

## QGIS Application - Bug report #15942

### Bad GML causes crash

2016-12-06 12:12 PM - Michael Moore

<b>Status:</b>	Closed	
<b>Priority:</b>	High	
<b>Assignee:</b>	Even Rouault	
<b>Category:</b>	Web Services clients/WFS	
<b>Affected QGIS version:</b>	2.18.7	<b>Regression?:</b> No
<b>Operating System:</b>	Ubuntu	<b>Easy fix?:</b> No
<b>Pull Request or Patch supplied:</b>	No	<b>Resolution:</b>
<b>Crashes QGIS or corrupts data:</b>	Yes	<b>Copied to github as #:</b> 23858
<b>Description</b>		
<p>I'm writing a WFS 2.0.0 server with GML 3.2. The GML I am serving up currently does NOT meet the GML spec and I didn't expect it to actually work in QGIS yet.</p> <p>However, trying to add the layer caused QGIS to crash. I would expect an error message or other graceful handling of bad XML instead of a hard crash.</p> <p>gdalinfo works against the XML without crashing.</p> <p>I have attached the gml and backtrace (as reported by OSX) below.</p> <p>I'm on Mac OSX, using the kyngchaos build 2.18.0 with no plugins installed.</p> <hr/> <p>Possible lead: When I fixed the namespace declarations in the original &lt;wfs:FeatureCollection&gt; tag QGIS no longer crashes, although the geometry is not displayed (though this is probably due to the GML still being incorrect).</p>		

#### Associated revisions

##### Revision 66518eb9 - 2017-11-11 12:11 PM - Even Rouault

[GML parser/WFS provider] Fix crash when typename and geometry field name are identical (fixes #15942)

##### Revision 8ae45fab - 2017-11-11 12:17 PM - Even Rouault

[GML parser/WFS provider] Fix crash when typename and geometry field name are identical (fixes #15942)

#### History

##### #1 - 2016-12-06 12:14 PM - Michael Moore

Shoot. I named the file bad\_geojson.gml instead of bad\_gml.gml. It is in fact GML and not GeoJSON.

Sorry for any confusion.

##### #2 - 2016-12-06 12:26 PM - Jürgen Fischer

- Status changed from Open to Closed

**#3 - 2016-12-06 01:15 PM - Michael Moore**

- File 3\_GetFeature.xml added
- File 2\_DescribeFeatureType.xml added
- File 1\_GetCapabilities.xml added

After a more thorough inspection, it looks I've been able to set up a place where you can (probably) reproduce this.

1. Add <http://stuporglue.org/qgis/> as a WFS Server Connection
2. Connect
3. Add the geom / walkin:geom layer
4. Crash

QGIS will make three WFS requests:

1. <http://stuporglue.org/qgis/?SERVICE=WFS&#38;REQUEST=GetCapabilities&#38;VERSION=2.0.0>
2. <http://stuporglue.org/qgis/?SERVICE=WFS&#38;REQUEST=DescribeFeatureType&#38;VERSION=2.0.0&#38;TYPENAME=walkin:geom>
3. <http://stuporglue.org/qgis/?SERVICE=WFS&#38;REQUEST=GetFeature&#38;VERSION=2.0.0&#38;TYPENAMES=walkin:geom&#38;STARTINDEX=0&#38;COUNT=1&#38;SRSNAME=urn:ogc:def:crs:EPSG::4326>

It will crash after the 3rd.

I have attached the output of these three requests below.

In addition, you can see a .gif of QGIS crashing here: <http://stuporglue.org/qgis/>

**#4 - 2016-12-07 08:37 PM - Michael Moore**

Jürgen,

Can you tell me why this was closed so quickly?

It's an issue that causes a segfault in QGIS and it's reproducible with the instructions I provided in my latest comment.

Thanks,  
Michael Moore

**#5 - 2016-12-07 11:53 PM - Jürgen Fischer**

- Tracker changed from Support to Feature request
- Project changed from QGIS Redmine (QGIS bug tracker) to QGIS Application

**#6 - 2016-12-07 11:54 PM - Jürgen Fischer**

- Tracker changed from Feature request to Bug report
- Status changed from Closed to Open
- Affected QGIS version set to 2.18.0
- Crashes QGIS or corrupts data set to No

**#7 - 2017-03-07 11:08 AM - Giovanni Manghi**

- Subject changed from Bad GML can cause QGIS to crash with SIGSEGV to Bad GML causes crash
- Crashes QGIS or corrupts data changed from No to Yes

- Affected QGIS version changed from 2.18.0 to 2.18.4
- Target version set to Version 2.18
- Priority changed from Normal to High
- Category set to Web Services clients/WFS

**#8 - 2017-05-01 01:02 AM - Giovanni Manghi**

- Easy fix? set to No
- Regression? set to No

**#9 - 2017-05-12 07:53 PM - Giovanni Manghi**

- Description updated
- Affected QGIS version changed from 2.18.4 to 2.18.7

**#10 - 2017-11-11 11:44 AM - Even Rouault**

- Assignee set to Even Rouault

**#11 - 2017-11-11 12:11 PM - Even Rouault**

- Status changed from Open to Closed
- % Done changed from 0 to 100

Applied in changeset commit:qgis|66518eb9ee609042de02f175a2f8e1b47ae22bc8.

**Files**

bad_geojson.gml	418 KB	2016-12-06	Michael Moore
backtrace.txt	105 KB	2016-12-06	Michael Moore
1_GetCapabilities.xml	4.45 KB	2016-12-06	Michael Moore
2_DescribeFeatureType.xml	1.96 KB	2016-12-06	Michael Moore
3_GetFeature.xml	1.92 KB	2016-12-06	Michael Moore