

homebrew-awesome-brew

github.com/romankurnovskii/homebrew-awesome-brew

Scanned 24 September 2026 at 10:25 · Report generated 29 October 2026 · Ruby · 115 stars

OVERALL ASSESSMENT

Low

Combined score 18 · 21 findings after filtering

Summary

7 findings likely need attention, 14 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 (17)

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

MALICIOUS PATTERN

Low (1)

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
bandit	Insecure coding patterns in Python source	0	7	5	12
semgrep	Insecure coding patterns across many languages	0	6	0	6
yara	Signatures of malicious behaviour in source files	0	0	2	2
guarddog	Malicious package and install-time behaviour	0	0	1	1

7 of 21 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:	2	/.github/dependabot.yml:13
MEDIUM	semgrep	Detected non-static command inside `...`. If unverified user data can reach this call site, this is a code injection vulnerability. A malicious actor can inject a malicious script to execute arbitrary code.	2	/Formula/unrar.rb:35
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	2	/.github/workflows/update_casks.yml:19
MEDIUM	bandit	Call to requests without timeout	7	/generate_casks.py:118
LOW	guarddog	Detects reading of environment variables (credential access, often contains secrets) [threat-runtime-environment-read]	1	/generate_casks.py:76
LOW	bandit	Starting a process with a partial executable path	2	/update_casks.py:74
LOW	bandit	Consider possible security implications associated with the subprocess module.	1	/update_casks.py:3
LOW	bandit	subprocess call - check for execution of untrusted input.	2	/update_casks.py:74

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	yara	YARA rule matched: detect_downloader — Downloads a remote resource - common and low-signal alone; see detect_download_and_execute for the composite version	2	/ generate_c asks.py

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.