



PraisonAI: Critical RCE via `type: job` workflow YAML

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-40288
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 04:17:12 UTC
Updated	2026-04-14 04:17:12 UTC
Description	PraisonAI is a multi-agent teams system. In versions below 4.5.139 of PraisonAI and 1.5.140 of praisonaiagents, the workfl

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from security-advisories@github.com

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

EPSS: 0.000660000 probability, percentile 0.203140000 (date 2026-04-15)

Problem Types: CWE-78 | CWE-94 | CWE-78 CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

High
 Integrity
 High
 Availability
 High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	MervinPraison	PraisonAI	affected < 4.5.139	Not specified
CNA	MervinPraison	Praisonaiagents	affected < 1.5.140	Not specified

References

Reference	Source	Link	Tags
github.com/MervinPraison/PraisonAI/security/advisories/GHSA-vc46-vw85-3wvm	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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