



CVE-2022-41930

Published on: Not Yet Published

Last Modified on: 11/30/2022 04:50:00 PM UTC

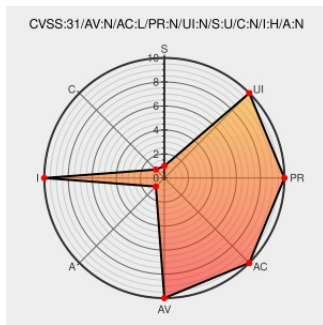
CVE-2022-41930 - advisory for GHSA-p5v9-g8w8-5q4v

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

org.xwiki.platform:xwiki-platform-user-profile-ui is missing authorization to enable or disable users. Any user (logged in or not) with access to the page XWiki.XWikiUserProfileSheet can enable or disable any user profile. This might allow to a disabled user to re-enable themselves, or to an attacker to disable any user of the wiki. The problem has been patched in XWiki 13.10.7, 14.5RC1 and 14.4.2. Workarounds: The

problem can be patched immediately by editing the page `XWiki.XWikiUserProfileSheet` in the wiki and by performing the changes contained in <https://github.com/xwiki/xwiki-platform/commit/5be1cc0adf917bf10899c47723fa451e950271fa>.

CVE-2022-41930 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 12.4, < 13.10.7**

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

CVSS3 Score: **8.2 - HIGH**

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

CVE References

Description	Tags	Link
Missing Authorization to enable or disable users in org.xwiki.platform:xwiki-platform-user-profile-ui · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-p5v9-g8w8-5q4v
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19792

XWIKI-19792: User should not be able to disable themselves · xwiki/xwiki-platform@5be1cc0 · GitHub

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

MISC [github.com/xwiki/xwiki-platform/commit/5be1cc0adf917bf10899c47723fa451e950271fa](#)

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


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

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2022-41930	2022-11-23 20:38:41

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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](#)