New issue

Jump to bottom

# unmatched array length in core_java.c #16304

Closed aar0nge opened this issue on Mar 25, 2020 · 1 comment · Fixed by #16313

Labels crash good first issue java

Milestone 4.4.0 - pangolin

aar0nge commented on Mar 25, 2020 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

seg fault

### Steps to reproduce the behavior

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

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

```
 -- phrack, better than java in the browser -- jvoisin
[0x00000000]> java o
Segmentation fault (core dumped)
```

in `core_java.c` , `END_CMDS` not match the actual length in `JAVA_CMDS`

XVilka added crash good first issue java 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 the pr with the fix please
...

philoinovsky mentioned this issue on Mar 26, 2020

**Fix unmatched array length in core_java.c (issue #16304)** #16313

Merged

4 tasks

radare closed this as completed in #16313 on Mar 26, 2020

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

`Fix unmatched array length in core_java.c (issue #16304) (#16313)` ced0223

Assignees

No one assigned

Labels

crash good first issue java

Projects

None yet

Milestone

4.4.0 - pangolin

Development

Successfully merging a pull request may close this issue.

**Fix unmatched array length in core_java.c (issue #16304)**

3 participants