Server-Side Request Forgery (SSRF) in Craft CMS with Asset Uploads Mutations

Moderate **angrybrad** published **GHSA-3m9m-24vh-39wx** last week

Package

php **craftcms/cms** (Composer)

Affected versions	Patched versions
>= 5.0.0-RC1, <= 5.9.14	5.9.15
>= 4.0.0-RC1, <= 4.17.8	4.17.9

Description

Required Permissions

The exploitation requires a few permissions to be enabled in the used GraphQL schema:

- "Edit assets in the volume"
- "Create assets in the volume"

Details

The implementation fails to restrict the URL Scheme. While the application is intended to "upload assets", there is no whitelist forcing `http` or `https`. This allows attackers to use the Gopher protocol to wrap raw TCP commands.

Impact: Combined with the DWORD bypass, an attacker can hit internal services without triggering any "127.0.0.1" string-matching filters.

Example Payload: gopher://2130706433:6379/_FLUSHALL (Targets local Redis via DWORD).

Remediation Strategy

To prevent mathematical IP obfuscation, the application must normalize the hostname before validation.

References

`d20aecf`

Severity

Moderate

CVE ID

CVE-2026-41129

Weaknesses

▶ CWE-918

Credits

r3dbrothers Reporter