skip to content
Back to GitHub.com
Security Lab
Bounties Research Advisories Get Involved Events

February 12, 2021

GHSL-2020-199: Open redirect vulnerability in Slashify - CVE-2021-3189

GitHub Security Lab

Coordinated Disclosure Timeline

- 10/19/2020: Report sent to scottcorgan@gmail.com (https://registry.npmjs.org/slashify/latest)
- 01/20/2021: Issue reported to affected projects: `uktrade/data-hub-frontend` and `ministryofjustice/hmpps-book-secure-move-frontend`
- 01/20/2021: Issue gets fixed in ministryofjustice/hmpps-book-secure-move-frontend
- 01/21/2021: MITRE assigns CVE-2021-3189
- 02/02/2021: Issue gets fixed in uktrade/data-hub-frontend

Summary

Open redirect in Slashify

Product

The slashify npm package.

Tested Version

Latest commit at the date of reporting.

Details

The package is an Express middleware that normalises routes by stripping any final slash, redirecting, for example, `bookings/latest/` to `bookings/latest`. However, it does not validate the path it redirects to in any way. In particular, if the path starts with two slashes (or two backslashes, or a slash and a backslash, etc.) it may redirect to a different domain.

Consider the example from the docs. Assume we have run it and started a server on `localhost:3000`, then visiting `localhost:3000///github.com/` redirects you to https://github.com.

Impact

Open redirect

CVE

- CVE-2021-3189

Credit

This issue was discovered and reported by GitHub team member @max-schaefer (Max Schaefer).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include `GHSL-2020-199` in any communication regarding this issue.

GitHub

Product

- Features
- Security
- Enterprise
- Customer stories
- Pricing
- Resources

Platform

- Developer API
- Partners
- Atom
- Electron
- GitHub Desktop

Support

- Docs
- Community Forum
- Professional Services
- Status
- Contact GitHub

Company

- About
- Blog
- Careers
- Press
- Shop

-
-
-

-
-
-