NULL Pointer Dereference in r_bin_ne_get_entrypoints function in radareorg/radare2

0

Valid Reported on Apr 6th 2022

Description

A NULL pointer deference vulnerability in `r_bin_ne_get_entrypoints` function due to a missing check before using the pointer.

Version

```
radare2 5.6.7 27746 @ linux-x86-64 git.5.6.6
commit: 2b77b277d67ce061ee6ef839e7139ebc2103c1e3 build: 2022-04-06__14:41:3
```

POC

```
radare2 -q -A poc
```

poc

Analysis

At `/format/ne/ne.c:383`, there's a deference of `bin->entry_table` without checking if it contains a valid pointer.

```
383         ut8 bundle_length = *(ut8 *)(bin->entry_table + off);     <<
384         if (!bundle_length) {
385                 break;
```

ASAN

```
=================================================================
==2195761==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000
==2195761==The signal is caused by a READ memory access.
==2195761==Hint: address points to the zero page.
    #0 0x7f0ebaffa472 in r_bin_ne_get_entrypoints /root/fuzzing/radare2_fuz
    #1 0x7f0ebaff5938 in entries /root/fuzzing/radare2_fuzzing/radare2/libr
    #2 0x7f0ebacd28e1 in r_bin_object_set_items /root/fuzzing/radare2_fuzzi
    #3 0x7f0ebacd1553 in r_bin_object_new /root/fuzzing/radare2_fuzzing/rad
    #4 0x7f0ebacbde4c in r_bin_file_new_from_buffer /root/fuzzing/radare2_f
    #5 0x7f0ebac7a4bc in r_bin_open_buf /root/fuzzing/radare2_fuzzing/radar
    #6 0x7f0ebac78ec7 in r_bin_open_io /root/fuzzing/radare2_fuzzing/radare
    #7 0x7f0ebbc04675 in r_core_file_do_load_for_io_plugin /root/fuzzing/rad
    #8 0x7f0ebbbfc969 in r_core_bin_load /root/fuzzing/radare2_fuzzing/radd
    #9 0x7f0ebecec2d2 in r_main_radare2 /root/fuzzing/radare2_fuzzing/radar
    #10 0x55fe077ace4f in main /root/fuzzing/radare2_fuzzing/radare2/binr/r
    #11 0x7f0ebea837fc in __libc_start_main csu/../csu/libc-start.c:332:16
```

Backtrace

```
pwndbg> bt
#0  0x00007ffff3a21472 in r_bin_ne_get_entrypoints (bin=0x608000020120) at
#1  0x00007ffff3a1c939 in entries (bf=0x60d0000006c0) at /root/fuzzing/radd
#2  0x00007ffff36f98e2 in r_bin_object_set_items (bf=0x60d0000006c0, bo=0x6
#3  0x00007ffff36f8554 in r_bin_object_new (bf=0x60d0000006c0, plugin=0x613
#4  0x00007ffff36e4e4d in r_bin_file_new_from_buffer (bin=0x616000000c80, f
#5  0x00007ffff36a14bd in r_bin_open_buf (bin=0x616000000c80, buf=0x603000
#6  0x00007ffff369fec8 in r_bin_open_io (bin=0x616000000c80, opt=0x7fffffff
#7  0x00007ffff462b676 in r_core_file_do_load_for_io_plugin (r=0x7fffee0328
#8  0x00007ffff462396a in r_core_bin_load (r=0x7fffee032800, filenameuri=0x
#9  0x00007ffff77132d3 in r_main_radare2 (argc=4, argv=0x7fffffffe498) at r
#10 0x000055555561ee50 in main (argc=4, argv=0x7fffffffe498) at radare2.c:9
#11 0x00007ffff74aa7fd in __libc_start_main (main=0x5555556
#12 0x00005555557753ba in _start ()
```

Impact

This vulnerability allows attackers to cause a denial of service (application crash).

CVE
CVE-2022-1283
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

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 602 times.

We are processing your report and will contact the radareorg/radare2 team
8 months ago

Chat with us

hmthabit modified the report 8 months ago

We have contacted a member of the **radareorg/radare2** team and are waiting to hear back 8 months ago

hmthabit modified the report 8 months ago

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 **18d1d0** 8 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation

terms

privacy policy

Chat with us