New issue

Jump to bottom

memory allocation of 18446744073709551610 bytes failed[1] #30

Closed p870613 opened this issue on Aug 9, 2021 · 4 comments

p870613 commented on Aug 9, 2021

HI !
I found a `memory allocation of 18446744073709551610 bytes failed` in the current master e232665
POC : poc.zip

```
$ ./bingrep out/default/crashes/poc
ELF EXEC EM_UNKNOWN-little-endian @ 0x8049080:

e_phoff: 0x80 e_shoff: 0xc e_flags: 0x10000 e_ehsize: 0 e_phentsize: 3 e_phnum: 0 e_shentsize: 36992 e_shnum: 2 e_shstrndx: 0

ProgramHeaders(0):


SectionHeaders(2):
memory allocation of 18446744073709551610 bytes failed[1]    552937 abort      ./bingrep out/default/crashes/poc
```

3

p870613 commented on Jan 24 Author

Assigned CVE-2021-39480.

m4b commented on Jan 24 Owner

Hello there! thanks for filing, let me see if this is fixed in later goblins, there was some checks done semi recently for sizes being required to be less than size of the binary being analyzed (which I believe is only practical solution to a section claiming it requires X amount of bytes)

m4b commented on Jan 24 • edited Owner

Ok looks like 0.9.0 doesn't have a bad memory allocation for your POC (it does unfortunately, have an absolutely atrocious error message 😈):

```
target/release/bingrep poc
bad input invalid utf8 (5)
```

for reference here is previous output of 0.8.5:

```
bingrep poc
ELF EXEC EM_UNKNOWN-little-endian @ 0x8049080:

e_phoff: 0x80 e_shoff: 0xc e_flags: 0x10000 e_ehsize: 0 e_phentsize: 3 e_phnum: 0 e_shentsize: 36992 e_shnum: 2 e_shstrndx: 0

ProgramHeaders(0):


SectionHeaders(2):
memory allocation of 18446744073709551610 bytes failedAborted (core dumped)
```

the output is nice(r), the core dump however is not :)

p870613 commented on Feb 7 Author

That's good.

Thanks !!!

p870613 closed this as completed on Feb 7

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants