

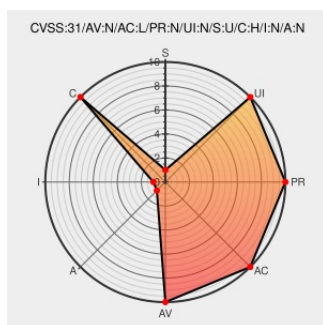


CVE-2023-26476

Published on: Not Yet Published

Last Modified on: 03/14/2023 04:53:00 PM UTC

CVE-2023-26476 - advisory for GHSA-5cf8-vrr8-8hjm

[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 3.2-m3, users can deduce the content of the password fields by repeated call to `LiveTableResults` and `WikisLiveTableResultsMacros`. The issue can be fixed by upgrading to versions 14.7-rc-1, 13.4.4, or 13.10.9 and higher, or in version $\geq 3.2M3$ by applying the patch manually on `LiveTableResults` and `WikisLiveTableResultsMacros`.

CVE-2023-26476 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Xwiki](#) - **xwiki-platform** version = $\geq 3.2-m3$, $< 13.4.4$

Affected Vendor/Software: [Xwiki](#) - **xwiki-platform** version = $\geq 13.5.0$, $< 13.10.9$

Affected Vendor/Software: [Xwiki](#) - **xwiki-platform** version = $\geq 14.0.0$, $< 14.7-rc-1$

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
XWIKI-19949: Livetable results allow reconstructing password hashes u... · xwiki/xwiki-platform@7f88255 · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/7f8825537c9523ccb5051abd78014d156f9791c8
Exposure of Sensitive Information to an Unauthorized Actor in org.xwiki.platform:xwiki-platform-livetable-ui,org.xwiki.platform:xwiki-platform-wiki-ui-mainwiki · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-5cf8-vrr8-8hjm

Loading...

jira.xwiki.org
text/html

◆ MISC jira.xwiki.org/browse/XWIKI-19949

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
Application	Xwiki	Xwiki	14.7	rc1	All	All
Application	Xwiki	Xwiki	3.2	milestone3	All	All
cpe:2.3:a:xwiki:xwiki:*****:						
cpe:2.3:a:xwiki:xwiki:14.7:rc1:*****:						
cpe:2.3:a:xwiki:xwiki:3.2:milestone3:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-26476 : XWiki Platform is a generic wiki platform. Starting in version 3.2-m3, users can deduce the conten... twitter.com/i/web/status/1...	2023-03-02 19:08:30
 /r/netcve	CVE-2023-26476	2023-03-02 19:38:37

← Previous ID

Next ID →

© CVE.report 2023   |

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](#)