



CVE-2023-26472

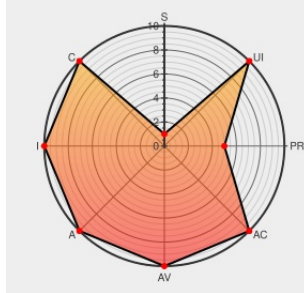
Published on: Not Yet Published

Last Modified on: 03/13/2023 05:23:00 PM UTC

CVE-2023-26472 - advisory for GHSA-vwr6-qp4q-2wj7

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

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



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

XWiki Platform is a generic wiki platform. Starting in version 6.2-milestone-1, one can execute any wiki content with the right of IconThemeSheet author by creating an icon theme with certain content. This can be done by creating a new page or even through the user profile for users not having edit right. The issue has been patched in XWiki 14.9, 14.4.6, and 13.10.10. An available workaround is to fix the bug in the page `IconThemesCode.IconThemeSheet` by applying a modification from commit 48caf7491595238af2b531026a614221d5d61f38.

CVE-2023-26472 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Xwiki](#) - [xwiki-platform](#) version = **>= 6.2-milestone-1, < 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**

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
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19731
Privilege escalation (PR) via async macro and IconThemeSheet from the	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-vwr6-qp4q-2wj7

XWIKI-19731: Fix escaping ·
xwiki/xwiki-platform@48caf74 · GitHub

[github.com](#)
[text/html](#)

 MISC [github.com/xwiki/xwiki-
platform/commit/48caf7491595238af2b531026a614221d5d61f38#diff-
2ec9d716673ee049937219cdb0a92e520f81da14ea84d144504b97ab2bdae243R45](https://github.com/xwiki/xwiki-platform/commit/48caf7491595238af2b531026a614221d5d61f38#diff-2ec9d716673ee049937219cdb0a92e520f81da14ea84d144504b97ab2bdae243R45)

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	6.2	milestone1	All	All
Application	Xwiki	Xwiki	6.2	milestone2	All	All
cpe:2.3:a:xwiki:xwiki:*****:						
cpe:2.3:a:xwiki:xwiki:6.2:milestone1:*****:						
cpe:2.3:a:xwiki:xwiki:6.2:milestone2:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-26472 : XWiki Platform is a generic wiki platform. Starting in version 6.2-milestone-1, one can execute an... twitter.com/i/web/status/1...	2023-03-02 19:06:49
 /r/netcve	CVE-2023-26472	2023-03-02 19:38:34

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2024   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)