NULL Pointer Dereference in radareorg/radare2

Valid Reported on Jan 28th 2022

0

NULL pointer dereference in `load_buffer`

radare2 suffers from a NULL pointer dereference error in `load_buffer` of `bin_xnu_kernelcache.c`

Environment

```
date
Fri Jan 28 11:03:53 PST 2022
```

```
uname -ms
Linux x86_64
```

```
./radare2 -v
radare2 5.5.5 27531 @ linux-x86-64 git.5.5.4
commit: 715c4e0ff14aadd4026c182626502df3f3a620ab build: 2022-01-28__08:00:4
```

ASAN

Address sanitizer output :

```
./radare2 -qq -AA nullpointerdereference
ASAN:DEADLYSIGNAL
=================================================================
==54209==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (p
```

```
==54209==The signal is caused by a WRITE memory access.
==54209==Hint: address points to the zero page.
    #0 0x7f9148ecf485 in load_buffer /home/shad3/Desktop/radare2-asan/libr/

    #1 0x7f9148c0fcee in r_bin_object_new /home/shad3/Desktop/radare2-asan/
    #2 0x7f9148c0a779 in r_bin_file_new_from_buffer /home/shad3/Desktop/rac
    #3 0x7f9148be8bf3 in r_bin_open_buf /home/shad3/Desktop/radare2-asan/li
    #4 0x7f9148be9279 in r_bin_open_io /home/shad3/Desktop/radare2-asan/lib
    #5 0x7f9149b79010 in r_core_file_do_load_for_io_plugin /home/shad3/Desk
    #6 0x7f9149b7a8f6 in r_core_bin_load /home/shad3/Desktop/radare2-asan/l
    #7 0x7f914df1fdc4 in r_main_radare2 /home/shad3/Desktop/radare2-asan/li
    #8 0x556796be6204 in main /home/shad3/Desktop/radare2-asan/binr/radare2
    #9 0x7f914db05bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6
    #10 0x556796be5d79 in _start (/home/shad3/Desktop/radare2-asan/binr/rac

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/shad3/Desktop/radare2-asan/libr/..//l
==54209==ABORTING
```

Explanation of the vulnerability

The vulnerability lies in the file

```
radare2/libr/bin/p/bin_xnu_kernelcache.c
```

Please consider the following code:

```
static bool load_buffer(RBinFile *bf, void **bin_obj, RBuffer *buf, ut64 lo
    ...
189 RKernelCacheObj *obj = NULL; // 1

191 RPrelinkRange *prelink_range = get_prelink_info_range_from_mach0 (main_
192 if (!prelink_range) {
193     goto beach;              // 2
194 }

....
```

```
243 beach:
244 r_buf_free (fbuf);
245 obj->cache_buf = NULL;        // 3
```

```
244 MACH0_(mach0_free) (main_mach0);
245 return false;
```

In case where the `get_prelink_info_range_from_mach0` fails (2) and the returned value is zero the programm will crash with a segfault at line 245 (3) since the `obj` pointer is being dereferenced, while being set as NULL on line 189 (1). (Write on address 0x0)

Attached POC

You can find the attached poc that triggers the vulnerability in the following link
Password : A7htCTD6Oli6rf1Waoz1
`nullpointerdereference`
Run as:

```
./radare2 -qq -AA nullpointerdereference
```

CVE
CVE-2022-0419
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (5.9)

Visibility
Public

Status
Fixed

Found by

Angelos T. Kalaitzidis
@0xshad3
unranked

This report was seen 468 times.

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

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

pancake validated this vulnerability 10 months ago

Angelos T. Kalaitzidis has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

pancake marked this as fixed in **5.6.0** with commit **feaa4e** 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Angelos 10 months ago — Researcher

@admin the description on the published CVE, seems to be wrong, can you please change that, thank you.

Jamie Slome 10 months ago — Admin

Updating it here:
https://github.com/CVEProject/cvelist/pull/4292

Once this has been merged the CVE should be populated and corrected. Not sure what happened here, apologies!

pancake 10 months ago — Maintainer

The correct version is 5.6.0, sorry for my mistake here. Could you make anoth
that? Should I?

Jamie Slome 10 months ago Admin

@truefae - resolved here. Once this has been merged the CVE will be updated to reflect 5.6.0.

Thanks! 🎊

> Sign in to join this conversation