Null pointer dereference in libr/bin/format/mach0/mach0.c in radareorg/radare2 in radareorg/radare2

0

Valid Reported on May 9th 2022

This vulnerability is of type heap-buffer-overflow. And after quick investigation I think it is very likely to be successfully exploited to remote code execution. The bug exists in latest stable release (radare2-5.6.8) and lastest master branch (5a9e0a19ba07e35382776fed9da2649ac824f526, updated in May 09, 2022). Specifically, the vulnerable code (located at libr/bin/format/mach0/mach0.c) and the bug's basic explanation are highlighted as follows:

```
4578                                ut64 page_end_idx = (R_MIN (limit_end, end)
4579                                for (; page_idx <= page_end_idx; page_idx++
4580                                        if (page_idx >= bin->chained_starts
4581                                                break;
4582                                        }
// Null pointer dereference here.
4583                                        ut16 page_start = bin->chained_star
4584                                        if (page_start == DYLD_CHAINED_PTR_
4585                                                continue;
4586                                        }
4587                                        ut64 cursor = start + page_idx * pa
```

Build the radare2 (5a9e0a19ba07e35382776fed9da2649ac824f526, updated in May 09, 2022) and run it using the input POC.

```
# build the radare2 with address sanitizer
export CFLAGS=" -fsanitize=address "; export CXXFLAGS=" -fsanitize=address
CFGARG=" --enable-shared=no " PREFIX=`realpath install` bash
# disable some features of address sanitizer to avoid false
export ASAN_OPTIONS=detect_leaks=0:abort_on_error=1:symbolize=0:allocator_m
```

```
# trigger the crash
./radare2 -A -q POC_FILE
```

The crash stack is:

```
==17553==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (p
==17553==The signal is caused by a READ memory access.
==17553==Hint: address points to the zero page.
    #0 0x7f22529f7d6e  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #1 0x7f22529b481e  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #2 0x7f225653869b  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #3 0x7f2256d42087  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #4 0x7f2256d2b614  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #5 0x7f22529ef49f  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #6 0x7f22529f481b  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #7 0x7f22526f66d9  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #8 0x7f22526f4cd2  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #9 0x7f22526d9b65  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #10 0x7f225267db72  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/
    #11 0x7f225267cb54  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/
    #12 0x7f2253910893  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/
    #13 0x7f2256acc154  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/
    #14 0x7f225683a0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #15 0x5634bce5339d  (/src/cmdline-fuzz/exprs/radare2-5.5.4/radare2+0x1e

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/
==17553==ABORTING
Aborted
```

Impact

It is likely to be exploitable. For more general description of heap buffer overflow, see CWE.

References

- Poc files

CVE
CVE-2022-1649

(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
High (7.6)

Registry
Other

Affected Version
5.6.8

Visibility
Public

Status
Fixed

Found by

Han0nly
@han0nly
legend

Fixed by

pancake
@trufae
maintainer

This report was seen 526 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

pancake validated this vulnerability 7 months ago

Han0nly has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

pancake marked this as fixed in 5.7.0 with commit a5aafb 7 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation