

seclab-taskflow-agent

github.com/GitHubSecurityLab/seclab-taskflow-agent

Scanned 29 October 2026 at 09:26 · Report generated 29 October 2026 · Python · 283 stars

OVERALL ASSESSMENT

High

Combined score 149 · 54 findings after filtering

Summary

24 findings likely need attention, 30 look like noise. Most notable: Found 'importlib.resources', which is a module only available on Python 3.7+. This does... (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

High (147)

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

MALICIOUS PATTERN

Low (2)

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	1	25	26
semgrep	Insecure coding patterns across many languages	5	8	0	13
dep_checker	Vulnerable, unpinned or typosquatted dependencies	10	0	3	13
guarddog	Malicious package and install-time behaviour	0	0	2	2

24 of 54 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
HIGH	semgrep	Found 'importlib.resources', which is a module only available on Python 3.7+. This does not work in lower versions, and therefore is not backwards compatible. Use importlib_resources instead for older Python versions.	1	/src/seclab_taskflow_agent/available_tools.py:14
HIGH	semgrep	the `encoding` argument to Popen is only available on Python 3.6+	1	/src/seclab_taskflow_agent/shell_utils.py:22
HIGH	dep_checker	CVE found: GHSA-7xgj-8392-5q4r in fastmcp==3.2.0 — ## Maintainer assessment and remediation This report is accepted as a FastMCP authorization vulnera	1	pyproject.toml
HIGH	dep_checker	CVE found: CVE-2026-96760 in authlib==1.6.12 — Authlib (prior to 1.9.0) contains a signature verification bypass vulnerability. The JsonWebSignatur	1	pyproject.toml
HIGH	dep_checker	CVE found: CVE-2026-114605 in dnspython==2.8.0 — ### Impact A maliciously crafted DNS message may cause dns.name.from_wire_parser() to use excessive	1	pyproject.toml
HIGH	dep_checker	CVE found: CVE-2026-114615 in authlib==1.6.12 — ## Summary `OctKey.import_key()` carries the only guard that stops an asymmetric public key from be	1	pyproject.toml
HIGH	dep_checker	CVE found: CVE-2026-114616 in authlib==1.6.12 — Reporter: Cavan Loughran, Celvex Group Inc. Summary Authlib's symmetric (oct) key handling accepts	1	pyproject.toml

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	dep_checker	CVE found: CVE-2026-114618 in authlib==1.6.12 — ### Description ### Summary Authlib's default RFC 7523 JWT bearer grant leaves <code>`get_audiences()`</code> empty	1	pyproject.toml
HIGH	dep_checker	CVE found: CVE-2026-114614 in authlib==1.6.12 — ### Summary <code>`authlib.common.security.is_secure_transport()`</code> is used throughout Authlib to enforce th	1	pyproject.toml
HIGH	dep_checker	CVE found: PYSEC-2026-4320 in certifi==2025.6.15 — Certifi versions before 2026.10.18 include the <code>`emSign ECC Root CA - G3`</code> root certificate in their b	1	pyproject.toml
HIGH	dep_checker	CVE found: CVE-2026-114620 in authlib==1.6.12 — ### Summary Authlib's RFC 9101 (JAR) extension passes the attacker-controlled <code>`request_uri`</code> authori	1	pyproject.toml
HIGH	dep_checker	CVE found: CVE-2026-114617 in authlib==1.6.12 — ### Summary <code>`OpenIDMixin.parse_id_token()`</code> reads the <code>`nonce_supported`</code> claim from the ID token it i	1	pyproject.toml
HIGH	semgrep	Using variable interpolation <code>`\${{...}}`</code> with <code>`github`</code> context data in a <code>`run:`</code> step could allow an attacker to inject their own code into the runner. This would allow them to steal secrets and code. <code>`github`</code> context data can have arbitrary user input and should be treated as untrusted. Instead, use	2	/.github/workflows/release.yml:52
HIGH	semgrep	By not specifying a USER, a program in the container may run as 'root'. This is a security hazard. If an attacker can control a process running as root, they may have control over the container. Ensure that the last USER in a Dockerfile is a USER other than 'root'.	1	/docker/Dockerfile:48

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "token usage model=%s input=%d output=%d " "cache_write=%d cache_read=%d" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/src/seclab_taskflow_agent/_stream.py:134
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	7	/.github/workflows/codeql.yml:42
MEDIUM	bandit	Probable insecure usage of temp file/directory.	1	/release_tools/publish_docker.py:31
LOW	guarddog	Detects reading of environment variables (credential access, often contains secrets) [threat-runtime-environment-read]	2	/src/seclab_taskflow_agent/capi.py:176
LOW	bandit	Consider possible security implications associated with the subprocess module.	5	/src/seclab_taskflow_agent/shell_utils.py:7
LOW	bandit	Starting a process with a partial executable path	8	/release_tools/copy_files.py:53
LOW	bandit	subprocess call - check for execution of untrusted input.	12	/release_tools/copy_files.py:51
LOW	dep_checker	Loose version constraint: 'Jinja2>=3.1.0' — attacker could push malicious update	1	pyproject.toml

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'anthropic>=0.50,<1' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'github-copilot-sdk>=0.2.2,<0.3' — attacker could push malicious update	1	pyproject.toml

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 29 October 2026.