» Issue39017



This issue tracker **has been migrated to GitHub**, and is currently **read-only**.
For more information, **see the GitHub FAQs in the Python's Developer Guide.**



This issue has been migrated to GitHub:
https://github.com/python/cpython/issues/83198

classification

Title:	[CVE-2019-20907] Infinite loop in the tarfile module		
Type:	security	**Stage**:	resolved
Components:		**Versions**:	Python 3.10, Python 3.9, Python 3.8, Python 3.7, Python 3.6, Python 3.5

process

Status:	closed	**Resolution**:	fixed
Dependencies:		**Superseder**:	
Assigned To:		**Nosy List**:	bc, ethan.furman, jvoisin, larry, lars.gustaebel, mgorny, miss-islington, ned.deily, petr.viktorin, rishi93, serhiy.storchaka
Priority:	normal	**Keywords**:	patch

Created on **2019-12-10 16:19** by **jvoisin**, last changed **2022-04-11 14:59** by **admin**. This issue is now **closed**.

Files

File name	Uploaded	Description	Edit
timeout-a52710a313fdb35fb428c3399277cb640fe2f686	jvoisin, 2019-12-10 16:19	Infinite loop reproducer.	
recursion.tar	bc, 2020-07-08 19:37	Minimal infinite loop reproducer	

Pull Requests

URL	Status	Linked	Edit
PR 21454	merged	rishi93, 2020-07-12 22:04	
PR 21482	merged	miss-islington, 2020-07-15 11:51	
PR 21483	merged	miss-islington, 2020-07-15 11:51	
PR 21484	merged	miss-islington, 2020-07-15 11:51	
PR 21485	merged	miss-islington, 2020-07-15 11:51	
PR 21489	merged	petr.viktorin, 2020-07-15 15:29	

Messages (17)

msg358200 - (view)	**Author: jvoisin (jvoisin)**	**Date: 2019-12-10 16:19**

While playing with fuzzing and Python, I stumbled upon an infinite loop in Python's tarfile module: just open the attached file with `tarfile.open('timeout-a52710a313fdb35fb428c3399277cb640fe2f686')`, and Python will be endlessly stuck in the `_proc_pax` function in tarfile.py, likely due to a missing check of `length` being strictly superior to zero.

msg373339 - (view) **Author: Ben Caller (bc) *** **Date: 2020-07-08 19:37**

I've attached a minimal tar file which reproduces this. I think the minimum length is 516 bytes.

We need a 512 byte PAX format header block as normal.

Then we need a pax header which matches the regex in
https://github.com/python/cpython/blob/b26a0db8ea2de3a8a8e4b40e69fc8642c7d7cb68/Lib/tarfile.py#L1243

```
    length, keyword = re.compile(br"(\d+) ([^=]+)=").groups()
```

We use the `length` variable to iterate:
https://github.com/python/cpython/blob/b26a0db8ea2de3a8a8e4b40e69fc8642c7d7cb68/Lib/tarfile.py#L1271

```
    while True:
        ...
        pos += length
```

So we can start the block with "0 X=". This makes length=0. So it will increment pos by 0 each loop and loop the same code forever.

Nice find.

Do you think this denial of service is worth requesting a CVE for? If so, can someone else do it.

msg373341 - (view) **Author: Ben Caller (bc) *** **Date: 2020-07-08 20:03**

A smaller bug: If instead of 0 you use a large number (> 2^63) e.g. 9999999999999999999 you get `OverflowError: Python int too large to convert to C ssize_t` rather than the expected `tarfile.ReadError` regardless of errorlevel.

msg373468 - (view) **Author: Rajarishi Devarajan (rishi93) *** **Date: 2020-07-10 14:13**

Hi ! I would like to start contributing to CPython. Can I start working on this issue ?

msg373473 - (view) **Author: Ethan Furman (ethan.furman) *** **Date: 2020-07-10 17:01**

Absolutely!

But first, you'll need to sign the Contributor License Agreement:

  https://www.python.org/psf/contrib/contrib-form/

Thank you for your help!

msg373577 - (view) **Author: Rajarishi Devarajan (rishi93) *** **Date: 2020-07-12 22:10**

Thank you. I have signed the CLA agreement. I have pushed my code changes and also written a testcase for this issue

msg373632 - (view) **Author: jvoisin (jvoisin)** **Date: 2020-07-14 09:29**

CVE-2019-20907 has been assigned to this issue.

msg373681 - (view) **Author: Petr Viktorin (petr.viktorin) *** **Date: 2020-07-15 11:51**

New changeset **5a8d121a1f3ef5ad7c105ee378cc79a3eac0c7d4** by Rishi in branch 'master':
~~**bpo-39017**~~: Avoid infinite loop in the tarfile module (~~**GH-21454**~~)
https://github.com/python/cpython/commit/5a8d121a1f3ef5ad7c105ee378cc79a3eac0c7d4

msg373683 - (view) **Author: Petr Viktorin (petr.viktorin) *** **Date: 2020-07-15 12:20**

Larry and Ned, do you want this fix in the security-only releases you manage?

