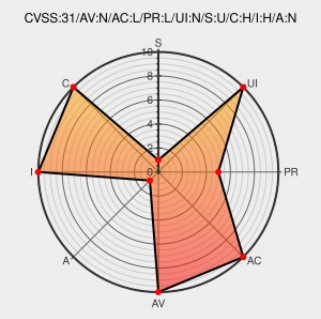
CVE-2022-31166

Published on: Not Yet Published

Last Modified on: 09/13/2022 10:43:00 PM UTC

CVE-2022-31166 - advisory for GHSA-g4h6-qp44-wqvx

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



Certain versions of Xwiki from Xwiki contain the following vulnerability:

XWiki Platform Old Core is a core package for XWiki Platform, a generic wiki platform. Starting in versions 11.3.7, 11.0.3, and 12.0RC1, it is possible to exploit a bug in XWikiRights resolution of groups to obtain privilege escalation. More specifically, editing a right with the object editor leads to adding a supplementary empty value to groups which is then resolved as a reference to XWiki.WebHome page. Adding an XWikiGroup xobject to that page then transforms it to a group, any user put in that group would then obtain the privileges related to the edited right. Note that this security issue is normally mitigated by the fact that XWiki.WebHome (and XWiki space in general) should be protected by default for edit rights. The problem has been patched in XWiki 13.10.4 and 14.2RC1 to not consider anymore empty values in XWikiRights. It's possible to work around the problem by setting appropriate rights on XWiki.WebHome page to prevent users to edit it.

CVE-2022-31166 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 11.3.7, < 13.10.4**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 14.0-rc-1, < 14.2-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
Log in - XWiki.org JIRA	jira.xwiki.org	MISC jira.xwiki.org/browse/XWIKI-18386

	text/html	
[XWIKI-15776] The groups displayer store values with a coma at the end - XWiki.org JIRA	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-15776
Improper Privilege Management in XWiki resolving groups in XWiki.WebHome · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-g4h6-qp44-wqvx
XWIKI-15776: The groups displayer store values with a coma at the end by surli · Pull Request #1800 · xwiki/xwiki-platform · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/pull/1800

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2022-31166: exploitation with Powershell, Python, Ruby, NMAP and Metasploit.

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-2022-31166 : XWiki Platform Old Core is a core package for XWiki Platform, a generic wiki platform. Starting in… twitter.com/i/web/status/1…	2022-09-07 14:13:05
@LinInfoSec	Xwiki - CVE-2022-31166: github.com/xwiki/xwiki-pl…	2022-09-07 17:01:35
/r/netcve	CVE-2022-31166	2022-09-07 15:38:44

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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