

# heap-buffer-overflow in radareorg/radare2

2

✓ Valid

Reported on Apr 5th 2022

## Description

Whilst experimenting with `radare2`, built from version `5.6.6`, we are able to induce a vulnerability at `bin_dyldcache.c:125` in function `va2pa`, using `radare2` as a harness.

```
118: static ut64 va2pa(uint64_t addr, ut32 n_maps, cache_map_t *maps, RBu
119:     ut64 res = UT64_MAX;
120:     ut32 i;
121:
122:     addr -= slide;
123:
124:     for (i = 0; i < n_maps; i++) {
//heap buffer overflow here
125:         if (addr >= maps[i].address && addr < maps[i].address + maps[i]
126:             res = maps[i].fileOffset + addr - maps[i].address;
127:             if (offset) {
128:                 *offset = addr - maps[i].address;
129:             }
130:             if (left) {
131:                 *left = maps[i].size - (addr - maps[i].address);
132:             }
133:             break;
134:         }
135:     }
```

Because there is no proper bounds checking, a heap-based out-of-bound read will be triggered when the software encounters a malformed file, which could result in denial of service.

We also found that the vulnerability exists in the master branch as well.

Chat with us

## Environment

Ubuntu 20.04 LTS x86\_64

gcc 10.3.0

clang 12.0.1

## Proof of Concept

The POC is: [poc](#)

The reproducing process is:

```
# build with address sanitizer
SANITIZE=address ./sys/sanitize.sh
# disable some features of address sanitizer to avoid false positives
export ASAN_OPTIONS=detect_leaks=0:abort_on_error=1:symbolize=1:allocator_n
# trigger the crash
./radare2 -AA -qq POC_FILE
```

The ASAN report is:

```
=====
==123279==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fffec
READ of size 8 at 0x7fffed4d7000 thread T0
#0 0x7ffff3d8b427 in va2pa /work/libraries/radare2-latest/libr/./libr
#1 0x7ffff3d946a6 in create_cache_bins /work/libraries/radare2-latest/li
#2 0x7ffff3d99489 in load_buffer /work/libraries/radare2-latest/libr/..
#3 0x7ffff3d2b371 in r_bin_object_new /work/libraries/radare2-latest/li
#4 0x7ffff3d25d77 in r_bin_file_new_from_buffer /work/libraries/radare2
#5 0x7ffff3d037bb in r_bin_open_buf /work/libraries/radare2-latest/libr
#6 0x7ffff3d03e42 in r_bin_open_io /work/libraries/radare2-latest/libr/
#7 0x7ffff463c094 in r_core_file_do_load_for_io_plugin /work/libraries/
#8 0x7ffff463d9b7 in r_core_bin_load /work/libraries/radare2-latest/li
#9 0x7ffff717b333 in r_main_radare2 /work/libraries/radare2-latest/libr
#10 0x5555555556ff in main /work/libraries/radare2-latest/binr/radare2/
#11 0x7ffff6f630b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
#12 0x55555555528d in _start (/work/libraries/radare2-l
```

Chat with us

0x7fffed4d7000 is located 0 bytes to the right of 12503040-byte region [0x7

allocated by thread T0 here:

```
#0 0x7ffff7693e17 in __interceptor_calloc ../../../../src/libsanitizer/
#1 0x7ffff3d97b0e in populate_cache_maps /work/libraries/radare2-latest/

#2 0x7ffff3d99334 in load_buffer /work/libraries/radare2-latest/libr/..
#3 0x7ffff3d2b371 in r_bin_object_new /work/libraries/radare2-latest/li
#4 0x7ffff3d25d77 in r_bin_file_new_from_buffer /work/libraries/radare2
#5 0x7ffff3d037bb in r_bin_open_buf /work/libraries/radare2-latest/libr
#6 0x7ffff3d03e42 in r_bin_open_io /work/libraries/radare2-latest/libr/
#7 0x7ffff463c094 in r_core_file_do_load_for_io_plugin /work/libraries/
#8 0x7ffff463d9b7 in r_core_bin_load /work/libraries/radare2-latest/li
#9 0x7ffff717b333 in r_main_radare2 /work/libraries/radare2-latest/libr
#10 0x55555555556ff in main /work/libraries/radare2-latest/bin/radare2/
#11 0x7ffff6f630b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
```

SUMMARY: AddressSanitizer: heap-buffer-overflow /work/libraries/radare2-latest/

Shadow bytes around the buggy address:

```
0x10007da92db0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x10007da92dc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x10007da92dd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x10007da92de0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x10007da92df0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10007da92e00:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x10007da92e10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x10007da92e20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x10007da92e30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x10007da92e40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x10007da92e50: fa 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
```

Chat with us

```
Container overflow:  tc
Array cookie:       ac
Intra object redzone: bb

ASan internal:      fe
Left alloca redzone: ca
Right alloca redzone: cb
Shadow gap:        cc
```

```
==123279==ABORTING
```

```
Aborted
```



## Impact

This vulnerability is capable of inducing denial of service.

### CVE

CVE-2022-1244

(Published)

### Vulnerability Type

CWE-122: Heap-based Buffer Overflow

### Severity

High (7.5)

### Registry

Other

### Affected Version

5.6.6

### Visibility

Public

### Status

Fixed

### Found by



hdthky

@hdthky

unranked ▼

Chat with us

Fixed by



pancake

@trufae

[maintainer](#)

This report was seen 800 times.

We are processing your report and will contact the [radareorg/radare2](#) team within 24 hours.  
8 months ago

pancake [8 months ago](#)

i confirm this issue is a thing. looking forward to fix it

pancake validated this vulnerability 8 months ago

hdthky 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 **2b77b2** 8 months ago

pancake has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

hdthky [7 months ago](#)

Researcher

This bug was found by Xingyuan Mo from 360 IceSword Lab

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 4l8sec

company

about

team

Chat with us