CVE-2022-41927

Published on: Not Yet Published

Last Modified on: 11/30/2022 04:22:00 PM UTC
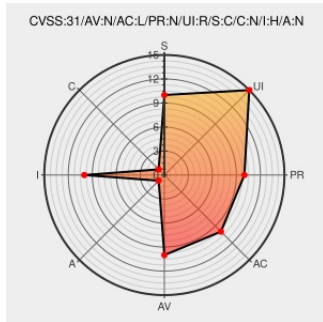
CVE-2022-41927 - advisory for GHSA-mq7h-5574-hw9f

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

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

Certain versions of Xwiki from Xwiki contain the following vulnerability:

XWiki Platform is vulnerable to Cross-Site Request Forgery (CSRF) that may allow attackers to delete or rename tags without needing any confirmation. The problem has been patched in XWiki 13.10.7, 14.4.1 and 14.5RC1. Workarounds: It's possible to patch existing instances directly by editing the page Main.Tags and add this kind of check, in the code for renaming and for deleting: ``` #if (!$services.csrf.isTokenValid($request.get('form_token'))) #set ($discard = $response.sendError(401, "Wrong CSRF token")) #end ```

CVE-2022-41927 has been assigned by 🐙 security-advisories@github.com to track the vulnerability - currently rated as `HIGH` severity.

Affected Vendor/Software: 🐙 **xwiki** - **xwiki-platform** version >= 3.2-milestone-2, < 13.10.7

Affected Vendor/Software: 🐙 **xwiki** - **xwiki-platform** version >= 14.0.0, < 14.4.1

CVSS3 Score: `7.4 - HIGH`

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

CVE References

Description	Tags	Link
XWIKI-19748: Wrong error code in tags · xwiki/xwiki-platform@7fd4cda · GitHub	`github.com` `text/html`	🐙 MISC github.com/xwiki/xwiki-platform/commit/7fd4cda0590180c4d34f557597e9e10e263def9e
Cross-Site Request Forgery (CSRF) allowing to delete or rename tags · Advisory · xwiki/xwiki-platform · GitHub	`github.com` `text/html`	🐙 CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-mq7h-5574-hw9f

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

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	All	All	All
Application	Xwiki	Xwiki	3.2	milestone2	All	All
Application	Xwiki	Xwiki	3.2	milestone3	All	All

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

cpe:2.3:a:xwiki:xwiki:14.4:*:*:*:*:*:*:*:

cpe:2.3:a:xwiki:xwiki:3.2:milestone2:*:*:*:*:*:*:

cpe:2.3:a:xwiki:xwiki:3.2:milestone3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-41927	2022-11-23 19:38:14

← Previous ID   Next ID→

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