Cvjark Update CVE-2022-35018.md History

1 contributor

49 lines (39 sloc) | 3.47 KB ...

Product link

https://github.com/amadvance/advancecomp

POC file

https://github.com/Cvjark/Poc/files/9060029/id4_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
=================================================================
==5443==ERROR: AddressSanitizer: SEGV on unknown address 0x632009000800 (pc
0x000000523ebb bp 0x7ffcd17c1c10 sp 0x7ffcd17c1ac0 T0)
==5443==The signal is caused by a READ memory access.
    #0 0x523ebb in col_equal(adv_mng_write_struct*, unsigned int, unsigned char*,
unsigned int) /home/bupt/Desktop/advancecomp/mngex.cc:238:14
    #1 0x5204c5 in compute_image_range(adv_mng_write_struct*, unsigned int*,
unsigned int*, unsigned int*, unsigned int*, unsigned char*, unsigned int)
/home/bupt/Desktop/advancecomp/mngex.cc:272:27
    #2 0x5204c5 in mng_write_delta_image(adv_mng_write_struct*, adv_fz_struct*,
unsigned int*, unsigned char*, unsigned int, unsigned char*, unsigned int)
/home/bupt/Desktop/advancecomp/mngex.cc:417:2
    #3 0x5204c5 in mng_write_image_raw(adv_mng_write_struct*, adv_fz_struct*,
unsigned int*, unsigned int, unsigned int, unsigned int, unsigned char*, unsigned
int, unsigned char*, unsigned int, int, int)
/home/bupt/Desktop/advancecomp/mngex.cc:607:4
    #4 0x51c459 in mng_write_image(adv_mng_write_struct*, adv_fz_struct*,
unsigned int*, unsigned int, unsigned int, unsigned int, unsigned char*, unsigned
int, unsigned char*, unsigned int, int, int)
/home/bupt/Desktop/advancecomp/mngex.cc:623:4
    #5 0x506670 in convert_image(adv_mng_write_struct*, adv_fz_struct*, unsigned
int*, unsigned int, unsigned int, unsigned int, unsigned char*, unsigned int,
unsigned char*, unsigned int, adv_scroll_coord_struct*)
/home/bupt/Desktop/advancecomp/remng.cc
    #6 0x507c26 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:510:5
    #7 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
    #8 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
    #9 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
    #10 0x50b705 in remng_all(int, char**)
/home/bupt/Desktop/advancecomp/remng.cc:985:3
    #11 0x5102d4 in process(int, char**)
/home/bupt/Desktop/advancecomp/remng.cc:1249:3
    #12 0x511a98 in main /home/bupt/Desktop/advancecomp/remng.cc:1268:3
    #13 0x7fc5adac2c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #14 0x41f289 in _start (/home/bupt/Desktop/advancecomp/advmng+0x41f289)

AddressSanitizer can not provide additional info.
```

```
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/advancecomp/mngex.cc:238:14 in
col_equal(adv_mng_write_struct*, unsigned int, unsigned char*, unsigned int)
==5443==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/advancecomp/mngex.cc:238:14 in
col_equal(adv_mng_write_struct*, unsigned int, unsigned char*, unsigned int)
```