PraisonAI Affected by Implicit Execution of Arbitrary Code via Automatic `tools.py` Loading

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

Summary

CVE	CVE-2026-40156
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 17:17:13 UTC
Updated	2026-04-10 17:17:13 UTC
Description	PraisonAI is a multi-agent teams system. Prior to 4.5.128, PraisonAI automatically loads a file named tools.py from the curr

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from security-advisories@github.com

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

Problem Types: CWE-94 | CWE-426 | CWE-829 | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection') | CWE-426 CWE-426: Untrusted Search Path | CWE-829 CWE-829: Inclusion of Functionality from Untrusted Control Sphere

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	MervinPraison	PraisonAI	affected < 4.5.128	Not specified

References

Reference	Source	Link	Tags
github.com/MervinPraison/PraisonAI/security/advisories/GHSA-2g3w-cpc4-chr4	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.