» Issue36462



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/80643

classification

Title:	CVE-2019-9674 : zip bomb vulnerability in Lib/zipfile.py		
Type:	security	**Stage**:	resolved
Components:	Library (Lib)	**Versions**:	Python 3.8, Python 3.7, Python 3.6, Python 3.5

process

Status:	closed	**Resolution**:	duplicate
Dependencies:		**Superseder**:	[security] CVE-2019-9674: Zip Bomb vulnerability View: ~~**36260**~~
Assigned To:		**Nosy List**:	brett.cannon, krnick, serhiy.storchaka, twouters, xtreak
Priority:	normal	**Keywords**:	

Created on **2019-03-28 15:46** by **krnick**, last changed **2022-04-11 14:59** by **admin**. This issue is now **closed**.

Messages (7)

msg339053 - (view)	**Author: JUN-WEI SONG (krnick) ***	**Date: 2019-03-28 15:46**

Dear Python Community,

we found a python module vulnerability during these days and we got a CVE number, CVE-2019-9674 after reported it to cve.mitre.org.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9674

The reserved information of CVE-2019-9674 is shown below:

[Description]

Lib/zipfile.py in Python through 3.7.2 allows remote attackers to cause a denial of service (resource consumption) via a ZIP bomb.

[Additional Information]

The python zipfile library version 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8. Allow attackers to cause a denial of service (disk volume exhaustion) via a ZIP bomb.

We have found python standard library zipfile doesn't have ZIP bomb detection and protection. If the user uses zipfile library to unzip a ZIP bomb file, this might cause a denial of service of the localhost.

[VulnerabilityType Other]

Denial-of-Service

Our proposed solutions:

```
    1.The compression ratio:

    Compression ratio = Uncompressed file size / Compressed file
size

    Since ZIP bomb file has a higher compression ratio (1028) than
    normal ZIP file (1 to 3). Therefore, we calculate the
compression
    ratio and set a threshold for the detection.

    2.Nested zip file

    There is a high chance that it is zip bomb if it is a nested
zip
    file.

    3.By limiting resources such as CPU, memory, disk usage.


Unsolved issue

    However, we have not yet determined the compression ratio. We
    temporarily set the compression ratio to 10, and if it
exceeds, it
    may be a ZIP bomb.

    It is likely that detection may misjudge nested compressed
files.
    For example, under normal circumstances, compressed files are
    included in the zip file.


Our solution code：

"""For ratio"""

def _exam_ratio(self, threshold=10):
    """If the ratio exceeds threshold, it may be a ZIP Bomb."""
    sum_file_size = sum([data.file_size for data in
self.filelist])
    sum_compress_size = sum([data.compress_size for data in
self.filelist])
    ratio = sum_file_size / sum_compress_size
    if (ratio > threshold):
        raise BadZipFile("Zip Bomb Detected")

"""For Nested zip file"""
```

```
if(members.filename.endswith(".zip")):
    raise BadZipFile("Nested Zip File Detected")


Thanks!
```

msg339055 - (view) **Author: Serhiy Storchaka (serhiy.storchaka) *** **Date: 2019-03-28 16:16**

I do not think that the library should limit the compression ratio. Large compression ratio is legit. For example, compressed file of size 1 GiB consisting of zeros has the compress ratio 1030 (and I suppose it is even larger if use bzip2 or lzma compressions).

If this is a problem for your program, your program should make a decision what ZIP files should be rejected.

I suggest to close this issue as "not a bug".

msg339056 - (view) **Author: Karthikeyan Singaravelan (xtreak) *** **Date: 2019-03-28 16:38**

Going by CVE number and report is this a duplicate of ~~issue36260~~ ?

msg339058 - (view) **Author: Brett Cannon (brett.cannon) *** **Date: 2019-03-28 16:43**

Closing as a duplicate of ~~issue36260~~.

msg339060 - (view) **Author: Karthikeyan Singaravelan (xtreak) *** **Date: 2019-03-28 16:54**

I would request closing the other one as duplicate and opening this since this contains the actual report or perhaps the report could be copied to ~~issue36260~~. Since Serhiy suggested closing this as not a bug I will leave it to him on resolution of the other issue too.

msg339063 - (view) **Author: Brett Cannon (brett.cannon) *** **Date: 2019-03-28 17:36**

You can also leave a comment in the other issue saying there's more details
in the closed duplicate.

On Thu, Mar 28, 2019 at 9:54 AM Karthikeyan Singaravelan <
report@bugs.python.org> wrote:

>
> Karthikeyan Singaravelan <**tir.karthi@gmail.com**> added the
comment:
>
> I would request closing the other one as duplicate and opening
this since
> this contains the actual report or perhaps the report could be
copied to
> ~~**issue36260**~~. Since Serhiy suggested closing this as not a bug I
will leave
> it to him on resolution of the other issue too.
>
> ----------
>
> _____
> Python tracker <**report@bugs.python.org**>
> <**https://bugs.python.org/issue36462**>
> _____
>

msg339085 - (view) **Author: JUN-WEI SONG (krnick) *** **Date: 2019-03-29 00:03**

Thanks to the python community, both of these issues are the same.

I also think it's a good thing to make related documentation to reduce this type of problem rather than implementing it on a low-level zipfile module. Perhaps we can customize such a requirement through a pip package.

History

Date	User	Action	Args
2022-04-11 14:59:13	admin	set	github: 80643
2019-03-29 00:03:09	krnick	set	messages: + **msg339085**
2019-03-28 17:36:02	brett.cannon	set	messages: + **msg339063**
2019-03-28 16:54:25	xtreak	set	messages: + **msg339060**
2019-03-28 16:43:08	brett.cannon	set	status: open -> closed superseder: **[security] CVE-2019-9674: Zip Bomb**

			vulnerability
			nosy: + **brett.cannon** messages: + **msg339058** resolution: duplicate stage: resolved
2019-03-28 16:38:25	xtreak	set	nosy: + **xtreak** messages: + **msg339056**
2019-03-28 16:16:59	serhiy.storchaka	set	messages: + **msg339055**
2019-03-28 15:50:18	matrixise	set	nosy: + **twouters**, **serhiy.storchaka**
2019-03-28 15:46:11	krnick	create	