



CVE-2022-31166

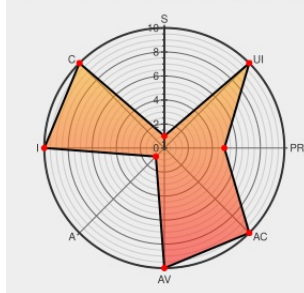
Published on: Not Yet Published

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](#)

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N



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](#)

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

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)
X @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
X @LinInfoSec	Xwiki - CVE-2022-31166: github.com/xwiki/xwiki-pl...	2022-09-07 17:01:35
r /r/netcve	CVE-2022-31166	2022-09-07 15:38:44

[← Previous ID](#)[Next ID →](#)

© CVE.report 2023 [X](#) [N](#) |

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