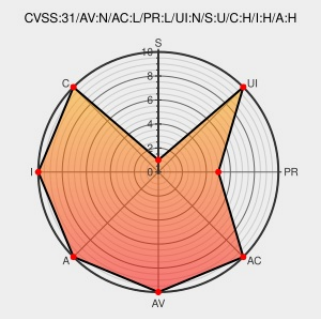
CVE-2023-35152

Published on: Not Yet Published

Last Modified on: 06/30/2023 07:12:00 AM UTC

CVE-2023-35152 - advisory for GHSA-rf8j-q39g-7xfm

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. Starting in version 12.9-rc-1 and prior to versions 14.4.8, 14.10.6, and 15.1, any logged in user can add dangerous content in their first name field and see it executed with programming rights. Leading to rights escalation. The vulnerability has been fixed on XWiki 14.4.8, 14.10.6, and 15.1. As a workaround, one may apply the patch manually.

CVE-2023-35152 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 12.9-rc-1, < 14.4.8**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 14.5, < 14.10.6**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **= >= 15.0-rc-1, < 15.1**

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
XWIKI-19900: Liked page whose FULLNAME contains dot(.) can not show i… · xwiki/xwiki-platform@6ce2d04 · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/6ce2d04a5779e07f6d3ed3f37d4761049b4fc3ac#diff-ef7f8b911bb8e584fda22aac5876a329add35ca0d1d32e0fdb62a439b78cfa49
Privilege escalation (PR) from account through like LiveTableResults · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/security/advisories/GHSA-rf8j-q39g-7xfm

Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19900
XWIKI-17733: Use a LiveTable to display the page liked in user profile · xwiki/xwiki-platform@0993a7a · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/0993a7ab3c102f9ac37ffe361a83a3dc302c0e45#diff-0b51114cb27f7a5c599cf40c59d658eae6ddc5c0836532c3b35e163f40a4854fR39
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-20611

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	12.9	rc1	All	All
Application	Xwiki	Xwiki	15.0	All	All	All
Application	Xwiki	Xwiki	15.0	rc1	All	All

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

cpe:2.3:a:xwiki:xwiki:12.9:rc1:*:*:*:*:*:*:

cpe:2.3:a:xwiki:xwiki:15.0:*:*:*:*:*:*:*:

cpe:2.3:a:xwiki:xwiki:15.0:rc1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-35152 : XWiki Platform is a generic wiki platform. Starting in version 12.9-rc-1 and prior to versions 14.... twitter.com/i/web/status/1…	2023-06-23 17:07:18
@cracbot	CVE-2023-35152 (CVSS:9.9, CRITICAL) is Awaiting Analysis. XWiki Platform is a generic wiki platform. Starting in ve… twitter.com/i/web/status/1…	2023-06-24 06:00:16
@samilaiho	Multiple vulnerabilities in XWiki Platform URL: Classification: Critical, Solution: Officia… twitter.com/i/web/status/1…	2023-06-24 06:00:20

← Previous ID

Next ID→

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