



# PraisonAI has RCE via Automatic tools.py Import

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

## Summary

<b>CVE</b>	CVE-2026-40287
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-14 04:17:11 UTC
<b>Updated</b>	2026-04-14 14:16:14 UTC
<b>Description</b>	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

Integrity

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	<a href="#">MervinPraison</a>	<a href="#">PraisonAI</a>	affected < 4.5.139	Not specified
CNA	<a href="#">MervinPraison</a>	<a href="#">Praisonaiagents</a>	affected < 1.5.140	Not specified

### References

Reference	Source	Link
<a href="https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-g985-wjh9-qxxc">github.com/MervinPraison/PraisonAI/security/advisories/GHSA-g985-wjh9-qxxc</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://github.com">github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)