



# Possible to hijack modules in current working directory

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

## Summary

<b>CVE</b>	CVE-2026-5271
<b>State</b>	PUBLISHED
<b>Assigner</b>	PSF
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-01 14:16:59 UTC
<b>Updated</b>	2026-04-02 00:16:24 UTC
<b>Description</b>	pymanager included the current working directory in sys.path meaning modules could be shadowed by modules in the current

## Risk And Classification

**Primary CVSS:** v4.0 5.6 MEDIUM from cna@python.org

**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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000140000 probability, percentile 0.027040000 (date 2026-04-02)

**Problem Types:** CWE-427 | CWE-427 CWE-427 Uncontrolled Search Path Element

Version	Source	Type	Score	Severity	Vector
4.0	cna@python.org	Secondary	5.6	MEDIUM	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/E:X/C...
4.0	CNA	CVSS	5.6	MEDIUM	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

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Active

Confidentiality

None

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX: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	<a href="#">Python Software Foundation</a>	<a href="#">Pymanager</a>	affected 26.0 26.1 python	Not specified

### References

Reference	Source	Link
<a href="https://github.com/python/pymanager/security/advisories/GHSA-jr5x-hgm4-rrm6">github.com/python/pymanager/security/advisories/GHSA-jr5x-hgm4-rrm6</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://github.com">github.com</a>
<a href="https://www.openwall.com/lists/oss-security/2026/04/01/5">www.openwall.com/lists/oss-security/2026/04/01/5</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://www.openwall.com">www.openwall.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>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Steve Dower (en)

**CNA:** LAKSHMIKANTHAN K (en)

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](#).

