PraisonAI has RCE via Automatic tools.py Import

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

Summary

CVE	CVE-2026-40287
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 04:17:11 UTC
Updated	2026-04-14 14:16:14 UTC
Description	PraisonAI is a multi-agent teams system. Versions 4.5.138 and below are vulnerable to arbitrary code execution through au

Risk And Classification

Primary CVSS: v3.1 8.4 HIGH from security-advisories@github.com

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

EPSS: 0.000230000 probability, percentile 0.062200000 (date 2026-04-15)

Problem Types: CWE-94 | CWE-426 | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection') | CWE-426 CWE-426: Untrusted Search Path

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:L/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
github.com/MervinPraison/PraisonAI/security/advisories/GHSA-g985-wjh9-qxxc	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
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.