New issue

Jump to bottom

AddressSanitizer: 1 memory leaks of fill_buffer() #198

Closed Clingto opened this issue on May 19, 2021 · 3 comments

Clingto commented on May 19, 2021

System info:
Ubuntu 16.04.6 LTS, X64, gcc 5.4.0, lrzip (latest master `465afe8`)
Compile Command:

```
$ chmod a+x mkinstalldirs
make distclean
./autogen.sh

mkdir -p build/bin
CC="gcc -fsanitize=address -fno-omit-frame-pointer -g" CXX="g++ -fsanitize=address -fno-omit-frame-pointer -g" ./configure --enable-static-bin --disable-shared
make -j
```

Run Command:

```
$ lrzip -t $POC
```

POC file:
https://github.com/Clingto/POC/blob/master/MSA/lrzip/lrzip-561-fill_buffer-memory-leak

ASAN info:

```
Failed to decompress buffer - lzmaerr=1
Invalid data compressed len 1285 uncompressed 1285 last_head 1285
No such file or directory

=================================================================
==21958==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 24 byte(s) in 1 object(s) allocated from:
    #0 0x7fdb9148d602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x42790f in fill_buffer  test/lrzip-uaf/git/build_asan/stream.c:1706
    #2 0x42790f in read_stream  test/lrzip-uaf/git/build_asan/stream.c:1799

SUMMARY: AddressSanitizer: 24 byte(s) leaked in 1 allocation(s).
```

ckolivas commented on Feb 27 — Owner

Unable to reproduce on latest master.

ckolivas closed this as completed on Feb 27

Clingto commented on Jul 23 • edited — Author

> Unable to reproduce on latest master.
> It seems that I can still reproduce the issue in lrzip (master `465afe8` and the latest `7bd6253`)

```
Decompressing...
Failed to decompress buffer - lzmaerr=1
Invalid data compressed len 1285 uncompressed 1285 last_head 1285
No such file or directory
Fatal error - exiting
Failed to decompress buffer - lzerr=-6

=================================================================
==15175==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 48 byte(s) in 2 object(s) allocated from:
    #0 0x7ffff6f02602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x42978b in fill_buffer test_cve/lrzip-latest/SRC_asan/stream.c:1719
    #2 0x42978b in read_stream test_cve/lrzip-latest/SRC_asan/stream.c:1812
    #3 0x41e1d6 in unzip_literal test_cve/lrzip-latest/SRC_asan/runzip.c:162
    #4 0x41e1d6 in runzip_chunk test_cve/lrzip-latest/SRC_asan/runzip.c:325
    #5 0x41e1d6 in runzip_fdtest_cve/lrzip-latest/SRC_asan/runzip.c:387
    #6 0x40e86a in decompress_file test_cve/lrzip-latest/SRC_asan/lrzip.c:951
    #7 0x4059ac in main test_cve/lrzip-latest/SRC_asan/main.c:720
    #8 0x7ffff579e83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)

SUMMARY: AddressSanitizer: 48 byte(s) leaked in 2 allocation(s).
```

ffontaine commented on Oct 15 — Contributor

FYI, this issue has been assigned CVE-2021-33451

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants