New issue

Jump to bottom

SEGV issue detected in pbc_wmessage_integer src/wmessage.c:137 #158

Open HotSpurzzZ opened this issue on Aug 27 · 0 comments

HotSpurzzZ commented on Aug 27

A SEGV has occurred when running program test.
The program does not check for the return value of pbc_wmessage_new (./test/test.c:16), resulting in the program still running when null is returned.

POC file:

https://github.com/HotSpurzzZ/testcases/blob/main/pbc/pbc_wmessage_integer_testcase

Verification steps :

1.Get the source code of pbc
2.Compile (Note the modification of the makefile to use AddressSanitizer)

```
cd pbc
make
```

3.use poc and run test

```
mv $poc test.pb
./test
```

AddressSanitizer output :

```
=================================================================
==10511==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x560d341408e6 bp
0x00000000007b sp 0x7ffdc783c030 T0)
==10511==The signal is caused by a READ memory access.
==10511==Hint: address points to the zero page.
    #0 0x560d341408e6 in pbc_wmessage_integer src/wmessage.c:137
    #1 0x560d34136ec9 in test ../test/test.c:21
    #2 0x560d34136931 in main ../test/test.c:39
    #3 0x7fde58430d8f in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
    #4 0x7fde58430e3f in __libc_start_main_impl ../csu/libc-start.c:392
    #5 0x560d34136c94 in _start (/root/Desktop/pbc/build/test+0x3c94)
```

```
AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV src/wmessage.c:137 in pbc_wmessage_integer
==10511==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant