PHYS ORG

PHP Group to try again to fix vulnerability

May 8 2012, by Bob Yirka

(Phys.org) -- The PHP group, under fire for prematurely pushing out a patch to fix a recently uncovered vulnerability in the language, says it is working on another patch to fix the problem as web site owners scramble to ensure the integrity of their sites. Fortunately, as dire as that sounds, few sites appear to be at risk because the vulnerability only exists for those running in Common Gateway Interface (CGI) mode.

PHP is a scripting language (it used to stand for "Personal Home Page" but now means PHP: Hypertext Processor) used by servers to provide web services and can be embedded into HTML documents rather than forcing programmers to call external routines. Doing so makes creating and maintaining pages much simpler, though as this latest vulnerability shows, it can also be less secure.

In this case, the problem is not so much that a vulnerability was found, but that it was accidently made public by some unknown person at

Eindbazen (the group that found the vulnerability) publishing it to Reddit (a social news website). That caused nefarious types to work up code that could easily test a web site for the vulnerability and then exploit it when found.

The vulnerability is that for websites running in CGI mode, it was found that a URL passed with a “-“ character could be used as a command string causing the site to carry out instructions via switches, e.g. -c, -s, -d. By doing so, hackers could gain a copy of index.php for example. Worse of course, they could also gain admittance to user data or be used to carry out instructions such as to a cause denial of service. To be clear, the problem is not that command strings can be passed to a web site, but that switches can be passed that cause commands to run on the server. Most servers allow characters to be passed as data strings for interpretation by PHP parsing.

Upon hearing of the vulnerability being made public, the PHP Group rushed to push out a patch. Unfortunately, the patch has proven to be ineffective, which has left some sites more vulnerable than before as owners ceased working on protection measures believing their server was safe.

Moving forward, the PHP Group has advised site owners to update their PHP version and then to test their site themselves to see if they are at risk. If so, they suggest those site owners contact Eindbazen for some possible remedies that can be used until a permanent fix is ready for distribution.

More information: www.php.net/

Citation: PHP Group to try again to fix vulnerability (2012, May 8) retrieved 24 April 2024 from https://phys.org/news/2012-05-php-group-vulnerability.html