

[UNIX] bMachine Cross Site Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0084.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/24/03

To: list@securiteam.com

Date: 24 Dec 2003 14:59:00 +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>

bMachine Cross Site Scripting Vulnerability

SUMMARY

<<http://boastology.com/>> BoastMachine is "a one of its kind Blog/Journal/Article publishing system". The product suffers from a cross-site scripting vulnerability allowing remote attackers to insert malicious HTML and/or JavaScript into the web pages returned by the product.

DETAILS

Vulnerable systems:

* bMachine version 2.6

This Blog system, based in PHP, suffers from cross-site scripting vulnerability (CSS/XSS). This can be exploited by including arbitrary HTML or script code in the comment form, using field's name, and even the comment box. This will execute any of the malicious code when viewing the comments on that message.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:iamroot@systemsecure.org>>
David S. Ferreira.

Securiteam: [UNIX] bMachine Cross Site Scripting Vulnerability

=====

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.