Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in xwiki-platform-tag-ui

Critical **surli** published **GHSA-2g5c-228j-p52x** on Sep 8

Package	Affected versions	Patched versions
org.xwiki.platform:xwiki-application-tag (Maven)	>= 1.7	None
org.xwiki.platform:xwiki-platform-tag-ui (Maven)	< 13.10.6, < 14.4	13.10.6,14.4

Description

Impact

The tags document `Main.Tags` in XWiki didn't sanitize user inputs properly, allowing users with view rights on the document (default in a public wiki or for authenticated users on private wikis) to execute arbitrary Groovy, Python and Velocity code with programming rights. This allows bypassing all rights checks and thus both modification and disclosure of all content stored in the XWiki installation. Also, this could be used to impact the availability of the wiki. Some versions of XWiki XML-escaped the tag (e.g., version 3.1) but this isn't a serious limitation as string literals can be delimited by `/` in Groovy and `<` and `>` aren't necessary, e.g., to elevate privileges of the current user.

On XWiki versions before 13.10.4 and 14.2, this can be combined with the authentication bypass using the login action, meaning that no rights are required to perform the attack. The following URL demonstrates the attack: `<server>/xwiki/bin/login/Main/Tags?xpage=view&do=viewTag&tag=%7B%7Basync+async%3D%22true%22+cached%3D%22false%22+context%3D%22doc.reference%22%7D%7D%7B%7Bgroovy%7D%7Dprintln%28%22hello+from+groovy%21%22%29%7B%7B%2Fgroovy%7D%7D%7B%7B%2Fasync%7D%7D` , where `<server>` is the URL of the XWiki installations.

On current versions (e.g, 14.3), the issue can be exploited by requesting the URL `<server>/xwiki/bin/view/Main/Tags?do=viewTag&tag=%7B%7Basync%20async%3D%22true%22%20cached%3D%22false%22%20context%3D%22doc.reference%22%7D%7D%7B%7Bgroovy%7D%7Dprintln(%22hello%20from%20groovy!%22)%7B%7B%2Fgroovy%7D%7D%7B%7B%2Fasync%7D%7D`, where `<server>` is the URL of the server. On XWiki 2.0 (that contains version 1.7 of the tag application), the URL `<server>/xwiki/bin/view/Main/Tags?do=viewTag&tag={{/html}}{{groovy}}println(%2Fhello from groovy!%2F){{%2Fgroovy}}` demonstrates the exploit while on XWiki 3.1 the following URL demonstrates the exploit: `<server>/xwiki/bin/view/Main/Tags?do=viewTag&tag={{/html}}{{footnote}}{{groovy}}println(%2Fhello%20from%20groovy!%2F){{%2Fgroovy}}{{/footnote}}`.

Patches

This has been patched in the supported versions 13.10.6 and 14.4.

Workarounds

The patch that fixes the issue can be manually applied to the document `Main.Tags` or the updated version of that document can be imported from version 14.4 of xwiki-platform-tag-ui using the import feature in the administration UI on XWiki 10.9 and later (earlier versions might not be compatible with the current version of the document).

References

- `6048680`
- https://jira.xwiki.org/browse/XWIKI-19747

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

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-2022-36100

Weaknesses

CWE-95