NULL Pointer Dereference in radareorg/radare2

Valid Reported on Feb 20th 2022

Description

NULL pointer dereference in bin_symbols.c

Environment

```
Distributor ID: Ubuntu
Description:    Ubuntu 20.04 LTS
Release:    20.04
Codename:   focal

radare2 5.6.3 27472 @ linux-x86-64 git.5.6.2
commit: d24dbb9fbb0b398a6a739847008ccef3ea7e687c
```

POC

```
radare2 -AA -qq ./poc
```

poc

ASAN

```
=================================================================
==2968491==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000
==2968491==The signal is caused by a READ memory access.
==2968491==Hint: address points to the zero page.
    #0 0x7fe53d2ad411 in symbols /home/ubuntu/fuzz/radare2/l
    #1 0x7fe53cd844ec in r_bin_object_set_items /home/ubunt
    #2 0x7fe53cd87d87 in r_bin_object_new /home/ubuntu/fuzz/radare2/libr/bi
```

```
    #3 0x7fe53cd78db0 in r_bin_file_new_from_buffer /home/ubuntu/fuzz/radar
    #4 0x7fe53cd33b67 in r_bin_open_buf /home/ubuntu/fuzz/radare2/libr/bin/
    #5 0x7fe53cd35009 in r_bin_open_io /home/ubuntu/fuzz/radare2/libr/bin/b

    #6 0x7fe53db772c8 in r_core_file_do_load_for_io_plugin /home/ubuntu/fuz
    #7 0x7fe53db772c8 in r_core_bin_load /home/ubuntu/fuzz/radare2/libr/cor
    #8 0x7fe53db772c8 in r_core_bin_load /home/ubuntu/fuzz/radare2/libr/cor
    #9 0x7fe540c852ba in r_main_radare2 /home/ubuntu/fuzz/radare2/libr/mair
    #10 0x7fe540a240b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #11 0x559b96c449fd in _start (/home/ubuntu/fuzz/radare2/binr/radare2/ra

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/ubuntu/fuzz/radare2/libr/..//libr/bi
==2968491==ABORTING
```

Impact

This vulnerability is capable of making the radare2 crash, thus affecting the availability of the system.

CVE
CVE-2022-0712
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (5.9)

Visibility
Public

Status
Fixed

Found by

cnitlrt
@cnitlrt
master

Chat with us

Fixed by

pancake

@trufae

maintainer

This report was seen 485 times.

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

cnitlrt modified the report 9 months ago

cnitlrt modified the report 9 months ago

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

pancake validated this vulnerability 9 months ago

cnitlrt has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

pancake marked this as fixed in **5.6.4** with commit **515e59** 9 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation