Heap-based Buffer Overflow in radareorg/radare2

Valid Reported on Feb 20th 2022

Description

heap-buffer-overflow /home/ubuntu/fuzz/radare2/libr/include/r_endian.h:176 in r_read_le32

Environment

```
Distributor ID: Ubuntu
Description:    Ubuntu 20.04 LTS
Release:    20.04
Codename:   focal

radare2 5.6.3 27472 @ linux-x86-64 git.5.6.2
commit: d24dbb9fbb0b398a6a739847008ccef3ea7e687c
```

ASAN

```
=================================================================
==3022342==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62400
READ of size 1 at 0x62400012dd3f thread T0
    #0 0x7f1a2103bcec in r_read_le32 /home/ubuntu/fuzz/radare2/libr/include
    #1 0x7f1a2103bcec in r_read_at_le32 /home/ubuntu/fuzz/radare2/libr/incl
    #2 0x7f1a2103bcec in r_read_le64 /home/ubuntu/fuzz/radare2/libr/include
    #3 0x7f1a2103bcec in r_coresym_cache_element_new /home/ubuntu/fuzz/rada
    #4 0x7f1a210323ea in parseDragons /home/ubuntu/fuzz/radare2/libr/..//l
    #5 0x7f1a210323ea in load_buffer /home/ubuntu/fuzz/radare2/libr/..//lib
    #6 0x7f1a210323ea in load_buffer /home/ubuntu/fuzz/radare2/libr/..//lib
    #7 0x7f1a20b08d17 in r_bin_object_new /home/ubuntu/fuzz/radare2/libr/bi
    #8 0x7f1a20af9db0 in r_bin_file_new_from_buffer /home/u
    #9 0x7f1a20ab4b67 in r_bin_open_buf /home/ubuntu/fuzz/r
    #10 0x7f1a20ab6009 in r_bin_open_io /home/ubuntu/fuzz/radare2/libr/bin/
```

```
    #11 0x7f1a218f82c8 in r_core_file_do_load_for_io_plugin /home/ubuntu/fu
    #12 0x7f1a218f82c8 in r_core_bin_load /home/ubuntu/fuzz/radare2/libr/co
    #13 0x7f1a218f82c8 in r_core_bin_load /home/ubuntu/fuzz/radare2/libr/co

    #14 0x7f1a24a062ba in r_main_radare2 /home/ubuntu/fuzz/radare2/libr/mai
    #15 0x7f1a247a50b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #16 0x560f17c179fd in _start (/home/ubuntu/fuzz/radare2/binr/radare2/ra

0x62400012dd3f is located 0 bytes to the right of 7231-byte region [0x62400
allocated by thread T0 here:
    #0 0x560f17d02a48 in __interceptor_malloc (/home/ubuntu/fuzz/radare2/bi
    #1 0x7f1a210355c1 in r_coresym_cache_element_new /home/ubuntu/fuzz/rada

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/ubuntu/fuzz/radare2/l
Shadow bytes around the buggy address:
  0x0c488001db50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c488001db60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c488001db70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c488001db80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c488001db90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c488001dba0: 00 00 00 00 00 00 00[07]fa fa fa fa fa fa fa fa
  0x0c488001dbb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c488001dbc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c488001dbd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c488001dbe0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c488001dbf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 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
  ==3022342==ABORTING
```

POC

```
./radare2 -qq -AA ./heap_overflow_poc
```

heap_overflow_poc

Impact

The bug causes the program reads data past the end of the intented buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.

CVE
CVE-2022-0713
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
Medium (5.3)

Visibility
Public

Status
Fixed

Found by

cnitlrt
@cnitlrt

master

Fixed by

pancake

@trufae

maintainer

This report was seen 537 times.

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

cnitlrt modified the report 9 months ago

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

pancake validated this vulnerability 9 months ago

cnitlrt has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

pancake marked this as fixed in **5.6.4** with commit **a35f89** 9 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation