Ticket #432 (assigned defect)

PHP crashed - [notice] EACCELERATOR

Opened 10 months ago
Last modified 3 weeks ago

Reported by:	cwebnet	Owned by:	hans
Priority:	major	Milestone:	
Component:	Optimizer	Version:	0.9.6.1
Keywords:		Cc:	

Description

Hi, i'd like report some issues on my logs

I have a LOT of crashes into my apache2 logs since 0.9.6 and 0.9.6.1 versions

```
] [notice] EACCELERATOR(3684): PHP crashed on opline 16 of main()
AND  autoload_class()
AND just:
] [notice] EACCELERATOR(18385): PHP crashed
```

this is not happend in 0.9.5.3 version, almost the crash is because of include(), include_once(), require_once() and require().

I think i will go back to 0.9.5.3.

*

PHP Version 5.2.13-0.dotdeb.1
Suhosin Patch 0.9.7
eAccelerator v0.9.6.1 and eAccelerator v0.9.6 in another server
Server API CGI/FastCGI with mod_fcgi

Hope this helps

Attachments

- ticket432.diff (979 bytes) - added by *hans* 9 months ago.
  optimizer fix

Change History

Changed 10 months ago by lissyx

comment:3

I also reproduce it with 0.9.6:

[root@php ~]# php-cgi test.php EACCELERATOR cached: "/root/test.php" [Mon Jun 28 11:54:37 2010] [notice] EACCELERATOR(45183): PHP crashed on opline 59 of _addLimitation() at /root/test.php:33

Bus error: 10 (core dumped) [root@php ~]# php-cgi -v PHP 5.3.2 with Suhosin-Patch (cgi-fcgi) (built: Jun 26 2010 11:05:49) Copyright (c) 1997-2009 The PHP Group Zend Engine v2.3.0, Copyright (c) 1998-2010 Zend Technologies

with eAccelerator v0.9.6, Copyright (c) 2004-2010 eAccelerator, by eAccelerator

Changed 9 months ago by hans   comment:4

- **Status** changed from *new* to *assigned*
- **Owner** changed from *somebody* to *hans*

woops i accidentally removed one of lissyx postings while cleaning this ticket of spam. this was the text:

I've just been notified of 502 errors on an OpenX installation running under PHP 5.3.2/nGinx with FastCGI.

After investigating, I've been able to reproduce the issue:

```php
<?php
    define('MAX_LIMITATION_EQUAL', 0);
    define('MAX_LIMITATION_NOT_EQUAL', 1);
    define('MAX_LIMITATION_BITWISE', 2);

$aLimitations = array();
$aParams['publisher_id'] = "5";

_addLimitation($aLimitations, 'publisher_id', 'p.affiliateid', $aParal

    function _addLimitation(&$aLimitations, $entityIdName, $columnName
    {
        // Add single quotes around non-integer columns
        if (($entityIdName == 'ad_type')
         || ($entityIdName == 'ad_active')
         || ($entityIdName == 'placement_active')
         || ($entityIdName == 'placement_anonymous')
        ) {
            $value = "'" . str_replace(',', "','", $value) . "'";
        }

        // If there are multiple values, use IN instead of =
        if (strpos($value, ',') !== false) {
            $aLimitations[] = "$columnName IN ($value)";
        } else {
            switch ($comparison_type) {
            case MAX_LIMITATION_NOT_EQUAL:
                $aLimitations[] = "$columnName != $value";
                break;
            case MAX_LIMITATION_BITWISE:
                $aLimitations[] = "($columnName & $value > 0)";
                break;
            default:
                $aLimitations[] = "$columnName = $value";
                break;
            }
        }
    }
?>
```

And take a look at the result:

```
[root@php ~]# php-cgi test.php
EACCELERATOR hit: "/root/test.php"
[Mon Jun 28 11:49:09 2010
] [notice] EACCELERATOR(41164): PHP crashed on opline 59 of _addLimit

Bus error: 10 (core dumped)
[root@php ~]# php test.php
```

```
[root@php ~]# php-cgi -v
PHP 5.3.2 with Suhosin-Patch (cgi-fcgi) (built: Jun 26 2010 11:05:49)
Copyright (c) 1997-2009 The PHP Group
Zend Engine v2.3.0, Copyright (c) 1998-2010 Zend Technologies
    with eAccelerator v0.9.6.1, Copyright (c) 2004-2010 eAccelerator,
[root@php ~]# php -v
PHP 5.3.2 with Suhosin-Patch (cli) (built: Jun 26 2010 11:05:49)
Copyright (c) 1997-2009 The PHP Group
Zend Engine v2.3.0, Copyright (c) 1998-2010 Zend Technologies
    with eAccelerator v0.9.6.1, Copyright (c) 2004-2010 eAccelerator,
[root@php ~]#
```

It looks like it's linked with FastCGI so ?

Changed 9 months ago by hans   comment:5

Confirmed. Its a bug in the eAccelerator optimizer. Workaround for now is to disable the optimizer with

eaccelerator.optimizer="0"

I will look into this ASAP.

Changed 9 months ago by hans   comment:6

- **Component** changed from *eAccelerator* to *Optimizer*

Changed 9 months ago by lissyx   comment:7

Thanks for confirming :)

About your workaround, what are the side effets of disabling the optimizer ? I fear that it might mean « loosing the big boost provided by eaccelerator ».

Changed 9 months ago by lissyx   comment:8

I played a bit with git bisect, here is what I discovered :)

```
0d62638a1c5bdf5af08663544e616b76dd1637aa is the first bad commit
commit 0d62638a1c5bdf5af08663544e616b76dd1637aa
Author: hans <hans@3147fa9f-2f0e-0410-9769-c5c2697de4ad>
Date:   Wed Nov 11 15:35:06 2009 +0000

    Fixed ticket #194, updated opcode.c

    git-svn-id: https://svn.eaccelerator.net/eaccelerator/trunk@364 3
:100644 100644 8e879389d8fd669795a995f9df5026fe353dcb05 8c741e4f2ad4f
:100644 100644 f1e5907b2a48863a4f98716a39e8f5f7d0f46669 484a3fd9758cd
:100644 100644 4e5d6ce6745fb06f037e21bd289e59a87078b0cb 3c72f6554a4ca
bisect run success
```

Changed 9 months ago by hans

- **attachment** *ticket432.diff* added

optimizer fix

Changed 9 months ago by hans   comment:9

Can you please try the attached patch and see if it solves your problems? (dont forget to re-enable eaccelerator.optimizer for testing ;))

Your reproduction script works fine on my development machine using this optimizer

patch.

I will test some more with a full OpenX install.

Just did a full install from scratch of OpenX 2.8.5 on PHP 5.3.2 with this patch applied to the current svn trunk of eAccelerator.

With eAccelerator optimizer enabled, everything went smooth and all backend pages seem to work.

Well, I'm sorry but it doesn't seems enough.

```
[root@php ~]# php-cgi -v
PHP 5.3.2 with Suhosin-Patch (cgi-fcgi) (built: Jun 26 2010 11:05:49)
Copyright (c) 1997-2009 The PHP Group
Zend Engine v2.3.0, Copyright (c) 1998-2010 Zend Technologies
    with eAccelerator v0.9.6.1+hyperion, Copyright (c) 2004-2010 eAcc
[root@php ~]# php-cgi test.php
[Fri Aug 13 10:53:35 2010
] [notice] EACCELERATOR(21477): PHP crashed on opline 59 of _addLimit

Bus error: 10 (core dumped)
```

Disabling optimizer doesn't change this.

One URL that exposes the flaw is /www/admin/stats.php?entity=global& breakdown=affiliates

Last edited 8 months ago by lissyx (previous) (diff)

What is hyperion?

I'm testing your exact test script as mentioned above and have no crash with vanilla 5.3.3 and the current trunk as well as the current svn state of the 0.9.6 branch of eAccelerator.

Did you empty your diskcache before testing? You need to clean out your cachedir when you disable the optimizer as well.

It might also be related to Suhosin, and i dont know what this hyperion is that your php-cgi -v states.

Last edited 8 months ago by hans (previous) (diff)

Tested with Suhosin patch 0.9.10 and svn trunk:

```
hans@meukee /tmp/eaccelerator $ php-cgi -v
PHP 5.3.3 with Suhosin-Patch (cgi-fcgi) (built: Aug 13 2010 13:53:21)
Copyright (c) 1997-2009 The PHP Group
Zend Engine v2.3.0, Copyright (c) 1998-2010 Zend Technologies
    with eAccelerator v1.0-dev, Copyright (c) 2004-2010 eAccelerator,
hans@meukee /tmp/eaccelerator $ sudo rm -rf *
hans@meukee /tmp/eaccelerator $ php-cgi ~/Sites/bug432.php
[37636] EACCELERATOR cached: "/Users/hans/Sites/bug432.php"
X-Powered-By: PHP/5.3.3
Content-type: text/html
```

```
hans@meukee /tmp/eaccelerator $ php-cgi ~/Sites/bug432.php
[37637] EACCELERATOR hit: "/Users/hans/Sites/bug432.php"
X-Powered-By: PHP/5.3.3
Content-type: text/html
hans@meukee /tmp/eaccelerator $
```

Don't worry for the hyperion, it's the name of the box, and I renamed my eaccelerator version to add it to be sure to I was dealing with the good one.

But you're right, I didn't purged the disk cache. I'm retesting.

Purging the disk cache and restarting my php-cgi processes, it looks like it's fixed !

Thanks, and sorry for the delay!

Hello,

With this patch included (or without, I dunno yet), on the same box (after upgrading to FreeBSD 7.3-RELEASE-p2), I get new errors :

```
/root/eAccelerator.OpenX.crash0.txt:] [notice] EACCELERATOR(11702): P
/root/eAccelerator.OpenX.crash1.txt:] [notice] EACCELERATOR(15057): P
```

This is OpenX 2.8.2 as packaged by FreeBSD.

```
# php-cgi -v
PHP 5.3.3 with Suhosin-Patch (cgi-fcgi) (built: Sep  3 2010 17:21:18)
Copyright (c) 1997-2009 The PHP Group
Zend Engine v2.3.0, Copyright (c) 1998-2010 Zend Technologies
    with eAccelerator v0.9.6.1, Copyright (c) 2004-2010 eAccelerator,
```

I'll try to dig into the OpenX code to grab a short piece of code that reproduce the issue.

For the record, I think the bug might be just lying in MAX_adRender(), as the other crash happens just after it's called :

```
3636 $outputbuffer = MAX_adRender($row, $zoneId, $source, $target, $c
3637 $output = array(
3638 'html'          => $outputbuffer,
3639 'bannerid'      => $row['bannerid'],
3640 'contenttype'   => $row['contenttype'],
3641 'alt'           => $row['alt'],
3642 'width'         => $row['width'],
3643 'height'        => $row['height'],
3644 'url'           => $row['url'],
3645 'campaignid'    => $row['campaignid'],
3646 'clickUrl'      => $row['clickUrl'],
3647 'logUrl'        => $row['logUrl'],
3648 'aSearch'       => $row['aSearch'],
3649 'aReplace'      => $row['aReplace'],
3650 'bannerContent' => $row['bannerContent'],
3651 'clickwindow'   => $row['clickwindow'],
3652 'aRow'          => $row,
3653 'context'       => _adSelectBuildContext($row, $context)
3654 );
```

```
3655 // Init block/capping fields to avoid notices below
3656 $row += array(
3657 'block_ad'            => 0,
3658 'cap_ad'              => 0,
3659 'session_cap_ad'      => 0,
3660 'block_campaign'      => 0,
3661 'cap_campaign'        => 0,
3662 'session_cap_campaign' => 0,
3663 'block_zone'          => 0,
3664 'cap_zone'            => 0,
3665 'session_cap_zone'    => 0,
3666 );
```

Changed 7 months ago by hans   comment:18

> The patch attached to this bug is not included in 0.9.6.1. Can you apply the attached
> patch, flush caches and test again? Thanks.

Changed 5 months ago by quintessence   comment:19

> I also had bus error(10) in logs after opening some files from OpenX (version 2.8.7) , I
> testes attached patch with no success . But I just installed latest svn (optimize.c 425
> revision) and there is no more crash , all seems to work correct . Thank you for fix .

```
PHP 5.3.3 with Suhosin-Patch (cli) (built: Oct 12 2010 11:59:12)
Copyright (c) 1997-2009 The PHP Group
Zend Engine v2.3.0, Copyright (c) 1998-2010 Zend Technologies
    with the ionCube PHP Loader v3.3.19, Copyright (c) 2002-2010, by
    with eAccelerator v1.0-dev, Copyright (c) 2004-2010 eAccelerator,
```

```
 eaccelerator.optimizer => 1 => 1
```

```
Server version: Apache/2.2.17
```

Changed 3 weeks ago by WJQTRACY   comment:20

> Wow, wonderful blog layout! Are you looking for Coach purses Wedges?...
> [url= http://www.coachpurses2011.com/]Coach pursesurl
> [url= http://www.coachpurses2011.com/]Coach purses on saleurl