply handles better the parsing of geometry collections, NOT ASSUMING the dimensionality advertised for the compound object is the same of the one for the elements.

#25 - 2016-01-26 02:51 AM - Sandro Santilli

I've handled to make QgsGeometry.fromWkb mess up with memory using this input:


```
0107000000020000000102000080020000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0008DEDB5A0F7C6B0BE0102000080020000000000000000000000000000000000000000000000000000000000000000000000000000000000008DED
0000008DEDB5A0F7C6B03E
```


Now working on a proper testcase to secure the later fix

#26 - 2016-01-26 03:18 AM - Sandro Santilli

So the code showing unrobust WKB parser is here: https://github.com/qgis/QGIS/pull/2722
It confirms the internal WKB parser *also* needs attention.

#27 - 2016-01-27 03:36 AM - Sandro Santilli

Beside boundary checking, the problem is with the parser inside geometry-simplifier just skipping 5 bytes in each component WKB, rather than reading them. They do contain the actual sub-geometry type, which in this case does not have the same dimensionality of the container. I think this bug can be closed as soon as the boundary checking is in place (fixing the crash). Further improvements should probably involve using the WkbPtr (once it also has boundary checking).

#28 - 2016-01-27 07:27 AM - Sandro Santilli

- % Done changed from 0 to 90

Related issue (broken fromWkb): #14182

#29 - 2016-01-27 07:29 AM - Sandro Santilli

- Status changed from In Progress to Closed

Fixed in changeset commit:"bc4d16e8d912d9f6a605daa02d2959cd8145e770".

#30 - 2016-01-27 07:30 AM - Sandro Santilli

- Status changed from Closed to Reopened
- Target version set to Version 2.14

I'm reopening this to signal the fix did not include an automated testcase
(I suggest we add a "ready for test" status)

#31 - 2016-01-30 09:24 AM - Sandro Santilli

Test file stubbed in https://github.com/qgis/QGIS/pull/2744 -- no specific test for this case yet (needs to fix #14182 first, or I'll find another workaround via friendship)

#32 - 2016-02-01 02:39 AM - Sandro Santilli

Finally handled to produce the automated testcase for this special WKB: https://github.com/qgis/QGIS/pull/2750

The test checks that simplification cannot happen, due to the supposedly "malformed" WKB.
But truth is that the WKB is not necessarely malformed and the simplifier code might be improved to handle the special case (of dimension mismatch).
Only, for the sake of *this* ticket, I think we must be happy with what we have now, as the whole simplification code might be replaced anyway to somethign that doesn't act directly on the WKB (recommended).

PR https://github.com/qgis/QGIS/pull/2483 might go in that direction

#33 - 2016-02-01 03:24 AM - Sandro Santilli

- Status changed from Reopened to Closed
- % Done changed from 90 to 100
- Resolution set to fixed/implemented

Test is in place, closing this as fixed and guard-tested.

Files

qgis-20150320-095230-3012-3620-exported.zip	3.63 MB	2015-03-20	Flo Ju
Trecks.gdb.zip	1.62 MB	2015-03-22	Flo Ju
valgrind.txt	439 KB	2016-01-19	Sandro Santilli