ganaware / pcf2bdf Public

Code Issues Pull requests Security Insights

New issue

Jump to bottom

Segmentation fault - ASAN Deadly Signal in pcf2bdf #5

Closed anishsujanani opened this issue on Jan 11 · 2 comments

anishsujanani commented on Jan 11 • edited

Hello **@ganaware**, as discussed earlier:
I have compiled pcf2bdf with address sanitization and fuzz-tested inputs with AFL. The file is partially parsed before the program crashes due to a segmentation fault. The actual input file is stored within the zipped folder attached.

Input:
`./pcf2bdf segfault_deadly_signal`

Output:

```
......
parsed content to stdout
......
ASAN:DEADLYSIGNAL
=================================================================
==5771==ERROR: AddressSanitizer: SEGV on unknown address 0x62400021edc8 (pc 0x000000405f16 bp
0x62400021edc8 sp 0x7ffc544ac210 T0)
==5771==The signal is caused by a READ memory access.
    #0 0x405f15 in main /home/ec2-user/pcf2bdf_research/pcf2bdf.cc:1190
    #1 0x7fcf86916139 in __libc_start_main (/lib64/libc.so.6+0x21139)
    #2 0x409b49 in _start (/home/ec2-user/pcf2bdf_research/with_asan/pcf2bdf+0x409b49)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/ec2-user/pcf2bdf_research/pcf2bdf.cc:1190 in main
==5771==ABORTING
```

segfault_deadly_signal.zip

ganaware commented on Jan 11 Owner

This problem was fixed by `3555aab` .

Thank you for the bug report.

ganaware closed this as completed on Jan 11

carnil commented on Feb 21

CVE-2022-23319 is assigned for this issue.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants