QGIS Application - Bug report #13919
QGIS server security patch: random crashes and performance regression

2015-12-01 12:26 AM - Andreas Neumann

Status:	Closed		
Priority:	Severe/Regression		
Assignee:	Nyall Dawson		
Category:	QGIS Server		
Affected QGIS version:	master	**Regression?:**	No
Operating System:	Linux Ubuntu 64bit	**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	
Crashes QGIS or corrupts data:	No	**Copied to github as #:**	21941

Description

With the commit:422abbd - PR#2056 I get random crashes when vector data is involved (from Postgis).

There is also a quite large performance regression - many more complex projects with lots of Postgis layers are 2-3 times slower than before this patch. This can be reproduced with any project that has lots of Postgis layers.

I will try to create a backtrace from the crashes - if someone can help me create one.

Associated revisions

Revision 752f6bd1 - 2016-01-22 08:45 AM - Nyall Dawson

Fix classes which violate rule of three, by implementing required
copy/= operators or making them private

This revealed (and fixes) some issues, including a potential crash
using server access control (refs #13919), and a potential crash with
diagrams

Revision 69ce5599 - 2016-01-22 08:48 AM - Nyall Dawson

Fix some oddities in server access control and bindings (refs #13919)

Revision 0446f507 - 2016-02-22 12:20 AM - Nyall Dawson

Fix slow filter rect requests with server python plugins (refs #13919)

Revision 90a4ae80 - 2016-02-22 01:00 AM - Nyall Dawson

Fix #13919, don't reset layer subsetStrings when server python plugins
are enabled

History

#1 - 2015-12-01 12:30 AM - Andreas Neumann

Maybe the issues can be related to Martin Dobias' comment on the issue?:

@sbrunner This is unfortunately very dangerous to introduce pointer to original QgsVectorLayer and has to be avoided.

The correct approach would be that a custom feature filter provider stores any data that it may need. This change may otherwise introduce race conditions and crashes - and others may mistakenly try to use mLayer for more functionality, leading to even more problems.

Please could you update QgsFeatureFilterProvider class so that it does not use QgsVectorLayer directly? There is mLayerID member variable in QgsMapLayerRenderer which may be used to identify a layer if necessary.

#2 - 2015-12-01 01:02 AM - Jürgen Fischer

- Assignee set to Stéphane Brunner

#3 - 2015-12-01 05:36 AM - Stéphane Brunner

Andreas Neumann I think that's not related on what Martin Dobias say....

Can you specify what you are doing?
Are you using QGIS server?
Is it also visible on QGIS client?

#4 - 2015-12-01 05:37 AM - Stéphane Brunner

In all case I will have a look on what Martin Dobias say :-)

#5 - 2015-12-01 06:37 AM - Andreas Neumann

I get a crash in my Apache log - randomly. And the WMS client gets a corrupted image - tested in both QGIS Desktop or OpenLayers as a client.

[Mon Nov 30 09:17:58.227308 2015] [core:error] [pid 15465] [client 10.63.238.200:51961] End of script output before headers: qgis_mapserv.fcgi, referer: http://gisbrowser/maps/leitungskataster/leitungskataster?format=image/png;%20mode=8bit&visibleLayers=Swisscom,Gas,Wasser,Fernw%C3%A4re,Elektro,Abwasser,%C3%9Cbersicht%20Vektor25,Nomenklatur,Geb%C3%A4ude,Grenzen,Einzelobjekte,Rohrleitungen,Bodenbedeckung,Liegenschaften%20Flten%20Fl%C3%A4che,Einzelobjekte%20Unterst%C3%A4nde,Einzelobjekte%20Unterirdische%20Geb%C3%A4ude&fullColorLayers=Orthofoto%202010%202010%20(25cm),Orthofoto%202008%20(10cm)&startExtent=692000,241500,700100,249000&maxExtent=692000,241500,700100,249000&search8;searchtables=abwasser.suchtabelle
[Mon Nov 30 09:17:59.308226 2015] [fcgid:error] [pid 14799] mod_fcgid: process /home/www/cgi/qgis_mapserv.fcgi(16196) exit(communication error), get signal 11, possible coredump generated

#6 - 2015-12-02 05:41 AM - Stéphane Brunner

Hello Andreas,

I'm having a look, I will get some new when I have something to test :-)

CU
Stéphane

#7 - 2015-12-04 05:42 AM - Stéphane Brunner

@Andreas Neumann

I just implements what's Martin Dobias speaks here:
https://github.com/sbrunner/QGIS/tree/access-control-fix

Can you test it?

#8 - 2015-12-28 05:14 AM - Andreas Neumann

Hi Stéphane,

I hope you had a good Christmas vacation!

I tested https://github.com/sbrunner/QGIS/commit/6d56cba465b3612c7e685d724e0e8ecc55c5e1bc

Unfortunately, I still get the crashes and the slowness ;-(

I could help debug QGIS Desktop issues, but I am not good at helping debug QGIS sever issues ...

Perhaps we need another QGIS dev to help us review the issue?

Let me know, if you have any ideas.

Andreas

#9 - 2015-12-28 05:15 AM - Andreas Neumann

Note that all the project I tested with QGIS server use Postgis as data source - if that helps.

#10 - 2016-01-19 02:46 AM - Stéphane Brunner

I don't succeed to reproduce it, do you have an example?
Do you use CGI or FCGID?
Witch version of postgres, postgis do you use?

#11 - 2016-01-21 11:50 PM - Nyall Dawson

- Status changed from Open to Feedback

Please test with current master, possibly fixed

#12 - 2016-02-04 02:17 AM - Andreas Neumann

Finally I had the chance to install QGIS server on a different (non-productive) server.

I have good and bad news.

The good news: the crashes are gone
The bad news: it is still considerably slower than before your patch, Stéphane.

I will ask Nyall if he is available to examine the issue why is so much slower.

#13 - 2016-02-16 03:47 AM - Nyall Dawson

- Status changed from Feedback to In Progress

- Assignee changed from Stéphane Brunner to Nyall Dawson

Tracked this down. Working on a fix now.

#14 - 2016-02-17 01:55 AM - Andreas Neumann

Hi Stéphane,

Nyall will soon provide a fix for my performance issue.

The issue was around incorrectly clearing the filters that do server side filtering. Then the server fetched all features and filtered locally - as I understand - rather than filtering on the PostgreSQL server.

BTW: Nyall praises your excellent and exhaustive unit tests! They also helped to uncover additional issues unrelated to this issue.

BTWII: the crash issue had to do with the inverted polygon renderer. Not sure if this was caused by your patch or some other issue.

Thanks to both of you!
Andreas

#15 - 2016-02-17 02:03 AM - Stéphane Brunner

Thanks @Nyall for your investigations, and @Andreas Neumann for your tests and patience :-)

#16 - 2016-02-21 06:08 PM - Nyall Dawson

- Status changed from In Progress to Closed

Fixed in changeset commit:"90a4ae806558690152f60d0cae96662b40753814".