

# segmentation fault in lzo\_decompress\_buf, stream.c 589

Bug #1893641 reported by [Doudou Huang](#) on 2020-08-31

This bug affects 1 person

6

Affects	Status	Importance	Assigned to	Milestone
<a href="#">lrzip (Ubuntu)</a>	Confirmed	Undecided	Unassigned	

## Bug Description

Hi, there.

There is invalid memory access in lzo\_decompress\_buf, stream.c 589 in the lrzip version 0.621 (newest branch 597belf). According to the trace, it seems to be an incomplete fix of CVE-2017-8845 and CVE-2019-10654. System:

```
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.6 LTS"
```

To reproduce, run:

```
lrzip -t seg-stream589
```

This is the output from the terminal:

```
Decompressing...
Segmentation fault
This is the trace reported by ASAN:

==177389==ERROR: AddressSanitizer: SEGV on unknown address 0x606000010000
(pc 0x7f19986a0144 bp 0x62100001cd54 sp 0x7f1994afed60 T1)
#0 0x7f19986a0143 in lzolx_decompress (/lib/x86_64-linux-gnu/liblzo2.so.2+0x13143)
#1 0x43faff in lzo_decompress_buf ../stream.c:589
#2 0x43faff in ucompthread ../stream.c:1529
#3 0x7f199804d6b9 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76b9)
#4 0x7f199747f41c in clone (/lib/x86_64-linux-gnu/libc.so.6+0x10741c)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ???0 lzolx_decompress
Thread T1 created by T0 here:
#0 0x7f19988e51e3 in pthread_create (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x361e3)
#1 0x451505 in create_pthread ../stream.c:133
#2 0x451505 in fill_buffer ../stream.c:1694
#3 0x451505 in read_stream ../stream.c:1781
#4 0x18 (<unknown module>)

==177389==ABORTING
```

## CVE References

[2017-8845](#)

[2019-10654](#)

<a href="#">Doudou Huang (tinywhite)</a> wrote on 2020-08-31:	#1
POC (104 bytes, application/octet-stream)	
<a href="#">Marc Deslauriers (mdeslaur)</a> wrote on 2020-08-31:	#2
CVE-2017-8845 and CVE-2019-10654 have not been fixed in Ubuntu 18.04 LTS, so it's quite likely you are hitting those.  Can I make this bug public?  Changed in lrzip (Ubuntu): status:New → Confirmed	
<a href="#">Doudou Huang (tinywhite)</a> wrote on 2020-08-31:	#3
It still exists in the newest branch of the upstream package.  I have reported the issue to the developers but there is no response.	
<a href="#">Marc Deslauriers (mdeslaur)</a> wrote on 2020-08-31:	#4
OK, I've found the upstream bug you reported. Adding it here so we can monitor when a fix will be available.  <a href="https://github.com/ckolivas/lrzip/issues/163">https://github.com/ckolivas/lrzip/issues/163</a>	
<a href="#">Doudou Huang (tinywhite)</a> on 2020-09-07	
information type:Private Security → Public	

### Report a bug

This report contains **Public** information  
Everyone can see this information.

You are [not directly subscribed](#) to this bug's notifications.

[Edit bug mail](#)

### Other bug subscribers

[Subscribe someone else](#)

Notified of all changes

[Doudou Huang](#)

May be notified

[Alejandro J. Alva...](#)  
[Ashani Holland](#)  
[Bruno Garcia](#)  
[CRC](#)  
[Charlie\\_Smotherman](#)  
[Debian PTS](#)  
[DoraannZ](#)  
[Franko Fang](#)  
[HaySayCheese](#)  
[Hidagawa](#)  
[Jesse Jones](#)  
[José Alfonso](#)  
[Matt j](#)  
[Mr. Minhaj](#)  
[Name Changed](#)  
[PCTeacher012](#)  
[Paolo Topa](#)  
[Peter Bullert](#)  
[Punnsa](#)  
[Richard Seguin](#)  
[Richard Williams](#)  
[Tom Weiss](#)  
[Vasanth](#)  
[Vic Parker](#)  
[ahepas](#)  
[basilisgabri](#)  
[dsfkj dfjx](#)  
[eoininmorán](#)  
[ganesh](#)  
[linuxgijs](#)  
[nikonikic42](#)  
[projevie@hotmail.com](#)  
[qadir](#)  
[sankaran](#)  
[van](#)

### Bug attachments

POC  
[Add attachment](#)

### Remote bug watches

[auto-github-ckolivas-lrzip #163](#)  
[closed]

Bug watches keep track of this bug in other bug trackers.

[See full activity log](#)

To post a comment you must [log in](#).

