

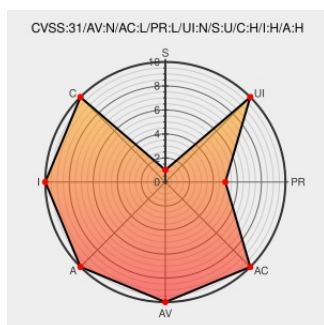


CVE-2023-29511

Published on: Not Yet Published

Last Modified on: 04/26/2023 07:43:00 PM UTC

CVE-2023-29511 - advisory for GHSA-rfh6-mg6h-h668

[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 with edit rights on a page (e.g., it's own user page), can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the section ids in

`XWiki.AdminFieldsDisplaySheet`. This page is installed by default.

The vulnerability has been patched in XWiki versions 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11.

CVE-2023-29511 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Xwiki](#) - **xwiki-platform** version = **>= 14.0-rc-1, < 14.4.8**

Affected Vendor/Software: [Xwiki](#) - **xwiki-platform** version = **>= 14.5, < 14.10.1**

Affected Vendor/Software: [Xwiki](#) - **xwiki-platform** version = **>= 15M2, < 13.10.11**

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
Privilege escalation (PR) from account/view through AdminFieldsDisplaySheet and admin.vm · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-rfh6-mg6h-h668
Loading...	jira.xwiki.org	MISC jira.xwiki.org/browse/XWIKI-20261

[text/html](#)

XWIKI-20261: Improved escaping of
AdminFieldsDisplaySheet · xwiki/xwiki-platform@f1e3108
· GitHub

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

MISC [github.com/xwiki/xwiki-platform/commit/f1e310826a19acdcdecdecdcfe171d21f24d6ede](#)

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	14.0	-	All	All
Application	Xwiki	Xwiki	14.0	rc1	All	All
cpe:2.3:a:xwiki:xwiki:*****:						
cpe:2.3:a:xwiki:xwiki:14.0:-:*****:						
cpe:2.3:a:xwiki:xwiki:14.0:rc1:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)[Next ID →](#)

© CVE.report 2023   |

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](#)