New issue

Jump to bottom

[BUG] stack exhaustion in function `compile`, mujs #162

Closed **kdsjZh** opened this issue on May 15 · 4 comments

kdsjZh commented on May 15 • edited

Brief summary

Hello, I was testing my fuzzer and found an echaustion bug in mujs. A stack exhaustion in function compile will be triggered when parsing a crafted js file, when `running ./mujs $POC`, as shown in the attachment

Compiling the program

I compile mujs's latest commit `db110ea` in ubuntu 22 (docker image) with clang version 12.0.1.
With command `CC=clang make build=sanitize`
In my test environment this bug cannot be reproduced if compiled via gcc so it's recommended to compile with clang-12

ASan output

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2685261==ERROR: AddressSanitizer: stack-overflow on address 0x7fff23e67f98 (pc 0x0000005424b3 bp
0x7fff23e683b0 sp 0x7fff23e67fa0 T0)
    #0 0x5424b3 in compile /benchmark/mujs/./regexp.c:674:11
    #1 0x5424f9 in compile /benchmark/mujs/./regexp.c:675:3
    #2 0x5424f9 in compile /benchmark/mujs/./regexp.c:675:3
    #3 0x5424f9 in compile /benchmark/mujs/./regexp.c:675:3
    #4 0x5424f9 in compile /benchmark/mujs/./regexp.c:675:3
    #5 0x5424f9 in compile /benchmark/mujs/./regexp.c:675:3
    #6 0x5424f9 in compile /benchmark/mujs/./regexp.c:675:3
    #7 0x5424f9 in compile /benchmark/mujs/./regexp.c:675:3
...
    #248 0x5424f9 in compile /benchmark/mujs/./regexp.c:675:3

SUMMARY: AddressSanitizer: stack-overflow /benchmark/mujs/./regexp.c:674:11 in compile
==2685261==ABORTING
```

POC

poc0.zip

Credit

Han Zheng
NCNIPC of China
Hexhive

ccxvii commented on May 17 — Owner

I don't have clang-12 can it be replicated with clang-11?

kdsjZh commented on May 17 • edited — Author

You can try with clang-11, pls let me know if it cannot be reproduced, I'll try to give you a set of instructions to reproduce via docker images.

kdsjZh commented on May 17 • edited — Author

My steps to reproduce via docker, if you failed in your environment, you could try the following.

```
docker pull ubuntu:22.04
# start a container
apt update && apt install vim git gcc make g++ wget libreadline-dev unzip -y
vim /etc/apt/source.list
# add clang's source for ubuntu 22.04, which can be found in https://apt.llvm.org/
# add gpg key
wget  https://apt.llvm.org/llvm-snapshot.gpg.key  && apt-key add llvm-snapshot.gpg.key
apt install clang-12 -y
git clone https://github.com/ccxvii/mujs && pushd mujs
wget https://github.com/ccxvii/mujs/files/8694862/poc0.zip && unzip poc0.zip
CC=clang-12 make build=sanitize && ./build/sanitize/mujs poc0
```

ccxvii added a commit that referenced this issue on May 17

Issue #162: Check stack overflow during regexp compilation. ... 160ae29

ccxvii commented on May 17 Owner

The recent commit will limit recursion during compilation, so should solve this issue.

👍 1

ccxvii closed this as completed on May 17

---

ccxvii added a commit that referenced this issue on May 17

`Issue #162: Cope with empty programs in mujs-pp.` `799b62b`

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants