

# Software Composition Analysis Report

acme/app

|        |                 |          |      |        |     |
|--------|-----------------|----------|------|--------|-----|
| FAILED | 6               | 0        | 5    | 1      | 0   |
|        | Vulnerabilities | Critical | High | Medium | Low |

## Target

|                  |                |
|------------------|----------------|
| Audited packages | 5              |
| Fails on         | High or higher |

## Run

|          |                                                                |
|----------|----------------------------------------------------------------|
| Date     | 2026-10-17 14:28:21 – 14:28:21 (UTC)                           |
| Duration | 0s                                                             |
| Software | PHP 8.5.11  Composer 2.8.12  pieceofcake2/security-sca 1.x-dev |

The vulnerabilities are those of the security advisories of Packagist (the GitHub Advisory Database and the FriendsOfPHP security advisories) at the time of the run.

## Vulnerabilities by risk

### 1. High

| No. | Vulnerability                                                                   | Risk | Package             |
|-----|---------------------------------------------------------------------------------|------|---------------------|
| 1-1 | CVE-2018-19296 Object injection                                                 | High | phpmailer/phpmailer |
| 1-2 | CVE-2020-13625 Insufficient output escaping of attachment names in PHPMailer    | High | phpmailer/phpmailer |
| 1-3 | CVE-2021-34551 RCE affecting Windows hosts via UNC paths to translation files   | High | phpmailer/phpmailer |
| 1-4 | CVE-2021-3603 Untrusted code may be run from an overridden address validator    | High | phpmailer/phpmailer |
| 1-5 | CVE-2020-15094 Prevent RCE when calling untrusted remote with CachingHttpClient | High | symfony/http-kernel |

### 2. Medium

| No. | Vulnerability                                              | Risk   | Package             |
|-----|------------------------------------------------------------|--------|---------------------|
| 2-1 | CVE-2022-24894 Prevent storing cookie headers in HttpCache | Medium | symfony/http-kernel |

### 3. Abandoned packages

| No. | Vulnerability | Risk      | Package       |
|-----|---------------|-----------|---------------|
| 3-1 | symfony/debug | Abandoned | symfony/debug |

### 4. Audited packages

| No. | Vulnerability             | Risk | Package |
|-----|---------------------------|------|---------|
| 4-1 | Packages of composer.lock | List | 5       |

1. High

1-1 CVE-2018-19296 Object injection

High

|                   |                                                                                                                             |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Risk              | High                                                                                                                        |
| Package           | phpmailer/phpmailer                                                                                                         |
| Installed version | v6.0.0                                                                                                                      |
| Affected versions | >=5.0.0,<5.2.27 >=6.0.0,<6.0.6                                                                                              |
| CVE               | CVE-2018-19296                                                                                                              |
| Advisory          | PKSA-dn5d-4vy3-wsfy, GitHub: GHSA-7w4p-72j7-v7c2, FriendsOfPHP/security-advisories: phpmailer/phpmailer/CVE-2018-19296.yaml |
| Reported          | 2017-07-26                                                                                                                  |

- <https://github.com/PHPMailer/PHPMailer/releases/tag/v6.0.6>
- <https://www.cve.org/CVERecord?id=CVE-2018-19296>
- <https://github.com/advisories/GHSA-7w4p-72j7-v7c2>

1. High

1-2 CVE-2020-13625 Insufficient output escaping of attachment names in PHPMailer

High

|                   |                                                  |
|-------------------|--------------------------------------------------|
| Risk              | High                                             |
| Package           | phpmailer/phpmailer                              |
| Installed version | v6.0.0                                           |
| Affected versions | <6.1.6                                           |
| CVE               | CVE-2020-13625                                   |
| Advisory          | PKSA-8sw7-9x88-c8bx, GitHub: GHSA-f7hx-fqwx-rvvj |
| Reported          | 2020-05-27                                       |

- <https://github.com/advisories/GHSA-f7hx-fqwx-rvvj>
- <https://www.cve.org/CVERecord?id=CVE-2020-13625>

1. High

1-3 CVE-2021-34551 RCE affecting Windows hosts via UNC paths to translation files

High

|                   |                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------|
| Risk              | High                                                                                                                       |
| Package           | phpmailer/phpmailer                                                                                                        |
| Installed version | v6.0.0                                                                                                                     |
| Affected versions | <6.5.0                                                                                                                     |
| CVE               | CVE-2021-34551                                                                                                             |
| Advisory          | PKSA-35kn-2ddp-d3p4, GitHub: GHSA-7q44-r25x-wm4q, FriendsOfPHP/security-advisories:phpmailer/phpmailer/CVE-2021-34551.yaml |
| Reported          | 2021-06-16                                                                                                                 |

- <https://github.com/PHPMailer/PHPMailer/releases/tag/v6.5.0>
- <https://www.cve.org/CVERecord?id=CVE-2021-34551>
- <https://github.com/advisories/GHSA-7q44-r25x-wm4q>

1. High

## 1-4 CVE-2021-3603 Untrusted code may be run from an overridden address validator

High

|                   |                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------|
| Risk              | High                                                                                                                      |
| Package           | phpmailer/phpmailer                                                                                                       |
| Installed version | v6.0.0                                                                                                                    |
| Affected versions | <6.5.0                                                                                                                    |
| CVE               | CVE-2021-3603                                                                                                             |
| Advisory          | PKSA-m8by-bb7v-7qt5, GitHub: GHSA-77mr-wc79-m8j3, FriendsOfPHP/security-advisories:phpmailer/phpmailer/CVE-2021-3603.yaml |
| Reported          | 2021-06-16                                                                                                                |

- <https://github.com/PHPMailer/PHPMailer/releases/tag/v6.5.0>
- <https://www.cve.org/CVERecord?id=CVE-2021-3603>
- <https://github.com/advisories/GHSA-77mr-wc79-m8j3>

1. High

1-5 CVE-2020-15094 Prevent RCE when calling untrusted remote with CachingHttpClient

High

|                   |                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------|
| Risk              | High                                                                                                                       |
| Package           | symfony/http-kernel                                                                                                        |
| Installed version | v4.4.0                                                                                                                     |
| Affected versions | >=4.3.0,<4.4.0 >=4.4.0,<4.4.13 >=5.0.0,<5.1.0 >=5.1.0,<5.1.5                                                               |
| CVE               | CVE-2020-15094                                                                                                             |
| Advisory          | PKSA-8knv-7jsn-12w8, GitHub: GHSA-754h-5r27-7x3r, FriendsOfPHP/security-advisories:symfony/http-kernel/CVE-2020-15094.yaml |
| Reported          | 2020-09-02                                                                                                                 |

- <https://symfony.com/cve-2020-15094>
- <https://www.cve.org/CVERecord?id=CVE-2020-15094>
- <https://github.com/advisories/GHSA-754h-5r27-7x3r>

## 2. Medium

**2-1 CVE-2022-24894 Prevent storing cookie headers in HttpCache****Medium**

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Risk              | Medium                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Package           | symfony/http-kernel                                                                                                                                                                                                                                                                                                                                                                                                      |
| Installed version | v4.4.0                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Affected versions | >=2.0.0,<2.1.0 >=2.1.0,<2.2.0 >=2.2.0,<2.3.0 >=2.3.0,<2.4.0 >=2.4.0,<2.5.0 >=2.5.0,<2.6.0 >=2.6.0,<2.7.0 >=2.7.0,<2.8.0 >=2.8.0,<3.0.0 >=3.0.0,<3.1.0 >=3.1.0,<3.2.0 >=3.2.0,<3.3.0 >=3.3.0,<3.4.0 >=3.4.0,<4.0.0 >=4.0.0,<4.1.0 >=4.1.0,<4.2.0 >=4.2.0,<4.3.0 >=4.3.0,<4.4.0 >=4.4.0,<4.4.50 >=5.0.0,<5.1.0 >=5.1.0,<5.2.0 >=5.2.0,<5.3.0 >=5.3.0,<5.4.0 >=5.4.0,<5.4.20 >=6.0.0,<6.0.20 >=6.1.0,<6.1.12 >=6.2.0,<6.2.6 |
| CVE               | CVE-2022-24894                                                                                                                                                                                                                                                                                                                                                                                                           |
| Advisory          | PKSA-hr4y-jwk2-1yb9, GitHub: GHSA-h7vf-5wrv-9fhv, FriendsOfPHP/security-advisories:symfony/http-kernel/CVE-2022-24894.yaml                                                                                                                                                                                                                                                                                               |
| Reported          | 2023-02-01                                                                                                                                                                                                                                                                                                                                                                                                               |

- <https://symfony.com/cve-2022-24894>
- <https://www.cve.org/CVERecord?id=CVE-2022-24894>
- <https://github.com/advisories/GHSA-h7vf-5wrv-9fhv>

3. Abandoned packages

3-1 symfony/debug

Abandoned

|             |                       |
|-------------|-----------------------|
| Package     | symfony/debug         |
| Use instead | symfony/error-handler |

The package is no longer maintained, so its vulnerabilities will not be fixed.

4. Audited packages

4-1 Packages of composer.lock

List

|             |   |
|-------------|---|
| Packages    | 5 |
| Direct      | 1 |
| Development | 1 |

The packages that were audited, in the versions of composer.lock. The packages that the project requires in its composer.json are direct; the others are required by them.

| Package              | Installed version | Kind                   | License       | Status            |
|----------------------|-------------------|------------------------|---------------|-------------------|
| phpmailer/phpmailer  | v6.0.0            | Production · direct    | LGPL-2.1-only | 4 vulnerabilities |
| phpunit/phpunit      | 9.6.0             | Development · indirect | BSD-3-Clause  | -                 |
| pieceofcake2/cakephp | v2.12.2           | Production · indirect  | MIT           | -                 |
| symfony/debug        | v4.4.44           | Production · indirect  | MIT           | Abandoned         |
| symfony/http-kernel  | v4.4.0            | Production · indirect  | MIT           | 2 vulnerabilities |