PHP 5.3.6 closes five security holes

Written by ph0bYx
Saturday, 19 March 2011 21:06 -

The PHP developers have released PHP 5.3.6, a maintenance update to the PHP interpreter. Among over 60 bug fixes are a number of fixes for security related problems.

A format string vulnerability in the phar extension of PHP 5.3.5, CVE-2011-1153 , may allow attackers to view memory, cause a denial of service or execute arbitrary code. There was also an integer overflow in the shmop_read() function which allowed for denial-of-service (CVE-2011-1092). Other flaws included crashes with crafted tags in exif metadata and ziparchive with empty archives. Security has also been enhanced in the protocol parsing done by the fastcgi process manager (FPM SAPI). Some of the flaws reportedly affect all versions of PHP 5.3.x and earlier.

The release also sees SQLite3 upgraded to version 3.7.4 and PCRE updated to version 8.11. The ability to connect to HTTPS sites through a proxy was also added as was options for debugging backtrace functions. A full list of changes is available in the change log . The PHP developers remind users that PHP 5.2 is no longer supported and encourage users to upgrade to PHP 5.3.6.

PHP 5.3.6 can be downloaded as source code or as Windows binaries from the php.net web site.