NULL Pointer Dereference in radareorg/radare2

Valid Reported on Apr 13th 2022

0

Description

NULL pointer dereference in r_bin_ne_get_segments

Environment

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

radare2 5.6.7 0 @ linux-x86-64 git.
commit: 5.6.7
```

Build

```
export CC=gcc CXX=g++ CFLAGS="-fsanitize=address -static-libasan" CXXFLAGS=
./configure && make
```

POC

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

poc

ASAN

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==945410==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000002 (
==945410==The signal is caused by a READ memory access.
==945410==Hint: address points to the zero page.
    #0 0x7f38cb2b3dc3 in r_bin_ne_get_segments /home/ubuntu/radare2-master/
    #1 0x7f38caed7304 in r_bin_object_set_items /home/ubuntu/radare2-master
    #2 0x7f38caed90ca in r_bin_object_new /home/ubuntu/radare2-master/libr/
    #3 0x7f38caeca6f3 in r_bin_file_new_from_buffer /home/ubuntu/radare2-ma
    #4 0x7f38cae85697 in r_bin_open_buf /home/ubuntu/radare2-master/libr/bi
    #5 0x7f38cae86a6f in r_bin_open_io /home/ubuntu/radare2-master/libr/bir
    #6 0x7f38cbcd2d2f in r_core_file_do_load_for_io_plugin /home/ubuntu/rad
    #7 0x7f38cbcd2d2f in r_core_bin_load /home/ubuntu/radare2-master/libr/c
    #8 0x7f38cbcd2d2f in r_core_bin_load /home/ubuntu/radare2-master/libr/c
    #9 0x7f38ce9f89d2 in r_main_radare2 /home/ubuntu/radare2-master/libr/ma
    #10 0x7f38ce7940b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #11 0x55957465dabd in _start (/home/ubuntu/radare2-master/binr/radare2/

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/ubuntu/radare2-master/libr/..//libr/b
==945410==ABORTING
```

Impact

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

CVE
CVE-2022-1382
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (5.3)

Registry
Other

Affected Version

5.6.7

Visibility
Public

Status
Fixed

Found by

cnitlrt
@cnitlrt
master

Fixed by

pancake
@trufae
maintainer

This report was seen 544 times.

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

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

cnitlrt modified the report 7 months ago

pancake validated this vulnerability 7 months ago

cnitlrt has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

pancake marked this as fixed in **5.6.8** with commit **48f0ea** 7 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

This vulnerability will not receive a CVE

Sign in to join this conversation