

[NT] ASPjar Guestbook login.asp SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0053.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/14/05

To: list@securiteam.com

Date: 14 Feb 2005 13:40:20 +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>

ASPjar Guestbook login.asp SQL Injection

SUMMARY

Due to a vulnerability in the way login.asp handles incoming requests, a remote attacker can cause the program to execute arbitrary SQL statements by supplying arbitrary values to the password parameter.

DETAILS

Vulnerable Systems:

* ASPjar Guestbook version 1.0

Exploit:

Supply in the password field ' or "=", this should allow you to bypass the authentication process used by ASPjar Guestbook.

Solution:

The product no longer exists, nor is the company that wrote it.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:farhadkey@yahoo.com>> farhad koosha.

Securiteam: [NT] ASPjar Guestbook login.asp SQL Injection

=====

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.