Authenticated SSRF via Upload Functionality

High **denolfe** published **GHSA-6r7f-q7f5-wpx8** 2 days ago

Package

payload (npm)

Affected versions	Patched versions
< 3.79.1	3.79.1

Description

Impact

An authenticated Server-Side Request Forgery (SSRF) vulnerability existed in the upload functionality.

Authenticated users with `create` or `update` access to an upload-enabled collection could cause the server to make outbound HTTP requests to arbitrary URLs.

You are affected if ALL of these are true:

- Payload version **< v3.79.1**
- At least one collection with `upload` enabled
- An authenticated user has `create` or `update` access to that collection

Patches

This vulnerability has been patched in **v3.79.1**.
Users should upgrade to **v3.79.1** or later.

Workarounds

Until you can upgrade:

- Restrict `create` and `update` access to upload-enabled collections to trusted roles only.
- Limit outbound network access from your Payload server where possible.

Severity

High 7.7 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-34746

Weaknesses

▶ CWE-918