huntr

Heap-based Buffer Overflow in radareorg/radare2

0

✔ **Valid** Reported on Apr 14th 2022

Description

Heap-based Buffer Overflow in r_read_le32

Environment

```
radare2 5.6.7 0 @ linux-x86-64 git.
commit: 5.6.7 build: 2022-04-12__15:06:26
```

Build

```
export CC=gcc CXX=g++ CFLAGS="-fsanitize=address -static-libasan" CXXFLAGS=
./configure && make
```

◀ ▬▬▬▬▬▬▬▬▬▬▬ ▶

POC

```
radare2 -q -A ./poc
```

poc

Asan

```
=================================================================
==3071761==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62400
READ of size 1 at 0x62400012dd3f thread T0
    #0 0x7fc8a4099d73 in r_read_le32 /home/ubuntu/radare2-master/libr/in
    #1 0x7fc8a4099d73 in r_read_at_le32 /home/ubuntu/radare2-master/libr/in
```

```
    #1 0x7fc8a4099d73 in r_read_at_le32 /home/ubuntu/radare2-master/libr/i
    #2 0x7fc8a4099d73 in r_read_le64 /home/ubuntu/radare2-master/libr/inclu
    #3 0x7fc8a4099d73 in r_read_ble64 /home/ubuntu/radare2-master/libr/incl
    #4 0x7fc8a4099d73 in r_read_ble /home/ubuntu/radare2-master/libr/inclu
    #5 0x7fc8a4099d73 in r_coresym_cache_element_new /home/ubuntu/radare2-m
    #6 0x7fc8a408feb3 in parseDragons /home/ubuntu/radare2-master/libr/..//
    #7 0x7fc8a408feb3 in load_buffer /home/ubuntu/radare2-master/libr/..//l
    #8 0x7fc8a408feb3 in load_buffer /home/ubuntu/radare2-master/libr/..//l
    #9 0x7fc8a3b6605a in r_bin_object_new /home/ubuntu/radare2-master/libr/
    #10 0x7fc8a3b576f3 in r_bin_file_new_from_buffer /home/ubuntu/radare2-m
    #11 0x7fc8a3b12697 in r_bin_open_buf /home/ubuntu/radare2-master/libr/b
    #12 0x7fc8a3b13a6f in r_bin_open_io /home/ubuntu/radare2-master/libr/bi
    #13 0x7fc8a495fd2f in r_core_file_do_load_for_io_plugin /home/ubuntu/ra
    #14 0x7fc8a495fd2f in r_core_bin_load /home/ubuntu/radare2-master/libr/
    #15 0x7fc8a495fd2f in r_core_bin_load /home/ubuntu/radare2-master/libr/
    #16 0x7fc8a76859d2 in r_main_radare2 /home/ubuntu/radare2-master/libr/m
    #17 0x7fc8a74210b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #18 0x5604fe78babd in _start (/home/ubuntu/radare2-master/binr/radare2/

0x62400012dd3f is located 0 bytes to the right of 7231-byte region [0x62400
allocated by thread T0 here:
    #0 0x5604fe876b08 in __interceptor_malloc (/home/ubuntu/radare2-master/
    #1 0x7fc8a40932a4 in r_coresym_cache_element_new /home/ubuntu/radare2-m

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/ubuntu/radare2-master
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
```

Chat with us

```
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
==3071761==ABORTING
```

◄   ►

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-2022-1383
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
Medium (4.8)

Registry
Other

Affected Version
5.6.7

Visibility
Public

Chat with us

Status
Fixed

Found by

cnitlrt
@cnitlrt
master ⌄

Fixed by

pancake
@trufae
maintainer

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

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

pancake validated this vulnerability 7 months ago

cnitlrt has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

pancake marked this as fixed in **5.6.8** with commit **1dd653** 7 months ago

pancake has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us