MOPS-2010-021: PHP fnmatch() Stack Exhaustion Vulnerability

May 11th, 2010

PHP’s fnmatch() function can be used to crash PHP through a stack exhaustion attack.

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 stack exhaustion vulnerability that crashes PHP in different ways depending on how libc implements fnmatch() on your platform e.g. a too deep recursion. It is not believed to be exploitable for code execution.

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. If you cannot reproduce it then you might need to adjust your stack ulimit. The code might not crash if your libc does not implement fnmatch() in a recursive way.

```
<?php
$a57 = str_repeat("A", 16000000);
$a265 = fnmatch($a57, "");
?>
```

Notes

Because this is very likely only a local stack exhaustion attack fixing it is considered low priority.