Cvjark / Poc Public

Code Issues 1 Pull requests Actions Projects Security ···

main ···

Poc / advancecomp / CVE-2022-35019.md

Cvjark Update CVE-2022-35019.md History

1 contributor

50 lines (40 sloc) | 2.57 KB ···

Product link

https://github.com/amadvance/advancecomp

POC file

https://github.com/Cvjark/Poc/files/9060033/id54_command_advmng_-z_SEGV_sample_No.zip

Command to reproduce

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

Product name & version

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

Problem Type

SEGV

Crash Detail

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==95612==ERROR: AddressSanitizer: SEGV on unknown address 0x616000010000 (pc
0x7f8d29a1faf8 bp 0x61900000042a sp 0x7ffc45b8ea68 T0)
==95612==The signal is caused by a WRITE memory access.
    #0 0x7f8d29a1faf8  (/lib/x86_64-linux-gnu/libz.so.1+0x9af8)
    #1 0x7f8d29a21419 in inflate (/lib/x86_64-linux-gnu/libz.so.1+0xb419)
    #2 0x7f8d29a274b3 in uncompress2 (/lib/x86_64-linux-gnu/libz.so.1+0x114b3)
    #3 0x7f8d29a275a2 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 0x7f8d286dcc86 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)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libz.so.1+0x9af8)
==95612==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libz.so.1+0x9af8)
```