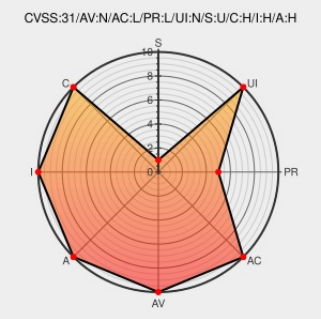
CVE-2023-29210

Published on: Not Yet Published

Last Modified on: 04/24/2023 06:31:00 PM UTC

CVE-2023-29210 - advisory for GHSA-p9mj-v5mf-m82x

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xwiki from Xwiki contain the following vulnerability:

XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights on commonly accessible documents including the notification preferences macros can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the user parameter of the macro that provide the notification filters. These macros are used in the user profiles and thus installed by default in XWiki. The vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10.

CVE-2023-29210 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 13.2-rc-1, < 13.10.11**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 14.0-rc-1, < 14.4.7**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 14.5, < 14.10**

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
Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in org.xwiki.platform:xwiki-platform-notifications-ui · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-p9mj-v5mf-m82x

XWIKI-20259: Improve escaping in Notification Preferences Macros · xwiki/xwiki-platform@cebf916 · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/cebf9167e4fd64a8777781fc56461e9abbe0b32a
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-20259

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	14.10	rc1	All	All

cpe:2.3:a:xwiki:xwiki:*:*:*:*:*:*:*:*:

cpe:2.3:a:xwiki:xwiki:14.10:rc1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→