# PraisonAI: ArtiPACKED Vulnerability via GitHub Actions Credential Persistence

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-40313 |
| **State** | PUBLISHED |
| **Assigner** | GitHub_M |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-04-14 04:17:13 UTC |
| **Updated** | 2026-04-14 04:17:13 UTC |
| **Description** | PraisonAI is a multi-agent teams system. In versions 4.5.139 and below, the GitHub Actions workflows are vulnerable to Art |

## Risk And Classification

**Primary CVSS:** v3.1 9.1 CRITICAL from security-advisories@github.com

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

**EPSS:** 0.000290000 probability, percentile 0.082000000 (date 2026-04-15)

**Problem Types:** CWE-829 | CWE-829 CWE-829: Inclusion of Functionality from Untrusted Control Sphere

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | security-advisories@github.com | Secondary | 9.1 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N |
| 3.1 | CNA | DECLARED | 9.1 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

None

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

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | MervinPraison | PraisonAI | affected < 4.5.140 | Not specified |

## References

| Reference | Source | Link |
|---|---|---|
| thehackernews.com/2024/08/github-vulnerability-artipacked-exposes.html | security-advisories@github.com | thehackernews.com |
| github.com/MervinPraison/PraisonAI/security/advisories/GHSA-3959-6v5q-45q2 | security-advisories@github.com | github.com |
| unit42.paloaltonetworks.com/github-repo-artifacts-leak-tokens | security-advisories@github.com | unit42.paloaltonetworks. |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.