

python / cpython Public

<> Code Issues 5k+ Pull requests 2.2k Actions Projects Security and q

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

Merged Yhg1s merged 20 commits into python:main from ambv:gh-135034 on Jun 3, 2025

Conversation 23 Commits 20 Checks 57 Files changed 11



ambv commented on Jun 2, 2025 • edited by encukou

Contributor

Addresses CVEs 2024-12718, 2025-4138, 2025-4330, and 2025-4517.

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

Co-authored-by: Petr Viktorin encukou@gmail.com

Signed-off-by: Łukasz Langa lukasz@langa.pl

- Issue: [Multiple tarfile extraction filter bypasses \(filter="tar" / filter="data" \) #135034](#)

Documentation preview <https://cpython-previews--135037.org.readthedocs.build/>

pythongh-135034: Normalize link targets in tarfile, add `os.path.real... 0c16f5f

ambv requested a review from ethanfurman as a code owner 11 months ago


bedevere-app Bot added the awaiting core review label on Jun 2, 2025

 **bedevere-app** (Bot) mentioned this pull request [on Jun 2, 2025](#)

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

 Closed

 **ambv** and others added 2 commits [11 months ago](#)


  [Fix lint](#)  [335921b](#)

  [Add blurb](#)  [fcefa72](#)


serhiy-storchaka commented [on Jun 2, 2025](#)

Member

See also [#71189](#).

  [Fix test_tarfile on WASI](#)  [9c275a7](#)

 **ambv** [force-pushed](#) the `gh-135034` branch from `d25f924` to `9c275a7` [11 months ago](#) Compare

  [Remove spurious line](#)  [b59eaaa](#)

 **AA-Turner** reviewed [on Jun 2, 2025](#)

[View reviewed changes](#)

> `Lib/test/test_tarfile.py` Outdated

 Show resolved

 **ambv** and others added 3 commits [11 months ago](#)

  [Fix invalid parent directory unwinding in test](#)  [fd5ba13](#)

  [Make tests more chatty](#)  [aeebdc8](#)

  [Use a better skip](#)  [f5544e6](#)

 **encukou** reviewed [on Jun 2, 2025](#)

View reviewed changes

> Lib/test/test_tarfile.py Outdated

 Show resolved

 **encukou** reviewed [on Jun 2, 2025](#)

View reviewed changes

> Lib/test/test_ntpath.py Outdated

 Show resolved

encukou commented [on Jun 2, 2025](#)

Member

See also [#71189](#).

To align with this, there'd be a `ntpath.ALLOW_MISSING` singleton rather than an `'allow_missing'` string. That's possible, of course. It can catch typos. But I don't think it's worth having to import an extra name.



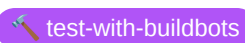
 **ambv** and others added 2 commits [11 months ago](#)

  [Work around Windows test failures](#)



 [3c5ed15](#)

  [Add ERROR_ACCESS_DENIED](#)

 [5af66c6](#)

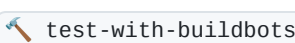
  **encukou** added the  label [on Jun 2, 2025](#)

bedevere-bot commented [on Jun 2, 2025](#)

 New build scheduled with the buildbot fleet by [@encukou](#) for commit [5af66c6](#) 

Results will be shown at:

<https://buildbot.python.org/all/#/grid?branch=refs%2Fpull%2F135037%2Fmerge>

If you want to schedule another build, you need to add the  label again.

