HSEC-2026-0002

See a problem?

Import Source	https://github.com/haskell/security-advisories/blob/generated/osv-export/2026/HSEC-2026-0002.json
JSON Data	https://api.osv.dev/v1/vulns/HSEC-2026-0002
Aliases	CVE-2026-40471
Published	2026-03-28T16:04:58Z
Modified	2026-03-28T16:15:09.093594Z
Summary	Hackage CSRF vulnerability

Details

Hackage CSRF vulnerability

- Vulnerable File: `src/Distribution/Server/Features/Votes.hs` (example)
- Impact: can forge requests through XSS

hackage-server lacked Cross-Site Request Forgery (CSRF) protection across its endpoints. Scripts on foreign sites could trigger requests to hackage server, possibly abusing latent credentials to upload packages or perform other administrative actions. Some unauthenticated actions could also be abused (e.g. creating new user accounts).

To fix the issue, a new CSRF middleware checks all requests. Requests using HTTP methods other than `GET`, `HEAD` and `OPTIONS` are subject to a check of the `Sec-Fetch-Site` header, which is widely supported by modern browsers. Cross-site requests are `403 Forbidden`. Certain approved and expected non-browser user agents (e.g. `cabal-install/*`) are exempted from the check, as are requests using token authentication (`Authorization: X-ApiKey ...`).

The fix has been committed and deployed on `hackage.haskell.org`.

Acknowledgements

- **Joshua Rogers** (https://joshua.hu/) of AISLE (https://aisle.com/) reported the issue to the Haskell Security Response Team.
- **Spenser Janssen** implemented the fix, and **Fraser Tweedale** reviewed it.

- **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

`9.6 (Critical)` `CVSS_V3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:R/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
