Password?Protected Thumbnail Bypass

GHSA : https://github.com/FlintSH/Flare/security/advisories/GHSA-3x7v-x3r6-mjh7

CVE : CVE-2026-30230

Summary

The thumbnail endpoint does not validate the password for password-protected files. It checks ownership/admin for private files but skips password verification, allowing thumbnail access without the password.

Affected Component

- Thumbnail endpoint: thumbnail/route.ts

Evidence (Code References)

- File password is fetched but never checked: thumbnail/route.ts:L32-L49
- Password checks exist in other endpoints:
- Download: download/route.ts:L50-L67
- Raw: raw/route.ts:L99-L107

Video POC

Your browser does not support the video tag.

Impact

- Visual content of password-protected files can be previewed through thumbnails without the password.
- Information disclosure of sensitive images despite password protection.

Expected vs Actual

- Expected: Password-protected files require a valid password for any content access, including thumbnails.
- Actual: Thumbnail content is served without password verification.

Reproduction Checklist

- Create User A and upload an image with a password.
- Note the file ID.
- Log in as User B (non-owner, non-admin).
- Request the thumbnail for User A’s file without providing the password.
- Expected: access denied.
- Actual: thumbnail returned.

Consider aligning thumbnail checks with the download/raw endpoints for consistent behavior.

Verification Checklist

- Create a password-protected image file.
- Access thumbnail as:
  - Unauthenticated user → denied
  - Authenticated non-owner → denied unless password provided
  - Owner/admin → allowed
- Confirm behavior matches download/raw endpoints.

Revision #3
Created 2026-03-02 14:20:33 UTC by Aryma
Updated 2026-03-06 01:21:49 UTC by Aryma