



# CVE-2022-41928

Published on: Not Yet Published

Last Modified on: 11/30/2022 04:38:00 PM UTC

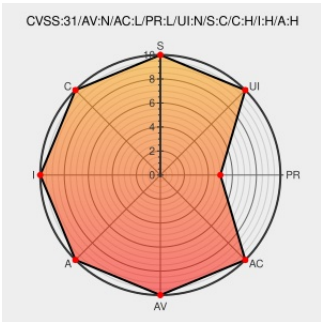
## CVE-2022-41928 - advisory for GHSA-9hqh-fmhg-vq2j

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of **Xwiki** from **Xwiki** contain the following vulnerability: XWiki Platform vulnerable to Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in AttachmentSelector.xml. The issue can also be reproduced by inserting the dangerous payload in the `height` or `alt` macro properties. This has been patched in versions 13.10.7, 14.4.2, and 14.5. The issue can be fixed on a running wiki by updating `XWiki.AttachmentSelector` with

the versions below: - 14.5-rc-1+: <https://github.com/xwiki/xwiki-platform/commit/eb15147adf94bddb92626f862c1710d45bcd64a7#diff-e1513599ab698991f6cbba55d38f3f464432ced8d137a668b1f7618c7e747e23> - 14.4.2+: <https://github.com/xwiki/xwiki-platform/commit/c02f8eb1f3c953d124f2c097021536f8bc00fa8d#diff-e1513599ab698991f6cbba55d38f3f464432ced8d137a668b1f7618c7e747e23> - 13.10.7+: <https://github.com/xwiki/xwiki-platform/commit/efd0df0468d46149ba68b66660b93f31b6318515#diff-e1513599ab698991f6cbba55d38f3f464432ced8d137a668b1f7618c7e747e23>

CVE-2022-41928 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 5.0-milestone-1, < 13.10.7**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 14.0.0, < 14.4.2**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

## CVE References

Description	Tags	Link
Loading...	<a href="#">jira.xwiki.org</a> <a href="#">text/html</a>	MISC <a href="https://jira.xwiki.org/browse/XWIKI-19800">jira.xwiki.org/browse/XWIKI-19800</a>
Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in AttachmentSelector.xml · Advisory · xwiki/xwiki-platform · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	CONFIRM <a href="https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-9hqh-fmhg-vq2j">github.com/xwiki/xwiki-platform/security/advisories/GHSA-9hqh-fmhg-vq2j</a>

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](mailto: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	<a href="#">Xwiki</a>	<a href="#">Xwiki</a>	All	All	All	All
Application	<a href="#">Xwiki</a>	<a href="#">Xwiki</a>	14.4.3	All	All	All
Application	<a href="#">Xwiki</a>	<a href="#">Xwiki</a>	14.4.4	All	All	All
Application	<a href="#">Xwiki</a>	<a href="#">Xwiki</a>	5.0	milestone1	All	All
Application	<a href="#">Xwiki</a>	<a href="#">Xwiki</a>	5.0	milestone2	All	All

```
cpe:2.3:a:xwiki:xwiki:*.*.*.*.*.*.*.*.:
```

```
cpe:2.3:a:xwiki:xwiki:14.4.3:*.*.*.*.*.*.*.*.:
```

```
cpe:2.3:a:xwiki:xwiki:14.4.4:*.*.*.*.*.*.*.*.:
```

```
cpe:2.3:a:xwiki:xwiki:5.0:milestone1:*.*.*.*.*.*.*.*.:
```

```
cpe:2.3:a:xwiki:xwiki:5.0:milestone2:*.*.*.*.*.*.*.*.:
```

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
/r/netcve	<a href="#">CVE-2022-41928</a>	2022-11-23 19:38:14

[← Previous ID](#)

[Next ID →](#)

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](#)**