lewdlime / abcm2ps Public

<> Code ⊙ Issues 32 Pull requests Actions Projects Wiki ···

New issue

Jump to bottom

stack buffer overflow in function get_key() in parse.c #84

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

chibataiki commented on Apr 26, 2021 • edited

Version `0cf4a55`
Stack buffer over found in parse.c in function get_key().

The root cause maybe is in function c_set_k_acc(), the array `accs` and `pits` size is 8.
If `s->u.key.sf` bigger than 7 , then the array `accs` and `pits` will access out of index and corrupt the stack, if the value of `s->u.key.sf` is more bigger, then the stack frame will be corrupted.

```
static void set_k_acc(struct SYMBOL *s)
{
        int i, j, nacc;
        char accs[8], pits[8];
        ...
        if (s->u.key.sf > 0) {
                for (nacc = 0; nacc < s->u.key.sf; nacc++) {
                        accs[nacc] = A_SH;
                        pits[nacc] = sharp_tb[nacc];
                }
}
```

gdb

```
gef➤  disassemble set_k_acc
Dump of assembler code for function set_k_acc:
   0x000055555559f74c <+0>:     endbr64
   0x000055555559f750 <+4>:     push   rbp
   0x000055555559f751 <+5>:     mov    rbp,rsp
   0x000055555559f754 <+8>:     sub    rsp,0x40
   0x000055555559f758 <+12>:    mov    QWORD PTR [rbp-0x38],rdi
...


   0x55555559f941 <set_k_acc+501>  mov    rax, QWORD PTR [rbp-0x8]
 → 0x55555559f945 <set_k_acc+505>  xor    rax, QWORD PTR fs:0x28
   0x55555559f94e <[buffer-over-flow_parse.c_set_k_acc.zip](https://github.com/leesavide/abcm2ps/files/6381703/buffer-over-flow_parse.c_set_k_acc.zip)+514>  je     0x55555559f955
<set_k_acc+521>
   0x55555559f950 <set_k_acc+516>  call   0x55555555ba40 <__stack_chk_fail@plt>
   0x55555559f955 <set_k_acc+521>  leave

─ source:parse.c+3943 ────
   3938         for (i = 0; i < nacc; i++) {
   3939                 s->u.key.accs[i] = accs[i];
   3940                 s->u.key.pits[i] = pits[i];
   3941         }
●  3942         s->u.key.nacc = nacc;
 → 3943  }


gef➤  x/gx $rbp-0x8
0x7fffffffe038: 0x0101010101010101
```

reproduce :

abcm2ps -E poc

buffer-over-flow_parse.c_set_k_acc.zip

reporter： chiba of topsec alphalab

moinejf added a commit that referenced this issue on Apr 28, 2021

`fix: crash when accidental without a note at start of line after K:` ··· `3169ace`

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