It's possible to overwrite the security rules of a page with a final page having the same reference

High **surli** published **GHSA-gg53-wf5x-r3r6** on Sep 7

Package

org.xwiki.platform:xwiki-platform-security (Maven)

Affected versions	Patched versions
>= 5.0	12.10.11, 13.10.1, 13.4.6

Description

Impact

A bug in the security cache is storing rules associated to document Page1.Page2 and space Page1.Page2 in the same cache entry.

That means that it's possible to overwrite the rights of a space or a document by creating the page of the space with the same name and checking the right of the new one first so that they end up in the security cache and are used for the other too.

Patches

The problem has been patched in XWiki 12.10.11, 13.10.1, 13.4.6.

Workarounds

No workaround other than patching.

References

https://jira.xwiki.org/browse/XWIKI-14075
https://jira.xwiki.org/browse/XWIKI-18983

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

High 7.1 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	Low
Availability	None

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

CVE ID

CVE-2022-31167

Weaknesses

CWE-285