

Re: @(#)Mordred Labs advisory – Integer overflow in PHP str_repeat() function

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-04/0097.html>

From: Jon Ribbens (jon+bugtraq@unequivocal.co.uk)

Date: 04/04/03

Date: Fri, 4 Apr 2003 21:20:13 +0100

From: Jon Ribbens <jon+bugtraq@unequivocal.co.uk>

To: bugtraq@securityfocus.com

Javi Lavandeira <javi@isr.co.jp> wrote:

- > You seem to be forgetting about PHP's `safe_mode`, `disable_functions`
- > and `open_basedir` directives. If configured properly, a user in a
- > server with PHP support should not be able to execute commands, read
- > other users' files or do anything outside his directory. Even though
- > PHP is running with the privileges of the web server, the user
- > doesn't have these privileges (again, if properly configured). Many
- > ISPs configure PHP in this way.
- >
- > **IF* the overflow really exists *AND* is exploitable, I would be*
- > *very worried, because *THEN* users could gain the privileges of the*
- > *web server and do things they shouldn't be doing.*

Then you should be very worried. Back in September 2000, Zeev Suraski (PHP developer and co-author of Zend, the PHP4 scripting engine) said: (<http://marc.theaimsgroup.com/?l=php-dev&m=96815200329214>)

- > *safe mode is indeed falsely advertised as being safe. It's very*
- > *likely to contain bugs. As far as I'm concerned, it should be*
- > *clearly advertised as something that would prevent the casual user*
- > *from doing stuff he's not supposed to do, but isn't suitable for*
- > *protecting against hackers.*