CSRF Protection Bypass in Authentication Flow

Moderate **denolfe** published **GHSA-p6mr-xf3r-ghq4** 2 days ago

Package

payload (npm)

Affected versions	Patched versions
< 3.79.1	3.79.1

Description

Impact

A Cross-Site Request Forgery (CSRF) vulnerability existed in the authentication flow. Under certain conditions, the configured CSRF protection could be bypassed, allowing cross-site requests to be made.

You are affected if ALL of these are true:

- Payload version **< v3.79.1**
- `serverURL` is configured

Patches

This vulnerability has been patched in **v3.79.1**. Additional validation has been added to the authentication flow.

Users should upgrade to **v3.79.1** or later.

Workarounds

There is no complete workaround without upgrading.

If you cannot upgrade immediately, setting `cookies.sameSite` to `'Strict'` will prevent the session cookie from being sent cross-site. However, this will also require users to re-authenticate when navigating to your application from external links (e.g. email, other sites).

Severity

Moderate 5.4 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity	Low
Availability	Low

Learn more about base metrics

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

CVE ID

CVE-2026-34749

Weaknesses

▶ CWE-352