XSS Cross Site Scripting

High surli published GHSA-5c66-v29h-xjh8 on Apr 20, 2021

Package

org.xwiki.platform:xwiki-platform-oldcore, org.xwiki.platform:xwiki-platform-web (Maven)

Affected versions	Patched versions
< 12.8, < 12.6.3	12.8, 12.6.3

Description

Impact

It is possible to persistently inject scripts in XWiki.

For unregistred users:

- By filling simple text fields

For registered users:

- By filling their personal information
- (if they have edit rights) By filling the values of static lists using App Within Minutes

That can lead to user's session hijacking, and if used in conjunction with a social engineering attack it can also lead to disclosure of sensitive data, CSRF attacks and other security vulnerabilities.
That can also lead to the attacker taking over an account.
If the victim has administrative rights it might even lead to code execution on the server, depending on the application and the privileges of the account.

Patches

It has been patched on XWiki 12.8 and 12.6.3.

Workarounds

There is no easy workaround except upgrading XWiki.

References

https://jira.xwiki.org/browse/XWIKI-17374

For more information

If you have any questions or comments about this advisory:

- Open an issue in Jira XWiki
- Email us at our security mailing list

Severity

High

CVE ID

CVE-2021-29459

Weaknesses

No CWEs