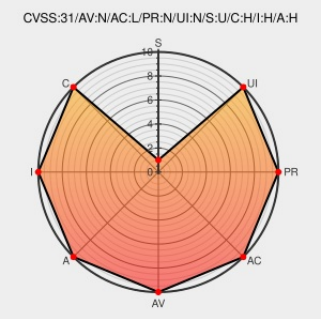
CVE-2023-26477

Published on: Not Yet Published

Last Modified on: 11/07/2023 04:09:00 AM UTC

CVE-2023-26477 - advisory for GHSA-x2qm-r4wx-8gpg

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 versions 6.3-rc-1 and 6.2.4, it's possible to inject arbitrary wiki syntax including Groovy, Python and Velocity script macros via the `newThemeName` request parameter (URL parameter), in combination with additional parameters. This has been patched in the supported versions 13.10.10, 14.9-rc-1, and 14.4.6. As a workaround, it is possible to edit `FlamingoThemesCode.WebHomeSheet` and manually perform the changes from the patch fixing the issue.

CVE-2023-26477 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 6.2.4, < 13.10.10**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 14.0, < 14.4.6**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 14.5, < 14.9-rc-1**

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
XWIKI-19757: Improved translation macro parameters escaping in Flamin… · xwiki/xwiki-platform@ea2e615 · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/ea2e615f50a918802fd60b09ec87aa04bc6ea8e2#diff-e2153fa59f9d92ef67b0afbf27984bd17170921a3b558fac227160003d0dfd2aR283-R284

Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in org.xwiki.platform:xwiki-platform-flamingo-theme-ui · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-x2qm-r4wx-8gpg
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19757

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-2023-26477 : XWiki Platform is a generic wiki platform. Starting in versions 6.3-rc-1 and 6.2.4, it's possible… twitter.com/i/web/status/1…	2023-03-02 18:02:42
/r/netcve	CVE-2023-26477	2023-03-02 18:38:48
/r/AJsBotPlayground	[CRITICAL] CVE Report on March 10, 2023 12:14	2023-03-10 12:14:48
/r/AJsBotPlayground	[CRITICAL] CVE Report on March 10, 2023 11:59	2023-03-10 11:59:25

← Previous ID

Next ID→