

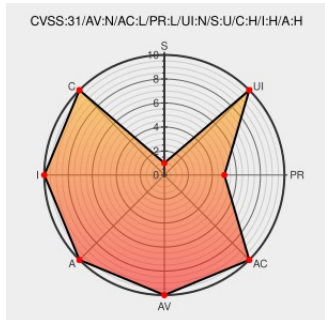


CVE-2023-29527

Published on: Not Yet Published

Last Modified on: 05/01/2023 05:27:00 PM UTC

CVE-2023-29527 - advisory for GHSA-jgrg-qvpp-9vwr

[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 offering runtime services for applications built on top of it. In affected versions a user without script or programming right may edit a user profile (or any other document) with the wiki editor and add groovy script content. Viewing the document after saving it will execute the groovy script in the server context which provides code execution. This vulnerability has been

patched in XWiki 15.0-rc-1 and 14.10.3. Users are advised to upgrade. There are no known workarounds for this issue.

CVE-2023-29527 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Xwiki](#) - **xwiki-platform** version = **>= 7.4.4, < 14.10.3**

CVSS3 Score: **8.8 - HIGH**

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

CVE References

Description	Tags	Link
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-20423
Privilege escalation (PR)/RCE from account through AWM view sheet · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-jgrg-qvpp-9vwr

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-2023-29527 : XWiki Platform is a generic wiki platform offering runtime services for applications built on top... twitter.com/i/web/status/1...	2023-04-19 00:13:24

[← 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