New issue

Jump to bottom

NULL pointer dereference in the printstatus() function #68

Closed **bsdb0y** opened this issue on Apr 2, 2021 · 1 comment

bsdb0y commented on Apr 2, 2021

Hi,

While fuzzing samurai 1.2 (and git nightly repo), I found a NULL pointer dereference in the printstatus() function, in build.c.

```
262 static void
263 printstatus(struct edge *e, struct string *cmd)
264 {
265         struct string *description;
266         char status[256];
267
268         description = buildopts.verbose ? NULL : edgevar(e, "description", true);
269         if (!description || description->n == 0)
270                 description = cmd;
271         formatstatus(status, sizeof(status));
272         fputs(status, stdout);
273         puts(description->s);
274 }
```

In the code snippet, it seems there are no checks on `cmd` parameter which leads to set the variable `description` to `NULL` on L270 and then on L273 it dereferences the NULL

Attaching a reproducer (gzipped so GitHub accepts it): test1.gz

Issue can be reproduced by running:

```
samu -f test1
```

```
=================================================================
==2291724==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x7fa51cd50675 bp 0x7ffdf10454f0 sp 0x7ffdf1044ca8 T0)
==2291724==The signal is caused by a READ memory access.
==2291724==Hint: address points to the zero page.
    #0 0x7fa51cd50675  (/lib/x86_64-linux-gnu/libc.so.6+0x18b675)
    #1 0x4355d1 in puts (/src/samurai/samu+0x4355d1)
    #2 0x4cb75f in printstatus /src/samurai-1.2/build.c:273:2
    #3 0x4cc1f1 in jobstart /src/samurai-1.2/build.c:312:3
    #4 0x4ca7c7 in build /src/samurai-1.2/build.c:568:19
    #5 0x4dc5aa in main /src/samurai-1.2/samu.c:256:2
    #6 0x7fa51cbec0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #7 0x41c42d in _start (/src/samurai/samu+0x41c42d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0x18b675)
==2291724==ABORTING
```

michaelforney closed this as completed in `d2af3bc` on Apr 4, 2021

michaelforney commented on Apr 4, 2021 Owner

Thanks for the report! This is something that should've been caught during parsing, but it only checked whether there was any `command = ...` line, even if the value was NULL. ninja errors on both missing on empty command value, so now we do the same.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants