gh-130577: tarfile now validates archives to ensure member offsets are non-negative #137027

Merged **ethanfurman** merged 3 commits into `python:main` from `aeurielesn:gh-130577` on Jul 28, 2025

Conversation 18 Commits 3 Checks 63 Files changed 3

aeurielesn commented on Jul 22, 2025 • edited by github-actions Bot — Contributor

- Issue: `tarfile.StreamError: seeking backwards is not allowed` due to unskipped block with bad checksum #130577

📚 Documentation preview 📚: https://cpython-previews--137027.org.readthedocs.build/

`pythongh-130577: tarfile now validates archives to ensure member offs…` ··· ✓ `235f9d4`

aeurielesn requested a review from **ethanfurman** as a code owner 9 months ago

bedevere-app Bot added the awaiting review label on Jul 22, 2025

bedevere-app Bot mentioned this pull request on Jul 22, 2025

`tarfile.StreamError: seeking backwards is not allowed` due to unskipped block with bad checksum #130577

Closed

ethanfurman approved these changes on Jul 23, 2025

View reviewed changes

bedevere-app Bot added awaiting merge and removed awaiting review labels on Jul 23, 2025

Typo 04fd085

gpshead approved these changes on Jul 25, 2025

View reviewed changes

gpshead left a comment — Member

It's rather sad that the number format used within tar files even explicitly allows a way to express negative values. is there even a use case for that in the file format(s)?

gpshead added needs backport to 3.9 needs backport to 3.10 needs backport to 3.11 needs backport to 3.12 needs backport to 3.13 needs backport to 3.14 and removed needs backport to 3.9 needs backport to 3.10 needs backport to 3.11 needs backport to 3.12 needs backport to 3.13 labels on Jul 25, 2025

gpshead commented on Jul 25, 2025 • edited — Member

Please cherry pick this commit to your branch (mispaste fixed): `aa57b01`

we don't want a whatsnew entry for this; whats new is for major features not bugfixes. a whatsnew entry makes backporting a chore (thus me removing the auto-backport labels for now)

(github is refusing to let me push changes to your branch. Please *always* allow maintainers to push edits to PR branches.)

👍 1

gpshead commented on Jul 25, 2025 — Member

(corrected mispasted commit link above)

gpshead self-assigned this on Jul 25, 2025

 `move credit to NEWS, and remove the whatsnew entry (painful for backp…` ··· ✓ `6d79444`

aeurielesn commented on Jul 26, 2025 Contributor Author

I enabled the allow edits to avoid any further issues and I cherry-picked the commit from your personal fork.

❤️ 1

aeurielesn commented on Jul 26, 2025 Contributor Author

By the way, thanks for the clarifications on the process 👍

❤️ 1

 **gpshead** added needs backport to 3.9 needs backport to 3.10 needs backport to 3.11 needs backport to 3.12 labels on Jul 27, 2025

705 hidden items

Load more…

This was referenced on Aug 19, 2025

CVE-2025-8194 ministryofjustice/hmpps-probation-integration-services#5392

Closed

Deps: Bump the github-actions group with 2 updates greenbone/gvm-tools#1245

Merged

Agent-Hellboy pushed a commit to Agent-Hellboy/cpython that referenced this pull request on Aug 19, 2025

 `pythongh-130577: tarfile now validates archives to ensure member offs…` ··· `ab78453`

github-actions Bot mentioned this pull request on Aug 19, 2025

Change: move delete and modify functions to asset files greenbone/gvmd#2519

Merged

pablogsal pushed a commit that referenced this pull request on Aug 19, 2025

 `[3.11] gh-130577: tarfile now validates archives to ensure member off…` ··· ✕ `b4ec174`

bedevere-bot commented on Aug 19, 2025

⚠️⚠️⚠️ Buildbot failure ⚠️⚠️⚠️

Hi! The buildbot **s390x RHEL9 Refleaks 3.11** (tier-3) has failed when building commit `b4ec174`.

What do you need to do:

1. Don't panic.
2. Check the buildbot page in the devguide if you don't know what the buildbots are or how they work.
3. Go to the page of the buildbot that failed (https://buildbot.python.org/#/builders/1586/builds/63) and take a look at the build logs.
4. Check if the failure is related to this commit (`b4ec174`) or if it is a false positive.
5. If the failure is related to this commit, please, reflect that on the issue and make a new Pull Request with a fix.

You can take a look at the buildbot page here:

https://buildbot.python.org/#/builders/1586/builds/63

Failed tests:

- test_typing

Test leaking resources:

- test_typing: memory blocks

Summary of the results of the build (if available):

==

▶ Click to see traceback logs

This was referenced on Aug 20, 2025

Change: move report_host_* to the asset files greenbone/gvmd#2520

Merged

Fix CI greenbone/ospd-openvas#1054

Merged

Fix: Add missing and amend G_LOG_DOMAIN #defines greenbone/gvmd#2521

Merged

Add scan agent config support greenbone/gvmd#2522

Merged

Change: move rest of Assets section out of manage_sql.c greenbone/gvmd#2523

Merged

Fix result and report id fetching in monthly-report script greenbone/gvm-tools#1246

Merged

Change: move host_notice into asset files greenbone/gvmd#2524

Merged

Deps: Bump the python-packages group with 5 updates greenbone/greenbone-feed-sync#294

Merged

Add: Ability to get, modify and verify scanners of type 'container-image' greenbone/gvmd#2525

Merged

Fix: Behavior with ENABLE_AGENTS feature flag greenbone/gvmd#2526

Merged

dimaqq commented on Aug 26, 2025 Contributor

I wonder if similar treatment is needed for e.g. `offset/numbytes` in the `TNUYPE_SPARSE` processing arc. And perhaps `origsize` too?

This was referenced on Aug 27, 2025

Remove separate default openvasd scanner greenbone/gvmd#2527

Merged

Fix: handle 0 ports case in get_port_lists filter greenbone/gvmd#2528

Merged

Fix: Address warnings when building with the gcc version in Debian testing greenbone/gvmd#2529

Merged

Add: Filter settings for compliance types greenbone/gvmd#2530

Merged

picnixz mentioned this pull request on Aug 28, 2025

Guard against negative offset/length values in tarfile's GNU sparse extraction #137396

Open

This was referenced on Aug 28, 2025

Fix: Add check if UUID exists when creating config greenbone/gvmd#2531

Merged

Change: Update openvasd to use the generic http scanner library greenbone/gvmd#2532

Merged

pablogsal pushed a commit that referenced this pull request on Sep 2, 2025

`[3.10] gh-130577: tarfile now validates archives to ensure member off…` ··· `57f5981`

kumaraditya303 pushed a commit to miss-islington/cpython that referenced this pull request on Sep 9, 2025

`[3.14] pythongh-130577: tarfile now validates archives to ensure memb…` ··· `7057dcb`

ambv pushed a commit that referenced this pull request on Sep 13, 2025

`[3.9] gh-130577: tarfile now validates archives to ensure member offs…` ··· `73f03e4`

hroncok pushed a commit to fedora-python/cpython that referenced this pull request on Feb 3

`00467: tarfile CVE-2025-8194` ··· `31cf6cf`

This was referenced on Mar 13

CVE-2025-8194: debian package libpython3.13-stdlib-3.13.5-2 All-Hands-AI/OpenHands-Cloud#347

Closed

CVE-2025-8194: debian package python3.13-minimal-3.13.5-2 All-Hands-AI/OpenHands-Cloud#352

Closed

Reviewers

gpshead ✓

ethanfurman ✓

sethmlarson ✓

Assignees

gpshead

Labels

type-security

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

6 participants