

[UNIX] Auto Directory Index Cross-Site Scripting Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0053.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/16/03

To: list@securiteam.com

Date: 16 Nov 2003 17:40:37 +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>

Auto Directory Index Cross-Site Scripting Vulnerabilities

SUMMARY

<<http://autoindex.sourceforge.net/>> AutoIndex is "a project whose goal is to create a "Windows Explorer" that can be used to browse through folders on websites", a cross site scripting vulnerability in the product allows remote attackers to inject arbitrary HTML and or JavaScript into the web pages returned by the product.

DETAILS

Vulnerable systems:

* Auto Directory Index version 1.2.3 and prior

The vulnerability is caused due to missing validation of input supplied to the "dir" parameter. This can be exploited by including arbitrary HTML or script code in the parameter, which will cause it to be executed in a user's browser session when viewed.

Example:

`http://[victim]/index.php?dir=< script>alert(document.domain);</script>`

Securiteam: [UNIX] Auto Directory Index Cross-Site Scripting Vulnerabilities

ADDITIONAL INFORMATION

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

=====

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.