

# plugin-php

github.com/prettier/plugin-php

Scanned 24 September 2026 at 10:16 · Report generated 29 October 2026 · PHP · 1,856 stars

OVERALL ASSESSMENT

Low

Combined score 13 · 27 findings after filtering

## Summary

6 findings likely need attention, 19 look like noise. Most notable: This Dependabot configuration does not set a cooldown period. Newly published packages ... (99% confidence).  
Generated from finding counts. A plain-English summary was not available for this scan.

## Risk, by type

MalDet scores two different questions separately, because they call for different responses: code can be badly written without being hostile, and hostile code is not always badly written.

VULNERABILITY

Low (13)

Insecure coding an attacker could exploit. Usually mistakes, and usually fixable in place.

MALICIOUS PATTERN

Safe (0)

Signs the code may be trying to do harm: hidden payloads, credential access, persistence, exfiltration.

## What each detector found

| DETECTOR    | LOOKS FOR                                         | HIGH | MEDIUM | LOW | TOTAL |
|-------------|---------------------------------------------------|------|--------|-----|-------|
| dep_checker | Vulnerable, unpinned or typosquatted dependencies | 0    | 0      | 19  | 19    |
| semgrep     | Insecure coding patterns across many languages    | 0    | 8      | 0   | 8     |

6 of 27 findings were rated more likely genuine than noise by the classifier.

## Evidence

Identical findings are grouped, so a single rule firing many times takes one row. Ordered worst first. “Seen” is how many times that finding occurred.

| SEVERITY | DETECTOR    | FINDING                                                                                                                                                                                                                                                                                                      | SEEN | EXAMPLE LOCATION                              |
|----------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----------------------------------------------|
| MEDIUM   | semgrep     | This Dependabot configuration does not set a cooldown period. Newly published packages can be malicious or unstable. Add a `cooldown` block with `default-days: 7` to each `package-ecosystem` entry under `updates` to wait 7 days before proposing updates to newly published package versions. Reference: | 1    | <code>/.github/dependabot.yml:3</code>        |
| MEDIUM   | semgrep     | GitHub Actions step uses a mutable tag or branch reference. Tags and branch names can be silently repointed by the action owner, enabling supply-chain attacks — as seen in the trivy-action and kics-github-action compromises. Pin the reference to a full 40-character commit SHA instead, e.g. `uses: ac | 5    | <code>/.github/workflows/nodejs.yml:20</code> |
| MEDIUM   | semgrep     | Detected possible user input going into a `path.join` or `path.resolve` function. This could possibly lead to a path traversal vulnerability, where the attacker can access arbitrary files stored in the file system. Instead, be sure to sanitize or validate user input first.                            | 2    | <code>/tests_config/run_spec.mjs:26</code>    |
| LOW      | dep_checker | Loose version constraint: 'cross-env^10.1.0' — attacker could push malicious update                                                                                                                                                                                                                          | 1    | <code>package.json</code>                     |
| LOW      | dep_checker | Loose version constraint: 'eslint-plugin-prettier-doc^1.1.0' — attacker could push malicious update                                                                                                                                                                                                          | 1    | <code>package.json</code>                     |
| LOW      | dep_checker | Loose version constraint: 'strip-ansi^7.1.0' — attacker could push malicious update                                                                                                                                                                                                                          | 1    | <code>package.json</code>                     |
| LOW      | dep_checker | Loose version constraint: 'rollup^4.60.0' — attacker could push malicious update                                                                                                                                                                                                                             | 1    | <code>package.json</code>                     |
| LOW      | dep_checker | Loose version constraint: 'prettier^3.6.1' — attacker could push malicious update                                                                                                                                                                                                                            | 1    | <code>package.json</code>                     |
| LOW      | dep_checker | Loose version constraint: 'php-parser^3.7.0' — attacker could push malicious update                                                                                                                                                                                                                          | 1    | <code>package.json</code>                     |
| LOW      | dep_checker | Loose version constraint: 'linguist-languages^9.4.0' — attacker could push malicious update                                                                                                                                                                                                                  | 1    | <code>package.json</code>                     |

| SEVERITY | DETECTOR    | FINDING                                                                                               | SEEN | EXAMPLE LOCATION |
|----------|-------------|-------------------------------------------------------------------------------------------------------|------|------------------|
| LOW      | dep_checker | Loose version constraint: 'jest-snapshot-serializer-raw^2.0.0' — attacker could push malicious update | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: 'jest-light-runner^0.7.9' — attacker could push malicious update            | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: '@babel/preset-env^7.27.2' — attacker could push malicious update           | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: 'c8^10.1.3' — attacker could push malicious update                          | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: '@rollup/plugin-terser^0.4.3' — attacker could push malicious update        | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: '@rollup/plugin-replace^6.0.3' — attacker could push malicious update       | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: '@rollup/plugin-node-resolve^16.0.3' — attacker could push malicious update | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: '@rollup/plugin-json^6.1.0' — attacker could push malicious update          | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: '@rollup/plugin-inject^5.0.5' — attacker could push malicious update        | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: '@rollup/plugin-commonjs^29.0.2' — attacker could push malicious update     | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: '@rollup/plugin-babel^7.0.0' — attacker could push malicious update         | 1    | package.json     |
| LOW      | dep_checker | Loose version constraint: '@rollup/plugin-alias^6.0.0' — attacker could push malicious update         | 1    | package.json     |

## How to read this report

---

- **This is a static scan.** The code was read, never executed. Behaviour that only appears at runtime is outside what any of these detectors can see.
- **Findings are not all equally real.** A classifier rates each finding on how likely it is to be genuine rather than noise, and that rating weights the scores. Measured against a hand-reviewed sample it reached precision 0.52 and recall 0.62 — useful for ranking, not a verdict on any single finding.
- **A high score is not proof of malice.** Security tools, penetration-testing frameworks and malware research repositories contain the same patterns as real malware by design. The two risk types above exist to keep that distinction visible.
- **Absence of findings is not proof of safety.** A detector that is not installed, or a language none of them parse, produces silence rather than a warning.
- **This scan is a snapshot.** The repository may have changed since 24 September 2026.