New issue

Jump to bottom

Heap-buffer-overflow in pcf2bdf #4

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 attached causes a memory access violation. The actual input file is stored within the zipped folder attached.

Input:
`./pcf2bdf heap_overflow_read_40b`

Output:

```
gzip: heap_overflow_read_40b: unexpected end of file
=================================================================
==5565==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000050 at pc
0x0000004095b0 bp 0x7fffff5362b0 sp 0x7fffff5362a0
READ of size 40 at 0x602000000050 thread T0
    #0 0x4095af in main /home/ec2-user/pcf2bdf_research/pcf2bdf.cc:852
    #1 0x7f7a5a1c6139 in __libc_start_main (/lib64/libc.so.6+0x21139)
    #2 0x409b49 in _start (/home/ec2-user/pcf2bdf_research/with_asan/pcf2bdf+0x409b49)

0x602000000051 is located 0 bytes to the right of 1-byte region [0x602000000050,0x602000000051)
allocated by thread T0 here:
    #0 0x7f7a5af01f41 in operator new[](unsigned long) (/lib64/libasan.so.4+0xd9f41)
    #1 0x4074a4 in main /home/ec2-user/pcf2bdf_research/pcf2bdf.cc:829

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/ec2-user/pcf2bdf_research/pcf2bdf.cc:852 in
main
Shadow bytes around the buggy address:
  0x0c047fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c047fff8000: fa fa 01 fa fa fa 01 fa fa fa[01]fa fa fa fa fa
  0x0c047fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==5565==ABORTING
```

heap_overflow_read_40b.zip

ganaware commented on Jan 11 — Owner

This problem was fixed by `aaf1680` .

Thank you for the bug report.

ganaware closed this as completed on Jan 11

---

carnil commented on Feb 21

CVE-2022-23318 was 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