Critical RCE via `type: job` workflow YAML

Critical **MervinPraison** published **GHSA-vc46-vw85-3wvm** 4 days ago

Package

praisonai (pip)

Affected versions	Patched versions
<= 4.5.138	>= 4.5.139

praisonaiagents (pip)

<= 1.5.139	>= 1.5.140

Description

`praisonai workflow run <file.yaml>` loads untrusted YAML and if `type: job` executes steps through `JobWorkflowExecutor` in job_workflow.py.

This supports:

- `run:` → shell command execution via `subprocess.run()`
- `script:` → inline Python execution via `exec()`
- `python:` → arbitrary Python script execution

A malicious YAML file can execute arbitrary host commands.

Affected Code

- workflow.py → `action_run()`
- job_workflow.py → `_exec_shell()`, `_exec_inline_python()`, `_exec_python_script()`

PoC

Create `exploit.yaml`:

```yaml
type: job
name: exploit
steps:
  - name: write-file
    run: python -c "open('pwned.txt','w').write('owned')"
```

Run:

```
praisonai workflow run exploit.yaml
```

Reproduction Steps

1. Save the YAML above as `exploit.yaml`.
2. Execute `praisonai workflow run exploit.yaml`.
3. Confirm `pwned.txt` appears in the working directory.

Impact

Remote or local attacker-supplied workflow YAML can execute arbitrary host commands and code, enabling full system compromise in CI or shared deployment contexts.

Reporter: Lakshmikanthan K (letchupkt)

Severity

Critical 9.8 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-40288

Weaknesses

- CWE-78
- CWE-94

Credits

l3tchupkt Reporter