SourcelessFileLoader does not use io.open_code()

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

Summary

CVE	CVE-2026-2297
State	PUBLISHED
Assigner	PSF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-04 23:16:10 UTC
Updated	2026-05-01 16:16:30 UTC
Description	The import hook in CPython that handles legacy *.pyc files (SourcelessFileLoader) is incorrectly handled in FileLoader (a ba

Risk And Classification

Primary CVSS: v4.0 5.7 MEDIUM from cna@python.org

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000180000 probability, percentile 0.047230000 (date 2026-05-05)

Problem Types: CWE-668 | CWE-668 CWE-668 Exposure of Resource to Wrong Sphere

Version	Source	Type	Score	Severity	Vector
4.0	cna@python.org	Secondary	5.7	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	5.7	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/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

Low

User Interaction

None

Confidentiality

None

ntegrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/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/MSC: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	Python Software Foundation	CPython	affected 3.13.13 python	Not specified
CNA	Python Software Foundation	CPython	affected 3.14.0 3.14.4 python	Not specified
CNA	Python Software Foundation	CPython	affected 3.15.0a1 3.15.0a7 python	Not specified

References

Reference	Source	Link
github.com/python/cpython/commit/482d6f8bdba9da3725d272e8bb4a2d25fb6a603e	cna@python.org	github.c
github.com/python/cpython/commit/e58e9802b9bec5cdbf48fc9bf1da5f4fda482e86	cna@python.org	github.c
github.com/python/cpython/issues/145506	cna@python.org	github.c
github.com/python/cpython/commit/69ddd9bb2cc4bd69b1565647c18659c6a789ccd9	cna@python.org	github.c
www.openwall.com/lists/oss-security/2026/03/05/6	af854a3a-2127-422b-91ae-364da2661108	www.op
github.com/python/cpython/pull/145507	cna@python.org	github.c
github.com/python/cpython/commit/876858c9f65d9ab656c7fa639f268ce7856d89dd	cna@python.org	github.c
github.com/python/cpython/commit/a51b1b512de1d56b3714b65628a2eae2b07e535e	cna@python.org	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

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 registred 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**