



CVE-2022-36099

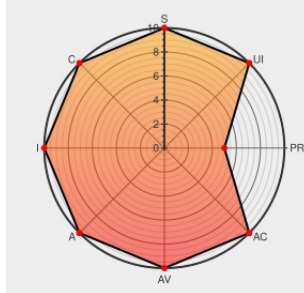
Published on: Not Yet Published

Last Modified on: 06/27/2023 08:52:00 PM UTC

CVE-2022-36099 - advisory for GHSA-xr6m-2p4m-jvqf

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H



Certain versions of [Xwiki](#) from [Xwiki](#) contain the following vulnerability:

XWiki Platform Wiki UI Main Wiki is software for managing subwikis on XWiki Platform, a generic wiki platform. Starting with version 5.3-milestone-2 and prior to versions 13.10.6 and 14.4, it's possible to inject arbitrary wiki syntax including Groovy, Python and Velocity script macros via the request (URL parameter) using the

`XWikiServerClassSheet` if the user has view access to this sheet and

another page that has been saved with programming rights, a standard condition on a public read-only XWiki installation or a private XWiki installation where the user has an account. This allows arbitrary Groovy/Python/Velocity code execution which allows bypassing all rights checks and thus both modification and disclosure of all content stored in the XWiki installation. Also, this could be used to impact the availability of the wiki. This has been patched in versions 13.10.6 and 14.4. As a workaround, edit the affected document `XWiki.XWikiServerClassSheet` or `WikiManager.XWikiServerClassSheet` and manually perform the changes from the patch fixing the issue. On XWiki versions 12.0 and later, it is also possible to import the document `XWiki.XWikiServerClassSheet` from the xwiki-platform-wiki-ui-mainwiki package version 14.4 using the import feature of the administration application as there have been no other changes to this document since XWiki 12.0.

CVE-2022-36099 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [xwiki](#) - **xwiki-platform** version **>= 5.3-milestone-2, < 13.10.6**

Affected Vendor/Software: [xwiki](#) - **xwiki-platform** version **>= 14.0, < 14.4**

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
[XWIKI-19746] Privilege escalation (PR) with view rights on XWiki.XWikiServerClassSheet - XWiki.org JIRA	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19746
Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in xwiki-platform-wiki-ui-mainwiki · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-xr6m-2p4m-jvqf
XWIKI-19746: Escape parameters for translation macro in XWikiServerCl... · xwiki/xwiki-platform@fc77f9f · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/fc77f9f53bc65a4a9bfae3d5686615309c0c76cc

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	5.3	milestone2	All	All

cpe:2.3:a:xwiki:xwiki:*.*:~::~

cpe:2.3:a:xwiki:xwiki:5.3:~::~

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-36099 : XWiki Platform Wiki UI Main Wiki is software for managing subwikis on XWiki Platform, a generic wi... twitter.com/i/web/status/1...	2022-09-08 20:46:03
/r/netcve	CVE-2022-36099	2022-09-08 21:38:28

← Previous ID

Next ID →

[site](#). This site includes MITRE data granted under the following [license](#).

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