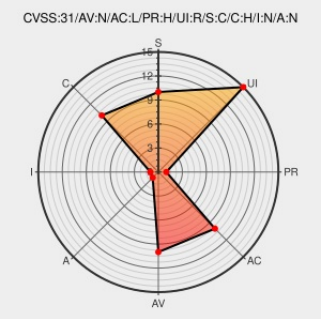
CVE-2022-41933

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 to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 13.1RC1, < 13.10.8**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 14.0.0, < 14.4.3**

CVSS3 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19945
Plaintext storage of password after a reset in org.xwiki.platform:xwiki-platform-security-authentication-default · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-q2hm-2h45-v5g3
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19869
XWIKI-19869: Improve user property storage · xwiki/xwiki-platform@443e839 · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/443e8398b75a1295067d74afb5898370782d863a#diff-f8a8f8ba80dfc55f044e2e60b521ce379176430ca6921b0f87b79cf682531f79L322
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	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-599v-w48h-rjrm

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	CVE-2022-41933	2022-11-23 21:38:12

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report