Out-of-bounds Read in r_bin_ne_get_entrypoints function in radareorg/radare2

0

Valid Reported on Apr 10th 2022

Description

Out-of-bounds (OOB) read vulnerability exists in `r_bin_ne_get_entrypoints` function in Radare2 5.6.7

Version

```
radare2 5.6.7 27777 @ linux-x86-64 git.5.6.6
commit: 0c4af43def68ce29f7a74847bb1b7286da155200 build: 2022-04-10__08:53:3
```

Analysis

The vulnerability exists due to the invalid type casting and dereferencing of `bin` struct members (`bin->segment_entries` , `bin->entry_table`)

POC

poc 1: /format/ne/ne.c:413
poc_06

```
radare2 -q -A poc_06
```

poc 2: /format/ne/ne.c:418
poc_09

```
radare2 -q -A poc_09
```

poc 3: /format/ne/ne.c:411

poc_17

```
radare2 -q -A poc_17
```

ASAN

```
==2274169==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200
READ of size 2 at 0x602000066048 thread T0
    #0 0x7f3a58920612 in r_bin_ne_get_entrypoints /root/fuzzing/radare2_fuz
    #1 0x7f3a5891dd43 in entries /root/fuzzing/radare2_fuzzing/radare2/libr
    #2 0x7f3a58790b23 in r_bin_object_set_items /root/fuzzing/radare2_fuzzi
    #3 0x7f3a5878f818 in r_bin_object_new /root/fuzzing/radare2_fuzzing/rad
    #4 0x7f3a58789f44 in r_bin_file_new_from_buffer /root/fuzzing/radare2_f
    #5 0x7f3a58767d0b in r_bin_open_buf /root/fuzzing/radare2_fuzzing/radar
    #6 0x7f3a5876838f in r_bin_open_io /root/fuzzing/radare2_fuzzing/radare
    #7 0x7f3a5909356c in r_core_file_do_load_for_io_plugin /root/fuzzing/ra
    #8 0x7f3a59094e3d in r_core_bin_load /root/fuzzing/radare2_fuzzing/radc
    #9 0x7f3a5bb8d676 in r_main_radare2 /root/fuzzing/radare2_fuzzing/radar
    #10 0x555b9a2695f8 in main /root/fuzzing/radare2_fuzzing/radare2/binr/r
    #11 0x7f3a5b98f7fc in __libc_start_main ../csu/libc-start.c:332
    #12 0x555b9a269179 in _start (/root/fuzzing/radare2_fuzzing/radare2/bir

0x602000066048 is located 8 bytes to the left of 8-byte region [0x602000066
allocated by thread T0 here:
    #0 0x7f3a5c0947cf in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x7f3a5891e23a in __read_nonnull_str_at /root/fuzzing/radare2_fuzzin
    #2 0x7f3a5891fa44 in __ne_get_resources /root/fuzzing/radare2_fuzzing/r
    #3 0x7f3a58922ad8 in __init /root/fuzzing/radare2_fuzzing/radare2/libr/
    #4 0x7f3a58922c4b in r_bin_ne_new_buf /root/fuzzing/radare2_fuzzing/rad
    #5 0x7f3a5891c4e4 in load_buffer /root/fuzzing/radare2_fuzzing/radare2/
    #6 0x7f3a5878f52c in r_bin_object_new /root/fuzzing/radare2_fuzzing/rad
    #7 0x7f3a58789f44 in r_bin_file_new_from_buffer /root/fuzzing/radare2_f
    #8 0x7f3a58767d0b in r_bin_open_buf /root/fuzzing/radare2_fuzzing/radar
    #9 0x7f3a5876838f in r_bin_open_io /root/fuzzing/radare2_fuzzing/radare
    #10 0x7f3a5909356c in r_core_file_do_load_for_io_plugin /root/fuzzing/r
    #11 0x7f3a59094e3d in r_core_bin_load /root/fuzzing/rad
    #12 0x7f3a5bb8d676 in r_main_radare2 /root/fuzzing/radare2_fuzzing/rad
    #13 0x555b9a2695f8 in main /root/fuzzing/radare2_fuzzing/radare2/binr/r
```

```
    #14 0x7f3a5b98f7fc in __libc_start_main ../csu/libc-start.c:332

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/fuzzing/radare2_fuzzi
Shadow bytes around the buggy address:
  0x0c0480004bb0: fa fa 00 03 fa fa 00 03 fa fa 00 03 fa fa 07 fa
  0x0c0480004bc0: fa fa fd fa fa fa 06 fa fa fa fd fa fa fa 06 fa
  0x0c0480004bd0: fa fa fd fa fa fa 06 fa fa fa fd fa fa fa fd fa
  0x0c0480004be0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa 02 fa
  0x0c0480004bf0: fa fa fd fa fa fa fd fa fa fa 00 00 fa fa 01 fa
=>0x0c0480004c00: fa fa 00 00 fa fa 00 00 fa[fa]00 fa fa fa 00 00
  0x0c0480004c10: fa fa 00 00 fa fa 00 fa fa fa 00 00 fa fa 00 00
  0x0c0480004c20: fa fa 06 fa fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c0480004c30: fa fa 00 fa fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c0480004c40: fa fa 00 00 fa fa 00 fa fa fa 00 00 fa fa 00 fa
  0x0c0480004c50: fa fa 00 00 fa fa 00 fa fa fa 00 00 fa fa 00 fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
```

Impact

This vulnerability may allow attackers to read sensitive information or cause a crash

This vulnerability may allow attackers to read sensitive information or cause a crash.

Occurrences

ne.c L411 ne.c L418

CVE
CVE-2022-1297
(Published)

Vulnerability Type
CWE-125: Out-of-bounds Read

Severity
Medium (6.6)

Registry
Other

Affected Version
5.6.7

Visibility
Public

Status
Fixed

Found by

hmthabit
@hmthabit
unranked

Fixed by

pancake
@trufae
maintainer

This report was seen 567 times.

Chat with us

We are processing your report and will contact the radareorg/radare2 team within 24 hours.

8 months ago

pancake 8 months ago Maintainer

I can repro. working on the fix. thank you!

pancake validated this vulnerability 8 months ago

hmthabit has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

pancake marked this as fixed in 5.6.8 with commit 0a5570 8 months ago

pancake has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

ne.c#L418 has been validated ✓

ne.c#L411 has been validated ✓

Sign in to join this conversation