

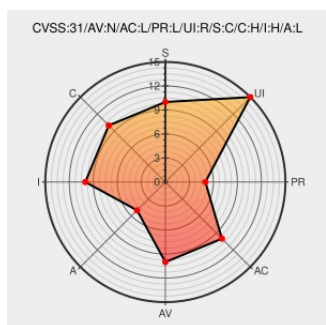


CVE-2022-36097

Published on: Not Yet Published

Last Modified on: 09/13/2022 07:40:00 PM UTC

CVE-2022-36097 - advisory for GHSA-9r9j-57rf-f6vj

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

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

XWiki Platform Attachment UI provides a macro to easily upload and select attachments for XWiki Platform, a generic wiki platform. Starting with version 14.0-rc-1 and prior to 14.4-rc-1, it's possible to store JavaScript in an attachment name, which will be executed by anyone trying to move the corresponding attachment. This issue has been patched in XWiki 14.4-rc-1. As a workaround, one may copy

`moveStep1.vm` to `webapp/xwiki/templates/moveStep1.vm` and replace vulnerable code with code from the patch.

CVE-2022-36097 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Xwiki](#) - **xwiki-platform** version **>= 14.0-rc-1, < 14.4-rc-1**

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
XWIKI-19667: The move attachment form is missing escaping and some tr... xwiki/xwiki-platform@fbc4bfb · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/fbc4bfb4e4f6ce8109addb281de86a03acdb9277
[XWIKI-19667] The move attachment form is missing escaping and some translations - XWiki.org JIRA	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19667

[raw.githubusercontent.com](#)[MISC raw.githubusercontent.com/xwiki/xwiki-platform/xwiki-](#)

[text/plain](#)[platform-14.0-rc-1/xwiki-platform-core/xwiki-platform-attachment/xwiki-platform-attachment-api/src/main/resources/templates/attachment/moveStep1.vm](#)[XSS in the move attachment form · Advisory · xwiki/xwiki-platform · GitHub](#)[github.com](#)[text/html](#)[CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-9r9j-57rf-f6vj](#)

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)
X @CVEreport	CVE-2022-36097 : XWiki Platform Attachment UI provides a macro to easily upload and select attachments for XWiki PI... twitter.com/i/web/status/1...	2022-09-08 20:38:04
r /r/netcve	CVE-2022-36097	2022-09-08 21:38:27

[← Previous ID](#)[Next ID →](#)

© [CVE.report](#) 2023 [X](#) [N](#) |

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](#)