New issue

Jump to bottom

Segfault in njs_json_stringify_iterator #322

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

Assignees

Labels bug fluff fuzzer

Changochen commented on Jun 27, 2020

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

POC:

```
var array = [];
var funky;
funky = {
  get value() { array[10000000] = 12; }
};
for (var i = 0; i < 10; i++)
  array[i] = i;
array[3] = funky;
'' == JSON.stringify(array);
```

cmd: `njs poc.js`

Stack dump:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==181398==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000040 (pc 0x7f2cbf620477 bp 0x7fff1a082ad0 sp 0x7fff1a082288 T0)
==181398==The signal is caused by a READ memory access.
==181398==Hint: address points to the zero page.
    #0 0x7f2cbf620477 in memcpy /build/glibc-OTsEL5/glibc-2.27/string/../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:139
    #1 0x4938d1 in __asan_memcpy /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cpp:22:3
    #2 0x5eb14a in njs_json_stringify_iterator /home/yongheng/njs/src/njs_json.c:1317:33
    #3 0x5eb14a in njs_json_stringify /home/yongheng/njs/src/njs_json.c:283:12
    #4 0x5ff82e in njs_function_native_call /home/yongheng/njs/src/njs_function.c:707:11
    #5 0x507611 in njs_function_frame_invoke /home/yongheng/njs/src/njs_function.h:172:16
    #6 0x507611 in njs_vmcode_interpreter /home/yongheng/njs/src/njs_vmcode.c:778:23
    #7 0x4c8f01 in njs_process_script /home/yongheng/njs/src/njs_shell.c:843:19
    #8 0x4c68ce in njs_process_file /home/yongheng/njs/src/njs_shell.c:562:11
    #9 0x4c68ce in main /home/yongheng/njs/src/njs_shell.c:286:15
    #10 0x7f2cbf586b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #11 0x41c089 in _start (/home/yongheng/njs/build/njs+0x41c089)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /build/glibc-OTsEL5/glibc-2.27/string/../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:139 in memcpy
==181398==ABORTING
```

xeioex added bug fluff fuzzer labels on Jun 28, 2020

xeioex assigned **lexborisov** on Sep 10, 2020

nginx-hg-mirror closed this as completed in `63aa001` on Oct 6, 2020

Assignees

lexborisov

Labels

bug fluff fuzzer

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants