
Long posts cause segmentation fault w.SVN551 patch

Posted by hypnotoad - 2008/03/11 02:10

Edit: Subject edited for clarification, see end of the thread.

There is a weird bug I hope to squash, and hopefully someone can help me with it. Are there any developers around, at all?

The problem lies somewhere in page 2 of this topic in my boards. If you try to go to page 2 of the topic you'll see that it's not possible - there is no response from the webserver and if I check the Apache log file (error.log), all I get is:

```
child pid 7365 exit signal Segmentation fault (11)
```

I and other members can reproduce that problem on a variety of browsers, OS etc. But I could not find a direction on what to look out for.

The stats:

Apache 2.0.55

Mysql 5.0.21

PHP 5.1.2

Joomla 1.0.12

Fireboard 1.0.4 with SVN-patch-package, updated from Joomlaboard, updated from Simpleboard

Template is a custom one, based on "default" - no fancy scripts like Moo used anywhere.

The server is a VPS with 256MB RAM, running Ubuntu 6.06.

=====

Re:Forum page cannot be opened - Apache dies

Posted by hypnotoad - 2008/03/11 16:21

I reproduced the problem on my local test installation, using the database and files from the server - the very same effect, with newer versions of Apache, MySQL and PHP (Ubuntu 7.10). Also, it can't be a resource issue - 1 GB Ram on a 2GHz machine should be enough!

I systematically tried to disable or change the following settings, all with no effect on the bug:

#posts per page / threads per page: 15 => 7

Mambots on board text

Template back to default

Emoticons

User stats

User profiles CB => Fireboard

=====

Re:Forum page cannot be opened - Apache dies

Posted by danialt - 2008/03/11 22:30

error looks like a system problem.

<http://drupal.org/node/220316>

=====

Re:Forum page cannot be opened - Apache dies

Posted by hypnotoad - 2008/03/13 01:26

Well sure it does - it's a segmentation fault. But other than showing the same symptome, I don't see how this is related to

the behavior shown in the link to Drupal you posted - I don't use e-accelerator or anything similar. It's a plain Ubuntu VPS installation, using the versions of php, apache etc that are available for it. Plus, I can reproduce the problem locally. Also Ubuntu, but completely different software packages (everything newer).

Other causes for Apache segfaults I found were conflicting modules, but I really use only a necessary set of apache modules:

```
ls -l /etc/apache2/mods-enabled/  
total 0  
lrwxrwxrwx 1 root root 36 Mar  6 07:36 cgi.load -> /etc/apache2/mods-available/cgi.load  
lrwxrwxrwx 1 root root 40 Mar  6 10:58 include.load -> /etc/apache2/mods-available/include.load  
lrwxrwxrwx 1 root root 37 Mar  6 10:53 php5.conf -> /etc/apache2/mods-available/php5.conf  
lrwxrwxrwx 1 root root 37 Mar  6 10:53 php5.load -> /etc/apache2/mods-available/php5.load  
lrwxrwxrwx 1 root root 40 Mar  6 10:58 rewrite.load -> /etc/apache2/mods-available/rewrite.load  
lrwxrwxrwx 1 root root 36 Mar  6 10:57 ssl.load -> /etc/apache2/mods-available/ssl.load  
lrwxrwxrwx 1 root root 39 Mar  6 10:58 suexec.load -> /etc/apache2/mods-available/suexec.load
```

I also tried disabling Joomla Cache and reverting the the default Joomla template - all with no success.

I was able, however, to reduce the possibilities. The problem must come from the text in "defunct" posts. When viewing threaded view and selecting the single "broken" posts, they don't work (producing the same segfault), all other posts display fine. When I delete the text in the posts manually in the database, the whole thread display fine again - but I don't think that's a solution for the long run...

Out of my mind, I think the problem might be somewhere in the parser...

Re:Forum page cannot be opened - Apache dies

Posted by hypnotoad - 2008/03/13 02:59

I found the reason for the page not loading: Long posts fail to show up ("white page of death") and the apache thread dies. It happens to any post longer than a certain number of characters on both of my Ubuntu systems (local and on the VPS)... :huh:

Edit: found the origin! The Developer Patch SVN551 causes the bug. A "vanilla" FB installation works, while long posts can't be displayed anymore after installing the patch. Abandoning that patch is not really an option for me - it made FB usable for the first time for me! I'll try to find the code causing this.

After some more searching, I found the cause in smile.class.php, line (about) 546:
\$utf8 = (preg_match("/^(||\xE0|{2})|\xED|\xF0|{3})|\xF4|{2})*\$"/, \$str)) ? true : false;

That got introduced in the newer version in SVN, using the imported function htmlspecialchars (v 1.6). The older version did not include checking for UTF and worked fine. The workaround I am using for now is to comment that line, and just write:
\$utf8=false;
instead.

Is it possible to find a proper fix for that? It seems like preg_matching that long regex to a long post crashes Apache on Debian/Ubuntu. A similar problem could be this one - with no solution, however.

Re:Forum page cannot be opened - Apache dies

Posted by frodon2 - 2008/04/01 16:37

Thanks a lot mate, i had the same issues for ages without being able to understand why. I will try your workaround and let you know if it works for me.

Workaround working as expected.

=====

Re:Long posts cause segmentation fault w.SVN551 pa

Posted by Oddsodz - 2008/04/07 22:24

Thanks for finding this out. This bug was getting on my tits.

The work around worked.

Thank you very much

=====

Re:Long posts cause segmentation fault w.SVN551 pa

Posted by KeithDickens - 2008/04/19 04:55

The work around worked slick.

This problem was going to keep my site from going live. What exactly are the repercussions of disabling this code though?

=====

Re:Long posts cause segmentation fault w.SVN551 pa

Posted by karn_edge - 2008/04/30 21:40

Awesome this fixed the issue, yeah I was getting the 500 Internal Server Error everytime I tried to look at a long post. The patch fixed a lot of other things but I have a lot of How To posts on our private forums for staff. Thanks.

=====

Re:Long posts cause segmentation fault w.SVN551 pa

Posted by SIGHUP - 2008/05/01 11:34

Thanks so much for the code! One of my users had a very long post and for the life of me could not figure out why it was bugging out me. This did it, thank you!

=====