

python / cpython Public

[Code](#) [Issues](#) 5k+ [Pull requests](#) 2.2k [Actions](#) [Projects](#) [Security and q](#)

New issue



[CVE-2026-2297] SourcelessFileLoader does not use io.open_code() #145506

Open

Assignees



Labels

3.10

3.11

3.12

3.13

3.14

3.15

stdlib

topic-importlib

type-security



zooba opened on Mar 4 · edited by StanFromIreland

Edits ▾

Member



The import hook in CPython that handles legacy `*.pyc` files (`SourcelessFileLoader`) is incorrectly handled in `FileLoader` (a base class) and so does not use `io.open_code()` to read the `.pyc` files. This means anyone who has hooked `io.open_code()` to do validation will be bypassed.

```
class FileLoader:
    ...
    def get_data(self, path):
        """Return the data from path as raw bytes."""
        if isinstance(self, (SourceLoader, ExtensionFileLoader)):
            with _io.open_code(str(path)) as file:
                return file.read()
        else:
            with _io.FileIO(path, 'r') as file:
                return file.read()
```



The `SourcelessFileLoader` subclass doesn't get caught by the `isinstance()` call, because it's neither of the classes listed. It should have `SourcelessFileLoader` added to the tuple.

This import hook is enabled by default, though the `SourceFileLoader` is higher priority, and it does correctly use `io.open_code()`.

Legacy `*.pyc` files may be used if a user has precompiled their sources and then removed the source code. Under default configuration, it will never be used.

I didn't find any GitHub results that were actual uses, though I expected they'd all be private forks anyway, so I think the impact is going to be very low. The fix is trivial, but this is also easily exploitable if it's the sole security measure - for any module that's going to be imported, put its `.pyc` earlier on the search path and that'll be picked first without verification.

(This has already been reviewed by the PSRT and assigned [CVE-2026-2297](#). The issue is just to get the fix merged.)



Linked PRs


- [gh-145506: Fixes CVE-2026-2297 by ensuring SourcelessFileLoader uses io.open_code #145507](#)
- [\[3.14\] gh-145506: Fixes CVE-2026-2297 by ensuring SourcelessFileLoader uses io.open_code \(GH-145507\) #145512](#)
- [\[3.13\] gh-145506: Fixes CVE-2026-2297 by ensuring SourcelessFileLoader uses io.open_code \(GH-145507\) #145513](#)
- [\[3.12\] gh-145506: Fixes CVE-2026-2297 by ensuring SourcelessFileLoader uses io.open_code \(GH-145507\) #145514](#)
- [\[3.11\] gh-145506: Fixes CVE-2026-2297 by ensuring SourcelessFileLoader uses io.open_code \(GH-145507\) #145515](#)
- [\[3.10\] gh-145506: Fixes CVE-2026-2297 by ensuring SourcelessFileLoader uses io.open_code \(GH-145507\) #145516](#)



 **zooba** self-assigned this [on Mar 4](#)

 **zooba** added [type-security](#) [3.11](#) [3.10](#) [topic-importlib](#) [3.12](#) [3.13](#) [3.14](#) [3.15](#) [on Mar 4](#)

 **StanFromIreland** added [stdlib](#) [on Mar 4](#)

 **zooba** added a commit that references this issue [on Mar 4](#)
[pythongh-145506](#): Fixes [CVE-2026-2297](#) by ensuring SourcelessFileLoader.  73f91c3

 **bedevere-app** mentioned this [on Mar 4](#)
[gh-145506: Fixes CVE-2026-2297 by ensuring SourcelessFileLoader uses io.open_code #145507](#)

 **zooba** added a commit that references this issue [on Mar 4](#)
[gh-145506](#): Fixes [CVE-2026-2297](#) by ensuring SourcelessFileLoader uses `.`  [Verified](#) a51b1b5

 **miss-islington** added 2 commits that reference this issue [on Mar 4](#)

[pythongh-145506](#): Fixes [CVE-2026-2297](#) by ensuring SourcelessFileLoader.  4ce6b1b

[pythongh-145506](#): Fixes [CVE-2026-2297](#) by ensuring SourcelessFileLoader.  d8a2f55

10 remaining items

Load more



Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Metadata

Assignees



Labels

- 3.10
- 3.11
- 3.12
- 3.13
- 3.14
- 3.15
- stdlib
- topic-importlib
- type-security

Projects

No projects


Milestone

No milestone

Relationships

None yet

Development

 Code with agent mode

No branches or pull requests

Participants



