

[NT] ASP-Dev Multiple Cross Site Scripting Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0002.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 04/03/05

To: list@securiteam.com

Date: 3 Apr 2005 13:55:02 +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>

ASP-Dev Multiple Cross Site Scripting Vulnerabilities

SUMMARY

<<http://asp-dev.com/>> ASP-Dev is "a web based forum written in ASP language".

The bbcode parsed by the forum code allows attackers to input JavaScript code into the forum. By exploiting this vulnerability attackers can steal information such as cookies from users.

DETAILS

Vulnerable Systems:

- * Asp-Dev FORUM version Rc3

When posting a message to the forum, an attacker can add Javascript code between bbcode instructions.

Proof of Concept:

[IMG]javasc+ript:alert(document.cookie)[/IMG]

ADDITIONAL INFORMATION

Securiteam: [NT] ASP-Dev Multiple Cross Site Scripting Vulnerabilities

The information has been provided by <mailto:zinho@hackerscenter.com>
Zinho.

=====

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.