SSRF via redirect following in Cloudflare image-binding-transform endpoint (incomplete fix for GHSA-qpr4)

Low **matthewp** published **GHSA-88gm-j2wx-58h6** 4 days ago

Package

@astrojs/cloudflare (npm)

Affected versions

<= 13.1.6

Patched versions

13.1.10

Description

Summary

The `fetch()` call for remote images in `packages/integrations/cloudflare/src/utils/image-binding-transform.ts` (line 28) uses the default `redirect: 'follow'` behavior. This allows the Cloudflare Worker to follow HTTP redirects to arbitrary URLs, bypassing the `isRemoteAllowed()` domain allowlist check which only validates the initial URL.

All three other image fetch paths in the codebase correctly use `{ redirect: 'manual' }`. This is an incomplete fix for GHSA-qpr4-c339-7vq8.

Confirmed on HEAD.

Root Cause

`image-binding-transform.ts` line 28:

```
const content = await (isRemotePath(href) ? fetch(imageSrc) :
assets.fetch(imageSrc));
```

Missing `{ redirect: 'manual' }`. The three protected paths:

```
// image-passthrough-endpoint.ts:23
response = await fetch(href, { redirect: 'manual' });

// assets/endpoint/shared.ts:11
const res = await fetch(src, { redirect: 'manual' });

// assets/utils/remoteProbe.ts:53
const response = await fetch(url, { redirect: 'manual' });
```

PoC

Demonstrated with Node.js that `fetch()` without `redirect: 'manual'` follows 302 redirects to arbitrary destinations:

```
# Server A (allowed domain) returns 302 → Server B (internal)
fetch('http://allowed:19741/img.jpg')                      → follows 302 → hits
http://internal:19742/secret
fetch('http://allowed:19741/img.jpg', {redirect:'manual'})   → returns 302, internal
server NOT hit
```

Attack path: attacker finds an open redirect on an allowed domain, crafts `/_image?href=https://allowed-cdn.com/redirect?url=http://internal-service/`, and the Worker follows the redirect to the unauthorized destination.

Impact

Bypasses the `image.domains` and `image.remotePatterns` allowlist for the default Cloudflare image service (`cloudflare-binding`). Enables blind SSRF to domains not in the allowlist. Same vulnerability class as GHSA-qpr4-c339-7vq8 (HIGH) which fixed the passthrough endpoint but missed this one.

Suggested Fix

```
const content = await (isRemotePath(href) ? fetch(imageSrc, { redirect: 'manual' }
assets.fetch(imageSrc));
```

Severity

Low 2.2 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-41321

Weaknesses

▶ CWE-918

Credits

kodareef5 Reporter