New issue

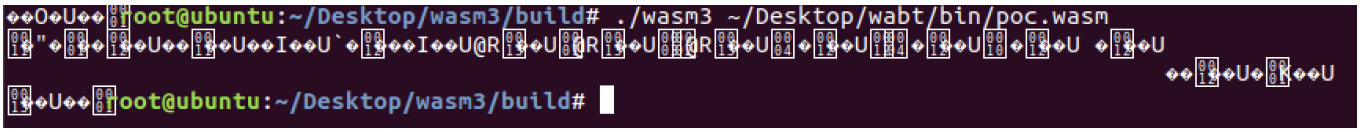
Jump to bottom

Heap Overflow in WASI read/write API #323

Closed ha1vk opened this issue on Apr 7 · 1 comment

ha1vk commented on Apr 7 Contributor

the WASI API which uses iovs is not check the iovs' buf address and buf length,it would result in out of buffer.
run the poc,you will see the memory information leak



If you build with asan,you will see that buffer-overflow detected
root@ubuntu:~/Desktop# ./m3 ~/Desktop/wabt/bin/poc.wasm

==44312==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x631000038818 at pc 0x7f3b4c5ce93e bp 0x7ffcdce54020 sp 0x7ffcdce537c8
READ of size 28672 at 0x631000038818 thread T0
#0 0x7f3b4c5ce93d (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x4c93d)
.....

poc.wasm.zip

ha1vk mentioned this issue on Apr 7

fix WASI API read/write pread/pwrite buffer overflow #324

Merged

 **vshymanskyy** closed this as completed on Apr 13

---

vshymanskyy commented on Apr 13 Member

Thanks for a great fix!

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants