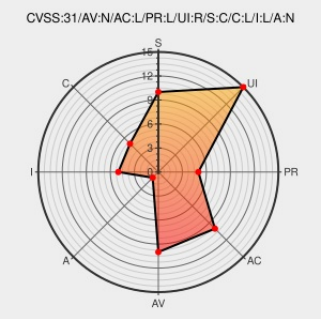
CVE-2023-29515

Published on: Not Yet Published

Last Modified on: 04/28/2023 05:23:00 PM UTC

CVE-2023-29515 - advisory for GHSA-44h9-xxvx-pg6x

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



Certain versions of Xwiki from Xwiki contain the following vulnerability:

XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user who can create a space can become admin of that space through App Within Minutes. The admin right implies the script right and thus allows JavaScript injection. The vulnerability can be exploited by creating an app in App Within Minutes. If the button should be disabled because the user doesn't have global edit right, the app can also be created by directly opening `/xwiki/bin/view/AppWithinMinutes/CreateApplication?wizard=true` on the XWiki installation. This has been patched in XWiki 13.10.11, 14.4.8, 14.10.1 and 15.0 RC1 by not granting the space admin right if the user doesn't have script right on the space where the app is created. Error message are displayed to warn the user that the app will be broken in this case. Users who became space admin through this vulnerability won't loose the space admin right due to the fix, so it is advised to check if all users who created AWM apps should keep their space admin rights. Users are advised to upgrade. There are no known workarounds for this vulnerability.

CVE-2023-29515 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= < 13.10.11**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 14.0.0, < 14.4.8**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 14.5.0, < 14.10.1**

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**

CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
Creating an App Within Minutes app grants space admin rights and thus allows cross-site scripting (XSS) · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-44h9-xxvx-pg6x
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-20190
XWIKI-20190: Properly handle AWM creation without script right · xwiki/xwiki-platform@e73b890 · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/e73b890623efa604adc484ad82f37e31596fe1a6

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-29515 : XWiki Platform is a generic wiki platform offering runtime services for applications built on top… twitter.com/i/web/status/1…	2023-04-19 00:09:35

← 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 registred 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