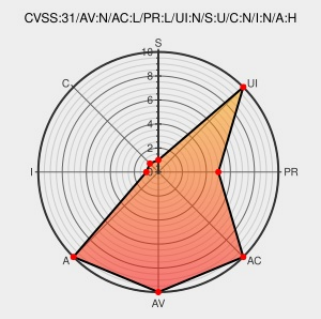
CVE-2023-26479

Published on: Not Yet Published

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

CVE-2023-26479 - advisory for GHSA-52vf-hvv3-98h7

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 6.0, users with write rights can insert well-formed content that is not handled well by the parser. As a consequence, some pages becomes unusable, including the user index (if the page containing the faulty content is a user page) and the page index. Note that on the page, the normal UI is completely missing and it is not possible to open the editor directly to revert the change as the stack overflow is already triggered while getting the title of the document. This means that it is quite difficult to remove this content once inserted. This has been patched in XWiki 13.10.10, 14.4.6, and 14.9-rc-1. A temporary workaround to avoid Stack Overflow errors is to increase the memory allocated to the stack by using the `-Xss` JVM parameter (e.g., `-Xss32m`). This should allow the parser to pass and to fix the faulty content. The consequences for other aspects of the system (e.g., performance) are unknown, and this workaround should be only be used as a temporary solution. The workaround does not prevent the issue occurring again with other content. Consequently, it is strongly advised to upgrade to a version where the issue has been patched.

CVE-2023-26479 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 6.0, < 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: 6.5 - MEDIUM

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

UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19838
Improper Handling of Exceptional Conditions in org.xwiki.platform:xwiki-platform-rendering-parser · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-52vf-hvv3-98h7
XWIKI-19838: Improve handling of unexpected parser errors · xwiki/xwiki-platform@e5b82cd · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/e5b82cd98072464196a468b8f7fe6396dce142a7

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-2023-26479 : XWiki Platform is a generic wiki platform. Starting in version 6.0, users with write rights can in… twitter.com/i/web/status/1…	2023-03-02 18:03:24
/r/netcve	CVE-2023-26479	2023-03-02 18:38:50
/r/AJsBotPlayground	[MEDIUM] CVE Report on March 10, 2023 12:14 [1/3]	2023-03-10 12:14:44
/r/AJsBotPlayground	[MEDIUM] CVE Report on March 10, 2023 11:59 [1/3]	2023-03-10 11:59:21

← Previous ID

Next ID→

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