

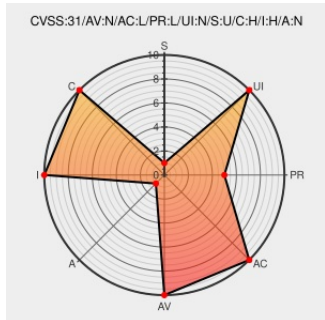


CVE-2023-26478

Published on: Not Yet Published

Last Modified on: 11/07/2023 04:09:00 AM UTC

CVE-2023-26478 - advisory for GHSA-8692-g6g9-gm5p

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Xwiki](#) from [Xwiki](#) contain the following vulnerability:

XWiki Platform is a generic wiki platform. Starting in version 14.3-rc-1,

``org.xwiki.store.script.TemporaryAttachmentsScriptService#uploadTemporaryAttachment`` returns an instance of ``com.xpn.xwiki.doc.XWikiAttachment``. This class is not supported to be exposed to users without the ``programing`` right. ``com.xpn.xwiki.api.Attachment`` should be used instead and takes care of checking the user's rights before performing dangerous operations. This has been patched in versions 14.9-rc-1 and 14.4.6. There are no known workarounds for this issue.

CVE-2023-26478 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Xwiki](#) - **xwiki-platform** version = **>= 14.3-rc-1, < 14.4.6**

Affected Vendor/Software: [Xwiki](#) - **xwiki-platform** version = **>= 14.5, < 14.9-rc-1**

CVSS3 Score: **8.1 - HIGH**

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

CVE References

Description	Tags	Link
XWIKI-20180: TemporaryAttachmentsScriptService#uploadTemporaryAttachm...	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/3c73c59e39b6436b1074d8834cf276916

· xwiki/xwiki-platform@3c73c59 · GitHub

Exposed Dangerous Method or Function in
org.xwiki.platform:xwiki-platform-store-filesystem-oldcore · Advisory · xwiki/xwiki-platform · GitHub

github.com
text/html

MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-8692-g6g9-gm5p

Loading...

jira.xwiki.org
text/html

MISC jira.xwiki.org/browse/XWIKI-20180

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xwiki	Xwiki	All	All	All	All
cpe:2.3:a:xwiki:xwiki:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-26478 : XWiki Platform is a generic wiki platform. Starting in version 14.3-rc-1, `org.xwiki.store... twitter.com/i/web/status/1...	2023-03-02 18:03:10
/r/netcve	CVE-2023-26478	2023-03-02 18:38:49
/r/AJsBotPlayground	[HIGH] CVE Report on March 10, 2023 12:14	2023-03-10 12:14:47
/r/AJsBotPlayground	[HIGH] CVE Report on March 10, 2023 11:59	2023-03-10 11:59:24

← Previous ID

Next ID→

© CVE.report 2024 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)