

[UNIX] WordPress wp_title() XSS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00030.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 13 Mar 2007 15:01:50 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

WordPress wp_title() XSS

SUMMARY

" <<http://www.wordpress.org/>> WordPress is a state-of-the-art semantic personal publishing platform with a focus on aesthetics, web standards, and usability." A cross site scripting vulnerability in WordPress's wp_title allows remote attackers to inject arbitrary HTML and/or JavaScript.

DETAILS

Vulnerable Systems:

- * WordPress version 2.0.10-alpha and prior
- * WordPress version 2.1.3-alpha
- * WordPress version 2.2-bleeding (Revision 5002)

Workaround:

\$title takes the value in raw (without any type of filter) of \$year which is an a query variable, that can be filled with any web browser via a simply GET parameter.

Solution/Fix:

The latest SVN Revision (greater than revision 5002) has already fixed

[UNIX] WordPress wp_title() XSS

this bug:

<<http://trac.wordpress.org/changeset/5003>>

<http://trac.wordpress.org/changeset/5003>

For series 2.1.x and 2.0.x, the vendor will fix this in the next set of dot releases.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:g30rg3x@xxxxxxxx>> g30rg3_x.

The original article can be found at:

<<http://chxsecurity.org/advisories/adv-1-mid.txt>>

<http://chxsecurity.org/advisories/adv-1-mid.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.