

JSPWiki Multiple Vulnerabilities

Vendor:

Janne Jalkanen JSPWiki – <http://www.jspwiki.org>

Application Description:

From JSPWiki website - "JSPWiki is a feature-rich and extensible WikiWiki engine built around a standard J2EE components (Java, servlets, JSP)."

Tested versions:

JSPWiki v2.4.104

JSPWiki v2.5.139

Earlier versions may also be affected.

JSPWiki Local .jsp File Inclusion Vulnerability

An input validation problem exists within JSPWiki which allows to execute (include) arbitrary local .jsp files. An attacker may leverage this issue to execute arbitrary server-side script code on a vulnerable server with the privileges of the web server process.

Example (including rss.jsp file from the application root directory):

<http://server/JSPWikiPath/Edit.jsp?page=Main&editor=../../rss>

Note: page parameter must be an existing page on the server.

This grants an attacker unauthorized access to sensitive .jsp files on the server and can lead to information disclosure.

Examples:

<http://server/JSPWikiPath/Edit.jsp?page=User&editor=../../Install>

<http://server/JSPWikiPath/Edit.jsp?page=User&editor=../../admin/SecurityConfig>

The first example disclose sensitive information such as the full path of the application on the server, page (and attachments) storage path, log files and work directory by including the application installation (Install.jsp).

The second example discloses the application security configurations by including the JSPWiki Security Configuration Verifier file (admin/SecurityConfig.jsp).

In addition, JSPWiki allow users to upload (attach) files to entry pages. An attacker can use the information disclosed by the installation file to upload a malicious .jsp file and locally execute it. By executing malicious server-side code, an attacker may be able to compromise the server.

January 15, 2008



Confidential

JSPWiki Cross-Site Scripting Vulnerability

An attacker may leverage cross-site scripting vulnerability to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. This may facilitate the theft of cookie-based authentication credentials as well as other attacks.

Example:

[http://server/JSPWikiPath/Edit.jsp?page=Main&editor=%3Cscript%3Ealert\(document.cookie\)%3C/script%3E](http://server/JSPWikiPath/Edit.jsp?page=Main&editor=%3Cscript%3Ealert(document.cookie)%3C/script%3E)

Credit:

Moshe B.A

BugSec LTD. - Security Consulting Company

<http://www.bugsec.com>



BugSec Ltd. Information Security | 11 Moshe Levi St. Rishon Le Zion 75070, Israel

Tel: +972-3-9622655 | Fax: +972-3-9511433 | Info@bugsec.com

Visit us at our Website: www.bugsec.com