PRs for 3.6 ad 3.7 are ready, should you wish to merge them.

msg373684 - (view) **Author: miss-islington (miss-islington)** **Date: 2020-07-15 12:30**

New changeset **f3232294ee695492f43d424cc6969d018d49861d** by Miss Islington (bot) in branch '3.9':
[3.9] ~~**bpo-39017**~~: Avoid infinite loop in the tarfile module (~~**GH-21454**~~) (~~**GH-21482**~~)
https://github.com/python/cpython/commit/f3232294ee695492f43d424cc6969d018d49861d

msg373685 - (view) **Author: miss-islington (miss-islington)** **Date: 2020-07-15 12:30**

New changeset **c55479556db015f48fc8bbca17f64d3e65598559** by Miss Islington (bot) in branch '3.8':
[3.8] ~~**bpo-39017**~~: Avoid infinite loop in the tarfile module (~~**GH-21454**~~) (~~**GH-21483**~~)
https://github.com/python/cpython/commit/c55479556db015f48fc8bbca17f64d3e65598559

msg373686 - (view) **Author: Larry Hastings (larry) *** **Date: 2020-07-15 12:34**

Yes, please. It's a simple low-risk fix. And 3.5.10rc1 is stuck waiting for a fix anyway. Thanks!

msg373687 - (view) **Author: Ned Deily (ned.deily) *** **Date: 2020-07-15 12:35**

New changeset **79c6b602efc9a906c8496f3d5f4d54c54b48fa06** by Miss Islington (bot) in branch '3.7':
~~**bpo-39017**~~: Avoid infinite loop in the tarfile module (~~**GH-21454**~~) (~~**GH-21484**~~)
https://github.com/python/cpython/commit/79c6b602efc9a906c8496f3d5f4d54c54b48fa06

msg373688 - (view) **Author: Ned Deily (ned.deily) *** **Date: 2020-07-15 12:36**

New changeset **47a2955589bdb1a114d271496ff803ad73f954b8** by Miss Islington (bot) in branch '3.6':
~~**bpo-39017**~~: Avoid infinite loop in the tarfile module (~~**GH-21454**~~) (~~**#21485**~~)
https://github.com/python/cpython/commit/47a2955589bdb1a114d271496ff803ad73f954b8

msg373689 - (view) **Author: Ned Deily (ned.deily) *** **Date: 2020-07-15 12:37**

Thanks, the PRs for 3.7 and 3.6 are now merged.

msg373764 - (view) **Author: Larry Hastings (larry) *** **Date: 2020-07-16 19:48**

New changeset **cac9ca8ed99bd98f4c0dcd1913a146192bf5ee84** by Petr Viktorin in branch '3.5':
[3.5] ~~**bpo-39017**~~: Avoid infinite loop in the tarfile module (~~**GH-21454**~~) (~~**#21489**~~)
https://github.com/python/cpython/commit/cac9ca8ed99bd98f4c0dcd1913a146192bf5ee84

msg373972 - (view) **Author: Michał Górny (mgorny) *** **Date: 2020-07-19 21:13**

Given that a CVE was assigned for this, I think it'd be better if the news were in the 'Security' category and not 'Library'.

History

Date	User	Action	Args
2022-04-11 14:59:24	admin	set	github: 83198
2020-08-03 10:07:01	vstinner	set	title: Infinite loop in the tarfile module -> [CVE-2019-20907] Infinite loop in the tarfile module
2020-07-19 21:13:23	mgorny	set	nosy: + **mgorny** messages: + **msg373972**
2020-07-16 19:49:38	larry	set	status: open -> closed resolution: fixed stage: patch review -> resolved
2020-07-16 19:48:17	larry	set	messages: + **msg373764**
2020-07-15 15:29:04	petr.viktorin	set	pull_requests: + **pull_request20632**
2020-07-15 12:37:56	ned.deily	set	messages: + **msg373689** versions: + Python 3.5, Python 3.6, Python 3.8, Python 3.9, Python 3.10
2020-07-15 12:36:39	ned.deily	set	messages: + **msg373688**
2020-07-15 12:35:12	ned.deily	set	messages: + **msg373687**
2020-07-15 12:34:22	larry	set	messages: + **msg373686**
2020-07-15 12:30:57	miss-islington	set	messages: + **msg373685**
2020-07-15 12:30:36	miss-islington	set	nosy: + **miss-islington** messages: + **msg373684**
2020-07-15 12:20:00	petr.viktorin	set	nosy: + **larry**, **ned.deily**, - **miss-islington** messages: + **msg373683**
2020-07-15 11:51:48	miss-islington	set	pull_requests: + **pull_request20629**

2020-07-15 11:51:41	miss-islington	set	pull_requests: + **pull_request20628**
2020-07-15 11:51:33	miss-islington	set	pull_requests: + **pull_request20627**
2020-07-15 11:51:26	miss-islington	set	nosy: + **miss-islington** pull_requests: + **pull_request20626**
2020-07-15 11:51:08	petr.viktorin	set	nosy: + **petr.viktorin** messages: + **msg373681**
2020-07-14 09:29:26	jvoisin	set	messages: + **msg373632**
2020-07-12 22:10:05	rishi93	set	messages: + **msg373577**
2020-07-12 22:04:37	rishi93	set	keywords: + **patch** stage: test needed -> patch review pull_requests: + **pull_request20602**
2020-07-10 17:01:05	ethan.furman	set	messages: + **msg373473**
2020-07-10 14:13:26	rishi93	set	messages: + **msg373468**
2020-07-10 10:56:27	rishi93	set	nosy: + **rishi93**
2020-07-08 20:03:20	bc	set	messages: + **msg373341**
2020-07-08 19:37:57	bc	set	files: + **recursion.tar** nosy: + **bc** messages: + **msg373339**
2019-12-10 21:37:50	ethan.furman	set	stage: test needed
2019-12-10 17:20:30	serhiy.storchaka	set	nosy: + **lars.gustaebel**, **serhiy.storchaka**
2019-12-10 16:19:56	jvoisin	create	