Cvjark Update CVE-2022-35020.md History

1 contributor

93 lines (82 sloc) | 5.65 KB ...

Product link

https://github.com/amadvance/advancecomp

POC file

https://github.com/Cvjark/Poc/files/9060026/id2_command_advmng_-z_heap-buffer-overflow_sample_No.zip

Command to reproduce

```
./advmng -z [sample file]
```

Product name & version

```
last github commit code : a543d4c
```

Problem Type

Heap buffer overflow

Crash Detail

```
==4414==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x631000060520
at pc 0x00000043e235 bp 0x7ffcd44f50d0 sp 0x7ffcd44f4880
READ of size 32768 at 0x631000060520 thread T0
    #0 0x43e234 in __interceptor_memcpy.part.46 /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:810
    #1 0x7f8d8c22f45f in inflate (/lib/x86_64-linux-gnu/libz.so.1+0xc45f)
    #2 0x7f8d8c2344b3 in uncompress2 (/lib/x86_64-linux-gnu/libz.so.1+0x114b3)
    #3 0x7f8d8c2345a2 in uncompress (/lib/x86_64-linux-gnu/libz.so.1+0x115a2)
    #4 0x544085 in mng_read_delta /home/bupt/Desktop/advancecomp/lib/mng.c:542:7
    #5 0x544085 in mng_read /home/bupt/Desktop/advancecomp/lib/mng.c:656:9
    #6 0x5418da in adv_mng_read /home/bupt/Desktop/advancecomp/lib/mng.c:748:9
    #7 0x5074e6 in convert_f_mng(adv_fz_struct*, adv_fz_struct*, unsigned int*,
unsigned int*, adv_scroll_info_struct*, bool, bool)
/home/bupt/Desktop/advancecomp/remng.cc:479:8
    #8 0x4fbd7d in convert_mng(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >
const&) /home/bupt/Desktop/advancecomp/remng.cc:593:3
    #9 0x4fc3dd in convert_mng_inplace(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&)
/home/bupt/Desktop/advancecomp/remng.cc:614:3
    #10 0x4ffc08 in remng_single(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, unsigned long long&,
unsigned long long&) /home/bupt/Desktop/advancecomp/remng.cc:950:4
    #11 0x50b705 in remng_all(int, char**)
/home/bupt/Desktop/advancecomp/remng.cc:985:3
    #12 0x5102d4 in process(int, char**)
/home/bupt/Desktop/advancecomp/remng.cc:1249:3
    #13 0x511a98 in main /home/bupt/Desktop/advancecomp/remng.cc:1268:3
    #14 0x7f8d8aee9c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #15 0x41f289 in _start (/home/bupt/Desktop/advancecomp/advmng+0x41f289)

0x631000060520 is located 0 bytes to the right of 64800-byte region
[0x631000050800,0x631000060520)
allocated by thread T0 here:
    #0 0x4b1850 in malloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x54332a in mng_read_delta /home/bupt/Desktop/advancecomp/lib/mng.c:455:18
    #2 0x54332a in mng_read /home/bupt/Desktop/advancecomp/lib/mng.c:656:9
    #3 0x5418da in adv_mng_read /home/bupt/Desktop/advancecomp/lib/mng.c:748:9
    #4 0x4fbd7d in convert_mng(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >
const&) /home/bupt/Desktop/advancecomp/remng.cc:593:3
    #5 0x4fc3dd in convert_mng_inplace(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&)
```

```
/home/bupt/Desktop/advancecomp/remng.cc:614:3
    #6 0x4ffc08 in remng_single(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, unsigned long long&,
unsigned long long&) /home/bupt/Desktop/advancecomp/remng.cc:950:4
    #7 0x50b705 in remng_all(int, char**)
/home/bupt/Desktop/advancecomp/remng.cc:985:3
    #8 0x5102d4 in process(int, char**)
/home/bupt/Desktop/advancecomp/remng.cc:1249:3
    #9 0x511a98 in main /home/bupt/Desktop/advancecomp/remng.cc:1268:3
    #10 0x7f8d8aee9c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:810 in
__interceptor_memcpy.part.46
Shadow bytes around the buggy address:
  0x0c6280004050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c6280004060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c6280004070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c6280004080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c6280004090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c62800040a0: 00 00 00 00[fa]fa fa fa fa fa fa fa fa fa fa fa
  0x0c62800040b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c62800040c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c62800040d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c62800040e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c62800040f0: 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
==4414==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:810 in __interceptor_memcpy.part.46
```