Cvjark / Poc Public

Code Issues 1 Pull requests Actions Projects Security ...

main

Poc / advancecomp / CVE-2022-35015.md

Cvjark Update CVE-2022-35015.md History

1 contributor

74 lines (64 sloc) | 3.14 KB

Product link

https://github.com/amadvance/advancecomp

POC file

https://github.com/Cvjark/Poc/files/9060007/id0_command_advzip_-x_heap-buffer-overflow_sample_No.zip

Command to reproduce

```
./advzip -x [POC file]
```

Product name & version

last github commit code : a543d4c

Problem Type

heap buffer overflow

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/advancecomp/./lib/endianrw.h:172:90 in le_uint32_read(void
const*)
```

Crash Detail

```
==96173==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x612000000149
at pc 0x00000051f317 bp 0x7fffeeb84d10 sp 0x7fffeeb84d08
READ of size 1 at 0x612000000149 thread T0
    #0 0x51f316 in le_uint32_read(void const*)
/home/bupt/Desktop/advancecomp/./lib/endianrw.h:172:90
    #1 0x51f316 in zip::open() /home/bupt/Desktop/advancecomp/zip.cc:860:10
    #2 0x504089 in extract_all(int, char**, bool)
/home/bupt/Desktop/advancecomp/rezip.cc:301:4
    #3 0x508c3d in process(int, char**)
/home/bupt/Desktop/advancecomp/rezip.cc:604:3
    #4 0x509b88 in main /home/bupt/Desktop/advancecomp/rezip.cc:623:3
    #5 0x7f194282ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #6 0x41f1e9 in _start (/home/bupt/Desktop/advancecomp/advzip+0x41f1e9)

0x612000000149 is located 0 bytes to the right of 265-byte region
[0x612000000040,0x612000000149)
allocated by thread T0 here:
    #0 0x4b17b0 in malloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x52ada4 in data_alloc(unsigned int)
/home/bupt/Desktop/advancecomp/data.cc:51:40

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/advancecomp/./lib/endianrw.h:172:90 in le_uint32_read(void
const*)
Shadow bytes around the buggy address:
  0x0c247fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff8020: 00 00 00 00 00 00 00 00 00[01]fa fa fa fa fa fa
  0x0c247fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==96173==ABORTING
```