[Security Report] ArtiPACKED Vulnerability – GitHub Actions Credential Persistence (`artipacked`)

Critical **MervinPraison** published **GHSA-3959-6v5q-45q2** 3 days ago

Package

praisonai (pip)

Affected versions	Patched versions
< 4.5.140	>= 4.5.140

Description

While auditing the repository for GitHub Actions security, I discovered **multiple instances** of the **ArtiPACKED** vulnerability (credential persistence through GitHub Actions artifacts).

Affected files (summary):
Many workflows and actions under `.github/workflows/` and `.github/actions/` use `actions/checkout@v4` (and similar) **without** setting `persist-credentials: false`.

Specific examples flagged by zizmor include:

- `.github/actions/claude-issue-triage-action/action.yml`
- `.github/workflows/benchmark.yml`
- `.github/workflows/build-image.yml`
- `.github/workflows/claude.yml`
- `.github/workflows/docker-publish.yml`
- `.github/workflows/gemini-*.yml`
- `.github/workflows/praisonai-*.yml`
- `.github/workflows/release.yml`
- Most test workflows (`test-*.yml`), `python-publish.yml`, etc.

Total findings: zizmor reported several `artipacked` warnings across the repository.

What is ArtiPACKED?

ArtiPACKED is a known attack vector in GitHub Actions discovered by Palo Alto Networks Unit 42 in August 2024.

By default, `actions/checkout` writes the **`GITHUB_TOKEN`** (and sometimes `ACTIONS_RUNTIME_TOKEN`) into the `.git/config` file for credential persistence.
If any workflow later uploads an **artifact** (test results, build outputs, logs, workspace, etc.), the token can be included in the artifact.

Since this is a **public repository**, anyone with read access can download these artifacts and steal the token.

Potential Impact

If a malicious actor obtains the leaked token, they could:

- Push malicious code directly to the `main` branch or create malicious Pull Requests
- Poison releases, PyPI packages, and Docker images (**supply chain attack**)
- Steal other repository secrets (OpenAI, Anthropic, Gemini, Groq, Claude, PAT tokens, etc.)
- Compromise the entire PraisonAI project and affect all downstream users who `pip install praisonai` or use the Docker images
- Escalate further depending on the token's permissions (many workflows currently use broad/default permissions)

This type of issue has affected major organizations and open-source projects. A successful attack here would be a classic **supply chain compromise**.

References

- Official Research: ArtiPACKED: Hacking Giants Through a Race Condition in GitHub Actions Artifacts (Palo Alto Networks Unit 42, Aug 2024)
- News Coverage: GitHub Vulnerability 'ArtiPACKED' Exposes Repositories to Potential Takeover

Recommended Fix (Simple & Effective)

Add the following to **every** `actions/checkout` step:

```yaml
- name: Checkout repository
  uses: actions/checkout@v4
  with:
    persist-credentials: false   # ← This prevents credential leakage
    fetch-depth: 1               # Optional: also improves speed
```

Reporter: Jaisurya-me

Severity

Critical 9.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVE ID

CVE-2026-40313

Weaknesses

▶ CWE-829

Credits

 **jaisurya-me** Reporter