



# pip self-update functionality can import newly installed modules after wheel installation

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-6357
<b>State</b>	PUBLISHED
<b>Assigner</b>	PSF
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-27 15:16:20 UTC
<b>Updated</b>	2026-04-27 23:16:03 UTC
<b>Description</b>	pip prior to version 26.1 would run self-update check functionality after installing wheel files which required importing well-kr

## Risk And Classification

**Primary CVSS:** v4.0 5.3 MEDIUM from cna@python.org

CVSS:4.0/AV:L/AC:L/AT:P/PR:H/UI:A/VC:H/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

**Problem Types:** CWE-829 | CWE-829 CWE-829 Inclusion of Functionality from Untrusted Control Sphere

Version	Source	Type	Score	Severity	Vector
4.0	cna@python.org	Secondary	5.3	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:H/UI:A/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:H/UI:A/VC:H/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

High

User Interaction

Active

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:P/PR:H/UI:A/VC:H/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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pip Maintainers	Pip	affected 26.1 python	Not specified

### References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/04/27/7	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>	
github.com/pypa/pip/pull/13923	cna@python.org	<a href="https://github.com">github.com</a>	
ichard26.github.io/blog/2026/04/whats-new-in-pip-26.1	cna@python.org	<a href="https://ichard26.github.io">ichard26.github.io</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** Damian Shaw (en)

**CNA:** Damian Shaw (en)

**CNA:** Richard Si (en)

**CNA:** Seth Larson (en)

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

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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)