PraisonAI MCP `tools/call` path-traversal and RCE via Python `.pth` injection

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

Summary

CVE	CVE-2026-44336
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 14:16:46 UTC
Updated	2026-05-08 15:53:24 UTC
Description	PraisonAI is a multi-agent teams system. Prior to version 4.6.34, PraisonAI's MCP (Model Context Protocol) server (praisor

Risk And Classification

Primary CVSS: v4.0 9.4 CRITICAL from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-20 | CWE-22 | CWE-94 | CWE-829 | CWE-913 | CWE-20 CWE-20: Improper Input Validation | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection') | CWE-829 CWE-829: Inclusion of Functionality from Untrusted Control Sphere | CWE-913 CWE-913: Improper Control of Dynamically-Managed Code Resources

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	9.4	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H
4.0	CNA	DECLARED	9.4	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	MervinPraison	PraisonAI	affected < 4.6.34	Not specified

References

Reference	Source	Link	Tags
github.com/MervinPraison/PraisonAI/security/advisories/GHSA-9mqq-jqxf-grvw	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report