CWD-Based Module Hijacking via sys.path Manipulation in pymanager Alias Wrapper

Moderate **zooba** published **GHSA-jr5x-hgm4-rrm6** yesterday

Package

Python install manager

Affected versions	Patched versions
26.0	26.1

Description

Summary

The alias wrapper generated by `pymanager` modifies `sys.path[0]` to an empty string (`""`).
In Python, this causes the interpreter to prioritize the current working directory (CWD) during module resolution.

As a result, if a user executes a pymanager-generated command (e.g., `pip`, `pytest`) from an attacker-controlled directory, a malicious module in that directory can be imported and executed instead of the intended package.

Impact

- Arbitrary local code execution
- No elevated privileges required
- Triggered through normal developer workflows
- Affects any command executed via pymanager alias wrappers

This issue is particularly dangerous in scenarios such as:

- Cloned repositories from untrusted sources

- Extracted archives
- Shared development environments

Root Cause

The issue originates from the following logic in `src/manage/aliasutils.py`:

```
sys.path[0] = ""
```

In Python, an empty string in `sys.path` represents the current working directory.
This effectively prioritizes untrusted directories during module import resolution.

Proof of Concept

```
mkdir exploit_repo
cd exploit_repo

echo print("[!] CWD HIJACK SUCCESSFUL") > requests.py

echo import sys > poc.py
echo sys.path[0] = "" >> poc.py
echo import requests >> poc.py

python poc.py
```

Observed Result

```
[!] CWD HIJACK SUCCESSFUL
```

The attacker-controlled module (requests.py) is imported from the current working directory instead of the legitimate package, resulting in arbitrary code execution.

Severity

Moderate 5.6 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Local
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	None
User interaction	Active

Vulnerable System Impact Metrics

Confidentiality	None
Integrity	High
Availability	None

Subsequent System Impact Metrics

Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:A/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N

CVE ID

CVE-2026-5271

Weaknesses

▶ CWE-426

Credits

l3tchupkt Reporter