New issue

Jump to bottom

Out-of-bounds read in draw.c in calculate_beam #83

Closed **chibataiki** opened this issue on Apr 26, 2021 · 0 comments

chibataiki commented on Apr 26, 2021 • edited ▾

Version `0cf4a55`
In function calculate_beam() in draw.c .
There is out of bounds read in array min_tb at line 357 and 359, the flaw will cause crash.

```
if (s->nhd == 0)
                stem_err = min_tb[0][(unsigned) s->nflags];
else
                stem_err = min_tb[1][(unsigned) s->nflags];
```

The (unsigned) s->nflags can be checked whether between 0 and 5.
I am not sure what the `stem_err` means so i didn't try to fix it.

gdb info:

```
──── source:draw.c+357 ────
    352                         }
    353                         x = s->voice == voice ? s->xs : s->x;
    354                         ys = a * x + b - staff_tb[s->staff].y;
    355                         if (s->voice == voice) {
    356                                 if (s->nhd == 0)
                // s=0x00007fffffffdff8  →  [...]  →  0x0000555555625d28, nflags=0x1, min_tb=0x00005555555ce640  →  0x4180000041800000
 →  357                                         stem_err = min_tb[0][(unsigned) s->nflags];
    358                                 else
    359                                         stem_err = min_tb[1][(unsigned) s->nflags];
    360                                 if (s->stem > 0) {
    361                                         if (s->pits[s->nhd] > 26) {
    362                                                 stem_err -= 2;
── trace ────
[#0] 0x555555570417 → calculate_beam(bm=0x7fffffffe050, s1=0x555555622618)
[#1] 0x55555557c659 → draw_sym_near()
[#2] 0x55555559542a → delayed_output(indent=0)
[#3] 0x55555559562d → output_music()
[#4] 0x555555597aeb → generate()
[#5] 0x555555597c2e → gen_ly(eob=0x0)
[#6] 0x55555559eca1 → do_tune()
[#7] 0x55555555e300 → abc_parse(p=0x55555561e0e0 "", fname=0x5555555fab00 ".poc", ln=0x1b)
[#8] 0x555555584b9e → txt_add_eos(fname=0x5555555fab00 ".poc", linenum=0x1b)
[#9] 0x555555585d81 → frontend(s=0x55555561d1a5 "X:X:\027\nC", '.' <repeats 14 times>, "mid\n\\:`\n\177\377\062~c .", ftype=0x0, f
────
gef➤  p (unsigned) s->nflags
$1 = 0xfffffffe
gef➤  p min_tb[0][(unsigned) s->nflags]
Cannot access memory at address 0x5559555ce638
```

reproduce:

```
abcm2ps -E  [poc]
```

out-of-bounds-read_calculate_beam_357.zip
out-of-bounds-read_calculate_beam_359.zip

reporter: chiba of topsec alphalab

chibataiki changed the title ~~Out-of-bounds read in draw.c+357 in calculate_beam~~ **Out-of-bounds read in draw.c in calculate_beam** on Apr 26, 2021

moinejf added a commit that referenced this issue on Apr 27, 2021

`fix: array overflow when wrong duration in voice overlay` ··· `2f56e11`

chibataiki closed this as completed on Apr 29, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant