

xwiki / xwiki-platform Public[Code](#) [Pull requests](#) 214 [Actions](#) [Projects](#) [Security and quality](#) 229

Reflected Cross-Site Scripting (XSS) in page history compare

Moderate michitux published [GHSA-w4fj-87j5-f25c](#) 15 hours ago

Package

 [org.xwiki.platform:xwiki-platform-web-templates](#) (Maven)

Affected versions

>= 10.4-rc-1, < 16.10.16
>= 17.0.0-rc-1, < 17.4.8
>= 17.5.0-rc-1, < 17.10.1

Patched versions

16.10.16
17.4.8
17.10.1

Description

Impact

A reflected cross-site scripting vulnerability (XSS) in the compare view between revisions of a page allows executing JavaScript code in the user's browser. If the current user is an admin, this can not only affect the current user but also the confidentiality, integrity and availability of the whole XWiki instance.

Patches

The problem has been patched by properly escaping the URL parameters.

Workarounds

The [patch](#) can be applied manually to `templates/changesdoc.vm` in the deployed WAR.

References

- [3c8a2ec](#)
- <https://jira.xwiki.org/browse/XWIKI-23472>

Attribution

We thank Mike Cole [@mikecole-mg](#) for discovering and reporting this vulnerability.

Severity

Moderate 6.5 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User interaction	Passive

Vulnerable System Impact Metrics

Confidentiality	None
Integrity	None
Availability	None

Subsequent System Impact Metrics

Confidentiality	High
Integrity	High
Availability	High

[Learn more about base metrics](#)

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:NVA:N/SC:H/SI:H/SA:H

CVE ID

CVE-2026-40105

Weaknesses

► CWE-80

Credits

 **mikecole-mg**

Reporter