XSS in the move attachment form

High **surli** published **GHSA-9r9j-57rf-f6vj** on Sep 8

Package

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

Affected versions	Patched versions
>= 14.0-rc-1	14.4-rc-1

Description

Impact

It's possible to store JavaScript in an attachment name, which will be executed by anyone trying to move the corresponding attachment.

For example, an attachment with name `><img src=1 onerror=alert(1)>.jpg` will execute the alert.

Patches

This issue has been patched in XWiki 14.4RC1.

Workarounds

It is possible to fix the vulnerability by copying moveStep1.vm to `webapp/xwiki/templates/moveStep1.vm` and replace

```
#set($titleToDisplay = $services.localization.render('attachment.move.title',
  [$attachment.name, $escapetool.xml($doc.plainTitle), $doc.getURL()]))
```

by

```
#set($titleToDisplay = $services.localization.render('attachment.move.title', [
  $escapetool.xml($attachment.name),
  $escapetool.xml($doc.plainTitle),
```

```
    $escapetool.xml($doc.getURL())
  ]))
```

See the corresponding patch.

References

- https://jira.xwiki.org/browse/XWIKI-19667

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 8.9 / 10

CVSS base metrics	
Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Changed
Confidentiality	High
Integrity	High
Availability	Low

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

CVE ID

CVE-2022-36097

Weaknesses

CWE-80