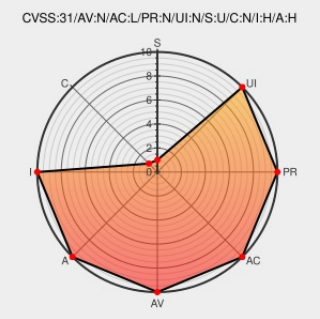
CVE-2021-44140

Published on: Not Yet Published

Last Modified on: 11/29/2021 02:42:00 PM UTC

CVE-2021-44140

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Jspwiki from Apache contain the following vulnerability:

Remote attackers may delete arbitrary files in a system hosting a JSPWiki instance, versions up to 2.11.0.M8, by using a carefuly crafted http request on logout, given that those files are reachable to the user running the JSPWiki instance. Apache JSPWiki users should upgrade to 2.11.0 or later.

CVE-2021-44140 has been assigned by security@apache.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache JSPWiki** version **<= 2.11.0.M8**

Vulnerability Patch/Work Around

Apache JSPWiki users should upgrade to 2.11.0 or later.

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	HIGH

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/5qglpjdhvobppx7j550lf1sk28f6011t
JSPWiki: CVE-2021-44140	jspwiki-wiki.apache.org text/html	MISC jspwiki-wiki.apache.org/Wiki.jsp?page=CVE-2021-44140

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

980003 Java (maven) Security Update for org.apache.jspwiki:jspwiki-main (GHSA-8gw6-w5rw-4g5c)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Jspwiki	All	All	All	All

cpe:2.3:a:apache:jspwiki:*:*:*:*:*:*:*:*:

Discovery Credit

Apache JSPWiki would like to thank haby0 (forhaby0@gmail.com) from Duxiaoman Financial Security Team for discovering and proposing the fix for this issue.

Social Mentions

Source	Title	Posted (UTC)
@oss_security	[CVE-2021-44140] Apache JSPWiki Arbitrary file deletion on logout: Posted by Juan Pablo Santos Rodríguez on Nov 23S… twitter.com/i/web/status/1…	2021-11-24 02:30:09
@mycbytes	jspwiki CVE-2021-44140 https://t.co/FPDho3zHY6	2021-11-24 08:59:56
@CVEreport	CVE-2021-44140 : Remote attackers may delete arbitrary files in a system hosting a JSPWiki instance, versions up to… twitter.com/i/web/status/1…	2021-11-24 11:19:46

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report