 **bedevere-bot** removed the  label on [Jun 2, 2025](#)

 **encukou** and others added 7 commits [11 months ago](#)

  [Switch to singleton](#) ...  [a124c42](#)

  [Add ENAMETOOLONG to expected failures. And an extra subTest.](#)  [5bf4a48](#)


  [Discard more special files](#)  [3b54acd](#)

  [Use shorter names on Android](#)  [7ff96a2](#)

  [Fix docs warning](#)  [f845343](#)

  [Attempt to restore ntpath test](#)  [fd2013a](#)

  [Revert "Attempt to restore ntpath test"](#) ...  [f8f2786](#)

 **encukou** added the  label on [Jun 3, 2025](#)

1710 hidden items

[Load more...](#)

 This was referenced 2 weeks ago

[Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415581](#) [RADAR-base/radar-helm-charts#9022](#)

 Closed

[Use of Incorrectly-Resolved Name or Reference SNYK-RHEL9-PYTHON3-10415440](#) [RADAR-base/radar-helm-charts#9023](#)

 Closed

[Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415830](#) [RADAR-base/radar-helm-charts#9024](#)

 Closed

[Directory Traversal SNYK-RHEL9-PYTHON3-10415579](#) [RADAR-base/radar-helm-charts#9025](#)

 Closed

Directory Traversal SNYK-RHEL9-PYTHON3-10415856 [RADAR-base/radar-helm-charts#9027](#)

 Closed

Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10409389 [RADAR-base/radar-helm-charts#9031](#)

 Closed

Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415372 [RADAR-base/radar-helm-charts#9032](#)

 Closed

Use of Incorrectly-Resolved Name or Reference SNYK-RHEL9-PYTHON3LIBS-10415418 [RADAR-base/radar-helm-charts#9033](#)

 Closed

Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415581 [RADAR-base/radar-helm-charts#9034](#)

 Closed

Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415830 [RADAR-base/radar-helm-charts#9035](#)

 Closed

Directory Traversal SNYK-RHEL9-PYTHON3-10409385 [RADAR-base/radar-helm-charts#9180](#)

 Open

Directory Traversal SNYK-RHEL9-PYTHON3-10415394 [RADAR-base/radar-helm-charts#9182](#)

 Open

Use of Incorrectly-Resolved Name or Reference SNYK-RHEL9-PYTHON3-10415440 [RADAR-base/radar-helm-charts#9185](#)

 Open

Directory Traversal SNYK-RHEL9-PYTHON3-10415579 [RADAR-base/radar-helm-charts#9186](#)

 Open

Directory Traversal SNYK-RHEL9-PYTHON3-10409385 [RADAR-base/radar-helm-charts#9187](#)



Directory Traversal SNYK-RHEL9-PYTHON3-10415856 [RADAR-base/radar-helm-charts#9188](#)



Directory Traversal SNYK-RHEL9-PYTHON3-10415394 [RADAR-base/radar-helm-charts#9189](#)



Use of Incorrectly-Resolved Name or Reference SNYK-RHEL9-PYTHON3-10415440 [RADAR-base/radar-helm-charts#9191](#)



Directory Traversal SNYK-RHEL9-PYTHON3-10415579 [RADAR-base/radar-helm-charts#9193](#)



Directory Traversal SNYK-RHEL9-PYTHON3-10415856 [RADAR-base/radar-helm-charts#9195](#)



Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10409389 [RADAR-base/radar-helm-charts#9197](#)



Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415372 [RADAR-base/radar-helm-charts#9199](#)



Use of Incorrectly-Resolved Name or Reference SNYK-RHEL9-PYTHON3LIBS-10415418 [RADAR-base/radar-helm-charts#9201](#)



Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10409389 [RADAR-base/radar-helm-charts#9202](#)



Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415581 [RADAR-base/radar-helm-charts#9203](#)



Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415372 [RADAR-base/radar-helm-charts#9204](#)



Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415830 [RADAR-base/radar-helm-charts#9205](#)



Use of Incorrectly-Resolved Name or Reference SNYK-RHEL9-PYTHON3LIBS-10415418 [RADAR-base/radar-helm-charts#9206](#)



This was referenced 5 days ago

Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415581 [RADAR-base/radar-helm-charts#9208](#)



Directory Traversal SNYK-RHEL9-PYTHON3LIBS-10415830 [RADAR-base/radar-helm-charts#9210](#)



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

Reviewers

encukou

AA-Turner

ethanfurman



Assignees

Yhg1s

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

7 participants

