New issue

Jump to bottom

command "adf" Segmentation fault #16215

Closed   aar0nge opened this issue on Mar 14, 2020 · 1 comment · Fixed by #16230

Labels   crash   good first issue

Milestone   4.4.0 - pangolin

aar0nge commented on Mar 14, 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)	radare2 4.3.1 23928 @ linux-x86-64 git.4.3.1-10-g1271d65 commit: `1271d65` build: 2020-03-11__10:01:54

Expected behavior

Handle input error

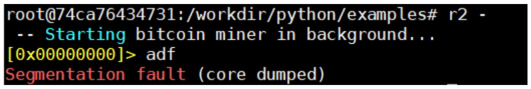
Actual behavior

Segmentation fault

Steps to reproduce the behavior

$ r2 -
[0x00000000]> adf
Segmentation fault (core dumped)

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



```
root@74ca76434731:/workdir/python/examples# r2 -
 -- Starting bitcoin miner in background...
[0x00000000]> adf
Segmentation fault (core dumped)
```

in `libr/core/anal.c` , when command "adf" has no or wrong argument,
`anal_fcn_data (core, input + 1) --> RAnalFunction *fcn = r_anal_get_fcn_in (core->anal, core->offset, -1);`
returns null pointer for `fnc` cause segmentation fault later in `ensure_fcn_range (fcn);`

radare commented on Mar 14, 2020   Collaborator

Can you send a PR as long as you know wheres the bug and how to fix it?

You can even use the pencil button in github and create the pr in there
…

XVilka added crash good first issue labels on Mar 16, 2020

XVilka added this to the **4.4.0 - pangolin** milestone on Mar 16, 2020

x0urc3 mentioned this issue on Mar 16, 2020

Fix segfault in adf #16230
Merged
4 tasks

radare closed this as completed in #16230 on Mar 16, 2020

Assignees
No one assigned

Labels
crash   good first issue

Projects
None yet

Milestone

4.4.0 - pangolin

Development

Successfully merging a pull request may close this issue.

Fix segfault in adf

3 participants