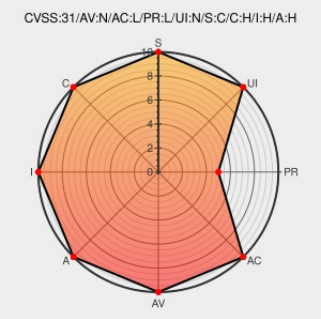
CVE-2022-41931

Published on: Not Yet Published

Last Modified on: 11/30/2022 05:00:00 PM UTC

CVE-2022-41931 - advisory for GHSA-5j7g-cf6r-g2h7

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



Certain versions of Xwiki from Xwiki contain the following vulnerability:

xwiki-platform-icon-ui is vulnerable to Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection'). Any user with view rights on commonly accessible documents including the icon picker macro can execute arbitrary Groovy, Python or Velocity code in XWiki due to improper neutralization of the macro parameters of the icon picker macro. The problem has been patched in XWiki 13.10.7, 14.5 and 14.4.2. Workarounds: The [patch](https://github.com/xwiki/xwiki-platform/commit/47eb8a5fba550f477944eb6da8ca91b87eaf1d01) can be manually applied by editing `IconThemesCode.IconPickerMacro` in the object editor. The whole document can also be replaced by the current version by importing the document from the XAR archive of a fixed version as the only changes to the document have been security fixes and small formatting changes.

CVE-2022-41931 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 6.4-milestone-2, < 13.10.7**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 14.0.0, < 14.4.2**

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-19805: Improve parameter escaping in	github.com	MISC github.com/xwiki/xwiki-

IconPickerMacro · xwiki/xwiki-platform@47eb8a5 · GitHub	text/html	platform/commit/47eb8a5fba550f477944eb6da8ca91b87eaf1d01
Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in xwiki-platform-icon-ui · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-5j7g-cf6r-g2h7
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19805

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	14.4.3	All	All	All
Application	Xwiki	Xwiki	14.4.4	All	All	All
Application	Xwiki	Xwiki	6.4	milestone2	All	All
Application	Xwiki	Xwiki	6.4	milestone3	All	All

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

cpe:2.3:a:xwiki:xwiki:14.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:xwiki:xwiki:14.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:xwiki:xwiki:6.4:milestone2:*:*:*:*:*:*:

cpe:2.3:a:xwiki:xwiki:6.4:milestone3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-41931	2022-11-23 20:38:41

← Previous ID

Next ID→

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