Cvjark Update CVE-2022-35014.md History

1 contributor

50 lines (39 sloc) | 3.91 KB ...

Product link

https://github.com/amadvance/advancecomp

POC file

https://github.com/Cvjark/Poc/files/9060018/id0_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

==4310==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x0000004298a4 bp
0x000000000001 sp 0x7fffdc8dd140 T0)
==4310==The signal is caused by a READ memory access.
==4310==Hint: this fault was caused by a dereference of a high value address (see
register values below).  Disassemble the provided pc to learn which register was
used.
    #0 0x4298a4 in bool
__sanitizer::atomic_compare_exchange_strong<__sanitizer::atomic_uint8_t>
(__sanitizer::atomic_uint8_t volatile*, __sanitizer::atomic_uint8_t::Type*,
__sanitizer::atomic_uint8_t::Type, __sanitizer::memory_order)
/home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_atomic_clang.h:80
    #1 0x4298a4 in
__asan::Allocator::AtomicallySetQuarantineFlagIfAllocated(__asan::AsanChunk*,
void*, __sanitizer::BufferedStackTrace*) /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_allocator.cpp:621
    #2 0x4298a4 in __asan::Allocator::Deallocate(void*, unsigned long, unsigned
long, __sanitizer::BufferedStackTrace*, __asan::AllocType)
/home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_allocator.cpp:697
    #3 0x4298a4 in __asan::asan_free(void*, __sanitizer::BufferedStackTrace*,
__asan::AllocType) /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_allocator.cpp:971
    #4 0x4b1550 in free /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:128
    #5 0x52382d in mng_write_done(adv_mng_write_struct*)
/home/bupt/Desktop/advancecomp/mngex.cc:709:2
    #6 0x5088ea 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:524:3
    #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 0x7fcbd84a9c86 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/tools/llvm-
12.0.1/llvm/projects/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_atomic_clang.h:80 in bool
__sanitizer::atomic_compare_exchange_strong<__sanitizer::atomic_uint8_t>
(__sanitizer::atomic_uint8_t volatile*, __sanitizer::atomic_uint8_t::Type*,
__sanitizer::atomic_uint8_t::Type, __sanitizer::memory_order)
==4310==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_atomic_clang.h:80 in bool
__sanitizer::atomic_compare_exchange_strong<__sanitizer::atomic_uint8_t>
(__sanitizer::atomic_uint8_t volatile*, __sanitizer::atomic_uint8_t::Type*,
__sanitizer::atomic_uint8_t::Type, __sanitizer::memory_order)
```