HSEC-2026-0004

See a problem?

Import Source	https://github.com/haskell/security-advisories/blob/generated/osv-export/2026/HSEC-2026-0004.json
JSON Data	https://api.osv.dev/v1/vulns/HSEC-2026-0004
Aliases	CVE-2026-40472
Published	2026-03-28T16:05:12Z
Modified	2026-03-28T16:15:05.535024Z
Summary	Hackage package metadata stored XSS vulnerability

Details

Hackage package metadata stored XSS vulnerability

User-controlled metadata from `.cabal` files are rendered into HTML `href` attributes without proper sanitization, enabling stored Cross-Site Scripting (XSS) attacks. The specific fields affected are:

- `homepage`
- `bug-reports`
- `source-repository.location`
- `description` (Haddock hyperlinks)

The Haskell Security Response Team audited the entire corpus of **published** packages on `hackage.haskell.org`—all published package versions but *not* candidates. No exploitation attempts were detected.

To fix the issue, *hackage-server* now inspects target URIs and only produces a hyperlink when the URI has an approved scheme: `http`, `https`, and (only for some fields) `mailto`.

The fix has been committed and deployed on `hackage.haskell.org`. Other operations of *hackage-server* instances should update as soon as possible to commit `2de3ae45082f8f3f29a41f6aff620d09d0e74058` or later.

Acknowledgements

- **Joshua Rogers** (https://joshua.hu/) of AISLE (https://aisle.com/) reported the issue to the Haskell Security Response Team.
- **Fraser Tweedale** implemented the fix.
- **Gershom Bazerman** merged the fix and deployed it to `hackage.haskell.org`.

Database specific


```
{
    "home": "https://github.com/haskell/security-advisories",
    "osvs": "https://raw.githubusercontent.com/haskell/security-advisories/refs/heads/generated/osv-export",
    "repository": "https://github.com/haskell/security-advisories"
}
```


References

https://github.com/haskell/hackage-server/commit/2de3ae45082f8f3f29a41f6aff620d09d0e74058

Affected packages

Hackage
hackage-server

Package

Name hackage-server

Purl pkg:hackage/hackage-server

Severity

9.9 (Critical) CVSS_V3 - CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L CVSS Calculator

Affected ranges

Type ECOSYSTEM

Events Introduced
0.1

Affected versions

▸ 0.*

Database specific

▸ source

▸ osv

▸ human_link
