SameSite Attackers may Bypass the CSRF Protection

Moderate **MGatner** published **GHSA-5hm8-vh6r-2cjq** on Aug 7

Package

php **CodeIgniter Shield** (Composer)

Affected versions	Patched versions
1.0.0-beta	1.0.0-beta.2

Description

Impact

This vulnerability may allow SameSite Attackers to bypass the CodeIgniter4 CSRF protection mechanism with CodeIgniter Shield.

For this attack to succeed, the attacker must have direct (or indirect, e.g., XSS) control over a subdomain site (e.g., `https://a.example.com/`) of the target site (e.g., `http://example.com/`).

This vulnerability exists whether `Config\Security::$csrfProtection` is `'cookie'` or `'session'` .
It is also exploitable whether `Config\Security::$regenerate` is `true` or `false` .

Patches

Upgrade to **CodeIgniter v4.2.3 or later** and **Shield v1.0.0-beta.2 or later**.

Workarounds

Do all of the following:

- set `Config\Security::$csrfProtection` to `'session'`
- remove old session data right after login (immediately after ID and password match)
- regenerate CSRF token right after login (immediately after ID and password match)

References

- CodeIgniter4 CSRF Protection
- SameSite Attacks
- SameSite Cookies
- The great SameSite confusion

For more information

If you have any questions or comments about this advisory:

- Open an issue or discussion in codeigniter4/shield
- Email us at security@codeigniter.com

Severity

Moderate 5.9 / 10

CVSS base metrics

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

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

CVE ID

CVE-2022-35943

Weaknesses

CWE-352

Credits

 wert310

 pedromigueladao

 lavish