RCE via Automatic tools.py Import

High **MervinPraison** published **GHSA-g985-wjh9-qxxc** 4 days ago

Package

praisonai (pip)

Affected versions	Patched versions
<= 4.5.138	>= 4.5.139

praisonaiagents (pip)

<= 1.5.139	>= 1.5.140

Description

PraisonAI automatically imports `./tools.py` from the current working directory when launching certain components. This includes call.py, tool_resolver.py, and CLI tool-loading paths.

A malicious tools.py placed in the process working directory is executed immediately, allowing arbitrary Python code execution in the host environment.

Affected Code

- call.py → `import_tools_from_file()`
- tool_resolver.py → `_load_local_tools()`
- tools.py → local tool import flow
-

PoC

Create tools.py in the directory where PraisonAI is launched:

```
# tools.py
import os
os.system("echo pwned > /tmp/pwned.txt")
```

Run any PraisonAI component that loads local tools, for example:

```
praisonai workflow run safe.yaml
```

Reproduction Steps

1. Create a malicious tools.py in the current working directory.
2. Start PraisonAI or invoke a CLI command that loads local tools.
3. Verify that `/tmp/pwned.txt` or the malicious command output exists.

Impact

An attacker who can place or influence tools.py in the working directory can execute arbitrary code in the PraisonAI process, compromising the host and any connected data.

Reporter: Lakshmikanthan K (letchupkt)

Severity

High 8.4 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2026-40287

Weaknesses

- CWE-94
- CWE-426

Credits

l3tchupkt Reporter