Denial of Service via quadratic complexity in OverlappingFieldsCanBeMerged validation

Moderate **spawnia** published **GHSA-68jq-c3rv-pcrr** last week

Package

php **webonyx/graphql-php** (Composer)

Affected versions	Patched versions
<= 15.31.4	15.31.5

Description

The `OverlappingFieldsCanBeMerged` validation rule exhibits quadratic time complexity when processing queries with many repeated fields sharing the same response name. An attacker can send a crafted query like `{ hello hello hello ... }` with thousands of repeated fields, causing excessive CPU usage during validation before execution begins.

This is not mitigated by existing QueryDepth or QueryComplexity rules.

Observed impact (tested on v15.31.4):

- 1000 fields: ~0.6s
- 2000 fields: ~2.4s
- 3000 fields: ~5.3s
- 5000 fields: request timeout (>20s)

Root cause: `collectConflictsWithin()` performs $O(n^2)$ pairwise comparisons of all fields with the same response name. For identical repeated fields, every comparison returns "no conflict" but the quadratic iteration count causes resource exhaustion.

Fix: Deduplicate structurally identical fields before pairwise comparison, reducing the complexity from $O(n^2)$ to $O(u^2)$ where u is the number of unique field signatures (typically 1 for this attack pattern).

Credit: Ashwak N (ashwakn04@gmail.com)

Severity

Moderate

CVE ID

CVE-2026-40476

Weaknesses

▶ CWE-407