

[New issue](#)[Jump to bottom](#)

Out-of-bounds read in elf parsing. #1

✓ Closed

liyansong2018 opened this issue on Jan 23 · 0 comments

Assignees



Labels

bug

liyansong2018 commented on Jan 23

Owner

poc

```
$ ./elfspirit parse id_000000
```

log

[+] ELF Header

```
e_type:          3 -> A shared object
e_machine:       62 -> Intel 80386
e_version:       1 -> Current version
e_entry:        4176
e_phoff:         64
e_shoff:       13608
e_flags:         0
e_ehsize:        64
e_phentsize:     56
e_phnum:         9
e_shentsize:     64
e_shentsize:     64
e_shstrndx:     27
```

[+] Section Header Table

[Nr]	Name	Type	Addr	Off	Size	Es	Flg	Lk	Inf	Al
------	------	------	------	-----	------	----	-----	----	-----	----

AddressSanitizer:DEADLYSIGNAL

=====

==193419==ERROR: AddressSanitizer: SEGV on unknown address 0x7f08638c5000 (pc 0x7f0842727231 bp 0x7ff

==193419==The signal is caused by a READ memory access.

#0 0x7f0842727231 (/lib/x86_64-linux-gnu/libc.so.6+0x15f231)

#1 0x7f08427c9a8c in __interceptor_strlen ../../../../src/libsanitizer/sanitizer_common/sanitizer

#2 0x55862b528026 in parse /home/lys/Tools/elfspirit/parse.c:975

```
#3 0x55862b4c5167 in readcmdline /home/lys/Tools/elfspirit/main.c:251
#4 0x55862b4c5167 in main /home/lys/Tools/elfspirit/main.c:263
#5 0x7f08425efe49 in __libc_start_main ../csu/libc-start.c:314
#6 0x55862b4c5d09 in _start (/home/lys/Tools/elfspirit/elfspirit+0x9d09)
```

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0x15f231)

==193419==ABORTING



[poc.zip](#)

  liyansong2018 added the `bug` label on Jan 23

 liyansong2018 closed this as completed in [c5b0f5a](#) on Jan 23


  liyansong2018 mentioned this issue on Mar 25

AFL-Fuzz Crash 000000: parse.c:1186 #4

 Closed

  liyansong2018 self-assigned this on Mar 28

Assignees

 liyansong2018

Labels

`bug`

Projects

 ElfspiritTodo

Status: Done

Milestone

No milestone

Development

Development

No branches or pull requests

1 participant

