

python / cpython Public

[Code](#) [Issues](#) 5k+ [Pull requests](#) 2.1k [Actions](#) [Projects](#) [Security and q](#)

New issue



Multiple tarfile extraction filter bypasses (`filter="tar" / filter="data"`) #135034

Closed

Labels

triaged

type-security



sethmlarson opened on Jun 2, 2025 · edited by encukou

Edits ▾

Contributor



Bug description:

Public issue for fixing [CVE-2025-4517](#), [CVE-2025-4330](#), [CVE-2025-4138](#), and [CVE-2024-12718](#). [See full advisory on security-announce](#).

[edit @encukou]: Also addresses [CVE-2025-4435](#). Sorry for leaving that out of the commit messages.

CPython versions tested on:

CPython main branch

Operating systems tested on:

No response

Linked PRs

- [gh-135034: Normalize link targets in tarfile, add `os.path.realpath\(strict='allow_missing'\)` #135037](#)
- [\[3.13\] gh-135034: Normalize link targets in tarfile, add `os.path.realpath\(strict='allow_missing'\)` \(GH-135037\) #135064](#)
- [\[3.14\] gh-135034: Normalize link targets in tarfile, add `os.path.realpath\(strict='allow_missing'\)` \(gh-135037\) #135065](#)
- [\[3.12\] gh-135034: Normalize link targets in tarfile, add `os.path.realpath\(strict='allow_missing'\)` \(GH-135037\) #135066](#)

- [\[3.11\] gh-135034: Normalize link targets in tarfile, add `os.path.realpath\(strict='allow_missing'\)` \(GH-135037\) #135068](#)
- [\[3.10\] gh-135034: Normalize link targets in tarfile, add `os.path.realpath\(strict='allow_missing'\)` \(GH-135037\) #135070](#)
- [\[3.9\] gh-135034: Normalize link targets in tarfile, add `os.path.realpath\(strict='allow_missing'\)` \(GH-135037\) #135084](#)
- [\[3.12\] gh-135034: Remove test_realpath_permission #135093](#)



sethmlarson added **type-security** on Jun 2, 2025

picnixz added **triaged** on Jun 2, 2025

ambv mentioned this on Jun 2, 2025

[\[3.9\] bpo-43757: Make pathlib use os.path.realpath\(\) to resolve symlinks in a path \(GH-25264\) #135035](#)

ambv added a commit that references this issue on Jun 2, 2025

[pythongh-135034](#): Normalize link targets in tarfile, add ``os.path.real`. 0c16f5f

bedevere-app mentioned this on Jun 2, 2025

[gh-135034: Normalize link targets in tarfile, add `os.path.realpath\(strict='allow_missing'\)` #135037](#)

Yhg1s added 2 commits that reference this issue on Jun 3, 2025

[gh-135034](#): Normalize link targets in tarfile, add ``os.path.realpath(s`. 3612d8f

[\[3.13\] pythongh-135034: Normalize link targets in tarfile, add ``os.pa`. 2637f45](#)


bedevere-app mentioned this on Jun 3, 2025



[\[3.13\] gh-135034: Normalize link targets in tarfile, add `os.path.realpath\(strict='allow_missing'\)` \(GH-135037\) #135064](#)

ambv added a commit that references this issue on Jun 3, 2025

[pythongh-135034](#): Normalize link targets in tarfile, add ``os.path.real`. 553d40f


  **bedevere-app** mentioned this [on Jun 3, 2025](#)



 [\[3.14\] gh-135034: Normalize link targets in tarfile, add os.path.realpath\(strict='allow_missing'\) \(gh-135037\) #135065](#)

  **Yhg1s** added a commit that references this issue [on Jun 3, 2025](#)

[3.12] [pythongh-135034](#): Normalize link targets in tarfile, add `os.pa.  c358142


  **bedevere-app** mentioned this [on Jun 3, 2025](#)

 [\[3.12\] gh-135034: Normalize link targets in tarfile, add os.path.realpath\(strict='allow_missing'\) \(GH-135037\) #135066](#)

  **Yhg1s** added a commit that references this issue [on Jun 3, 2025](#)

[3.11] [pythongh-135034](#): Normalize link targets in tarfile, add `os.pa.  371b4ea

  **bedevere-app** mentioned this [on Jun 3, 2025](#)

 [\[3.11\] gh-135034: Normalize link targets in tarfile, add os.path.realpath\(strict='allow_missing'\) \(GH-135037\) #135068](#)

  **Yhg1s** added a commit that references this issue [on Jun 3, 2025](#)

[3.10] [pythongh-135034](#): Normalize link targets in tarfile, add `os.pa.  4d959a0

910 remaining items



Load more



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

Metadata

Assignees

No one assigned

Labels

triaged

type-security

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants

