New issue

Jump to bottom

invalid free in cmd_info.c:cmd_info() #16303

Closed aar0nge opened this issue on Mar 25, 2020 · 1 comment · Fixed by #16318

Labels crash good first issue RIO

Milestone 4.4.0 - pangolin

aar0nge commented on Mar 25, 2020 • edited Contributor

Work environment

Questions	Answers
OS/arch/bits (mandatory)	Ubuntu x86 64
File format of the file you reverse (mandatory)	ELF
Architecture/bits of the file (mandatory)	x86/64
r2 -v full output, **not truncated** (mandatory)	rradare2 4.3.1 23909 @ linux-x86-64 git.4.3.1-1-ge55661b commit: e55661b build: 2020-03-22__22:18:20

Expected behavior

Handle input error

Actual behavior

double free/invalid pointer to free

Steps to reproduce the behavior

$ r2 -
[0x00000000]> in 0
[0x00000000]> oc 0
[0x00000000]> in 0
*** Error in `r2': free(): invalid pointer: 0x00007fffed1bcd00 ***
.....

Additional Logs, screenshots, source-code, configuration dump, ...

```
 -- I accidentally the kernel with radare2.
[0x00000000]> in 0
fd       3
file     malloc://512
size     0x200
humansz  512
mode     rwx
format   any
iorw     true
blksz    0x0
block    0x100

[0x00000000]> oc 0
Cannot open file
[0x00000000]> in 0
*** Error in `r2': free(): invalid pointer: 0x00007fffc6993d00 **
======= Backtrace: =========
```

The `in` command would first free the original `core->table_query`, then create a new `core->table_query` in `cmd_info.c:cmd_info()`,

```
R_FREE (core->table_query);
if (space && *space == ' ') {
        core->table_query = r_str_trim_dup (space + 1);
}
```

The `oc` command would free it in `core.c: r_core_fini`, which didn't NULL it out.

```
.....
        free (c->table_query);
        r_list_free (c->files);
        r_list_free (c->watchers);
        r_list_free (c->scriptstack);
.....
```

So execute `in 0` again would cause a double/invalid free.

XVilka added crash good first issue RIO labels on Mar 25, 2020

XVilka added this to the **4.4.0 - pangolin** milestone on Mar 25, 2020

radare commented on Mar 25, 2020 — Collaborator

send a pr, dont spend time reporting bugs if you have the fix
...

aar0nge mentioned this issue on Mar 26, 2020

fix c->table_query double free #16318

Merged

4 tasks

radare closed this as completed in #16318 on Mar 26, 2020

---

radare pushed a commit that referenced this issue on Mar 26, 2020

`Fix #16303 - c->table_query double free (#16318)` `cb8b683`

Assignees

No one assigned

Labels

crash **good first issue** **RIO**

Projects

None yet

Milestone

4.4.0 - pangolin

Development

Successfully merging a pull request may close this issue.

fix c->table_query double free

3 participants