



# CVE-2022-41933

Published on: Not Yet Published

Last Modified on: 12/02/2022 04:57:00 PM UTC

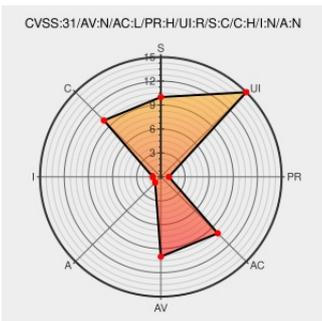
## CVE-2022-41933 - advisory for GHSA-q2hm-2h45-v5g3

[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. When the `reset a forgotten password` feature of XWiki was used, the password was then stored in plain text in database. This only concerns XWiki 13.1RC1 and newer versions. Note that it only concerns the reset password feature available from the "Forgot your password" link in the login view: the features allowing a

user to change their password, or for an admin to change a user password are not impacted. This vulnerability is particularly dangerous in combination with other vulnerabilities allowing to perform data leak of personal data from users, such as GHSA-599v-w48h-rjrm. Note that this vulnerability only concerns the users of the main wiki: in case of farms, the users registered on subwiki are not impacted thanks to a bug we discovered when investigating this. The problem has been patched in version 14.6RC1, 14.4.3 and 13.10.8. The patch involves a migration of the impacted users as well as the history of the page, to ensure no password remains in plain text in the database. This migration also involves to inform the users about the possible disclosure of their passwords: by default, two emails are automatically sent to the impacted users. A first email to inform about the possibility that their password have been leaked, and a second email using the reset password feature to ask them to set a new password. It's also possible for administrators to set some properties for the migration: it's possible to decide if the user password should be reset (default) or if the passwords should be kept but only hashed. Note that in the first option, the users won't be able to login anymore until they set a new password if they were impacted. Note that in both options, mails will be sent to users to inform them and encourage them to change their passwords.

CVE-2022-41933 has been assigned by [security-advisories@github.com](mailto:security-advisories@github.com) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [xwiki](#) - [xwiki-platform](#) version  $\geq 13.1RC1$ ,  $< 13.10.8$

Affected Vendor/Software: [xwiki](#) - [xwiki-platform](#) version  $\geq 14.0.0$ ,  $< 14.4.3$

CVSS3 Score: **6.5 - MEDIUM**

<b>Attack Vector</b>	<b>Attack Complexity</b>	<b>Privileges Required</b>	<b>User Interaction</b>
NETWORK	LOW	NONE	REQUIRED
<b>Scope</b>	<b>Confidentiality Impact</b>	<b>Integrity Impact</b>	<b>Availability Impact</b>
UNCHANGED	HIGH	NONE	NONE

## CVE References

Description	Tags	Link
Loading...	<a href="#">jira.xwiki.org</a> <a href="#">text/html</a>	MISC <a href="#">jira.xwiki.org/browse/XWIKI-19945</a>
Plaintext storage of password after a reset in org.xwiki.platform:xwiki-platform-security-authentication-default · Advisory · xwiki/xwiki-platform · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	CONFIRM <a href="#">github.com/xwiki/xwiki-platform/security/advisories/GHSA-q2hm-2h45-v5g3</a>
Loading...	<a href="#">jira.xwiki.org</a> <a href="#">text/html</a>	MISC <a href="#">jira.xwiki.org/browse/XWIKI-19869</a>
XWIKI-19869: Improve user property storage · xwiki/xwiki-platform@443e839 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="#">github.com/xwiki/xwiki-platform/commit/443e8398b75a1295067d74afb5898370782d863a#diff-f8a8f8ba80dfc55f044e2e60b521ce379176430ca6921b0f87b79cf682531f79L322</a>
Missing Authorization and Exposure of Private Personal Information to an Unauthorized Actor in org.xwiki.platform:xwiki-platform-web-templates · Advisory · xwiki/xwiki-platform · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="#">github.com/xwiki/xwiki-platform/security/advisories/GHSA-599v-w48h-rjrm</a>

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](mailto: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	13.1	rc1	All	All
cpe:2.3:a:xwiki:xwiki:*.***:*.***:*.***:*.***:*						
cpe:2.3:a:xwiki:xwiki:13.1:rc1:*.***:*.***:*						

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	<a href="#">CVE-2022-41933</a>	2022-11-23 21:38:12

[← Previous ID](#) [Next ID→](#)

© [CVE.report](#) 2022   |

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](#)**