

[UNIX] XSS Vulnerabilities Found in XMB Forum

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0074.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/23/03

To: list@securiteam.com

Date: 23 Jun 2003 10:44:59 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

XSS Vulnerabilities Found in XMB Forum

SUMMARY

<<http://www.xmbforum.com/>> XMB Forum is "a free web-based bulletin board system written in PHP with a MySQL backend". Multiple cross site scripting vulnerabilities have been found in the XMB Forum, these vulnerabilities would allow attackers to insert malicious HTML and JavaScript code into existing web pages.

DETAILS

Vulnerable systems:

- * XMB Forum version 1.8
- * XMB Forum version 1.9

Examples:

<http://path/to/XMBforum/member.php?action=viewpro&member=admin><script>alert(document.cookie)</script>

[http://path/to/XMBforum/buddy.php?action=<script>alert\(document.cookie\)</script>&buddy=<script](http://path/to/XMBforum/buddy.php?action=)

Securiteam: [UNIX] XSS Vulnerabilities Found in XMB Forum

>alert(document.cookie)</script>

Vendor status:

The vendor has been contacted. A fixed version is scheduled to be released.

ADDITIONAL INFORMATION

The information has been provided by <mailto:knight4vn@yahoo.com> thanh duong.

=====

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.