

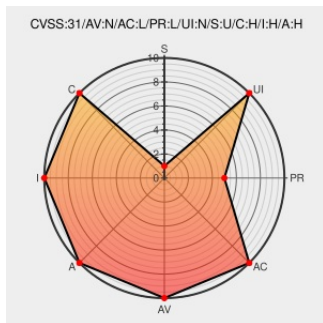


CVE-2023-35166

Published on: Not Yet Published

Last Modified on: 06/28/2023 02:01:00 AM UTC

CVE-2023-35166 - advisory for GHSA-h7cw-44vp-jq7h

[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. It's possible to execute any wiki content with the right of the TipsPanel author by creating a tip UI extension. This has been patched in XWiki 15.1-rc-1 and 14.10.5.

CVE-2023-35166 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Xwiki](#) - [xwiki-platform](#) version = **>= 8.1-milestone-1**, **< 14.10.5**

Affected Vendor/Software: [Xwiki](#) - [xwiki-platform](#) version = **>= 15.0-rc-1**, **< 15.1-rc-1**

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
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-20281
Privilege escalation (PR) from account through TipsPanel · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-h7cw-44vp-jq7h
XWIKI-20281: Improve tips rendering · xwiki/xwiki-platform@98208c5 · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/98208c5bb1e8cdf3ff1ac35d8b3d1cb3c28b3263#diff-4e3467d2ef3871a68b2f910e67cf84531751b32e0126321be83c0f1ed5d90b29L176-R178

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-2023-35166 : XWiki Platform is a generic wiki platform offering runtime services for applications built on top... twitter.com/i/web/status/1...	2023-06-20 20:02:33
 @cracbot	CVE-2023-35166 (CVSS:9.9, CRITICAL) is Received. XWiki Platform is a generic wiki platform offering runtime service... twitter.com/i/web/status/1...	2023-06-21 06:00:18
 @samilaiho	XWiki privilege escalation URL: Classification: Critical, Solution: Official Fix, Exploit M... twitter.com/i/web/status/1...	2023-06-21 06:10:41

[← 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](#)