URL Redirection to Untrusted Site ('Open Redirect') in @adonisjs/http-server

Moderate **thetutlage** published **GHSA-6qvv-pj99-48qm** 3 days ago

Package

@adonisjs/core (npm)

Affected versions	Patched versions
< 7.3.0	7.3.1

@adonisjs/http-server (npm)

< 8.2.0	8.2.0

Description

Impact

The `response.redirect().back()` method in `@adonisjs/http-server` is vulnerable to open redirects. The method reads the `Referer` header from the incoming HTTP request and redirects to that URL without validating the host. An attacker who can influence the `Referer` header (for example, by linking a user through an attacker-controlled page before a form submission) can cause the application to redirect users to a malicious external site.

This affects all AdonisJS applications that use `response.redirect().back()` or `response.redirect('back')`.

The vulnerability is classified as CWE-601: URL Redirection to Untrusted Site ('Open Redirect').

Patches

This has been fixed in `@adonisjs/http-server` version **8.2.0**. The `back()` method now validates the `Referer` header's host against the request's own `Host` header. Referrers from unrecognized hosts are rejected and the redirect falls back to `/` (or a developer-provided fallback URL).

Applications that operate across multiple domains can configure additional trusted hosts via the `redirect.allowedHosts` option in `config/app.ts`.

Users should upgrade to `@adonisjs/http-server@^8.2.0` (or `@adonisjs/core@^7.4.0` if using the core meta-package).

Workarounds

If upgrading is not immediately possible, avoid using `response.redirect().back()` in routes that are reachable by unauthenticated users or from pages that accept external traffic. Instead, redirect to a known safe path explicitly using `response.redirect().toPath('/dashboard')`.

References

- CWE-601: URL Redirection to Untrusted Site
- OWASP: Unvalidated Redirects and Forwards

Severity

Moderate 6.1 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-40255

Weaknesses

▶ CWE-601

Credits

thetutlage

Reporter