QGIS Application - Bug report #14182
Geometry.fromWkb crashes on unexpected/malformed WKB

2016-01-27 07:26 AM - Sandro Santilli

Status:	Closed		
Priority:	Normal		
Assignee:	Jürgen Fischer		
Category:	Geometry		
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	fixed/implemented
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	22184

Description

Testcase can be found on https://github.com/qgis/QGIS/pull/2722
This is a spin-off of ticket #12416

Last tested on commit:d80a632bd8a9033bffa17295c7c6bd3d49c232b5

History

#1 - 2016-02-01 03:09 AM - Sandro Santilli

The test in PR https://github.com/qgis/QGIS/pull/2722 was bogus, I'm working on another test, but it isn't easy to predict whether or not a segfault would happen.
Valgrind reports are clear on the matter, though.

#2 - 2016-02-01 03:20 AM - Sandro Santilli

So the new test is in https://github.com/qgis/QGIS/pull/2751.
Main problem is that parsing does NOT happen upfront but only when needed, so it takes forcing a call like "exportToWkt" to trigger memory errors.
I don't know if different code paths trigger different WKB parsing, which would be very hard to debug.

#3 - 2016-02-01 03:34 AM - Sandro Santilli

- Tag set to WKB

#4 - 2016-02-01 07:36 AM - Sandro Santilli

- Assignee changed from Sandro Santilli to Jürgen Fischer

Reassigning to Jurgen as he's championing https://github.com/qgis/QGIS/pull/2748 which provides a fix for this and a few more bugs.

#5 - 2016-02-02 12:57 AM - Sandro Santilli

- Category set to Geometry

#6 - 2016-02-10 02:26 AM - Sandro Santilli

- Resolution set to fixed/implemented

- Status changed from In Progress to Closed

- % Done changed from 0 to 100

fixed by commit:b9726d7285733c27d42456c115e28d5a37f3e0be