nginx / njs Public

Code Issues 41 Pull requests 2 Actions Security Insights

New issue Jump to bottom

Null pointer dereference in src/njs_vmcode.c:1049:17 #473

Closed andreafioraldi opened this issue on Feb 17 · 0 comments

Labels bug fuzzer

andreafioraldi commented on Feb 17

Hi,
this bug was found by fuzzing the current master branch, to reproduce build the OSS-Fuzz harness with ASan and UBSan.

The bug is a write to a NULL pointer, this is the sanitizer report:

```
INFO: Seed: 2125423890
INFO: Loaded 1 modules   (53334 inline 8-bit counters): 53334 [0x95f010, 0x96c066),
INFO: Loaded 1 PC tables (53334 PCs): 53334 [0x96c068,0xa3c5c8),
/out/njs_process_script_fuzzer: Running 1 inputs 1 time(s) each.
Running:
crashes/njs_njs_process_script_fuzzer/id:000002,sig:06,src:001260+005121,time:65254059,op:splice,rep:

src/njs_vmcode.c:1049:17: runtime error: member access within null pointer of type 'njs_value_t'
(aka 'union njs_value_s')
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior src/njs_vmcode.c:1049:17 in
AddressSanitizer:DEADLYSIGNAL
=================================================================
==1324882==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000005394e8 bp
0x7fffffffd4f0 sp 0x7fffffffd4c0 T0)
==1324882==The signal is caused by a WRITE memory access.
==1324882==Hint: address points to the zero page.
    #0 0x5394e8 in njs_vmcode_array /src/njs/src/njs_vmcode.c:1049:17
    #1 0x52b41d in njs_vmcode_interpreter /src/njs/src/njs_vmcode.c:580:23
    #2 0x52472e in njs_vm_start /src/njs/src/njs_vm.c:487:11
    #3 0x4ffe8e in njs_process_script (/out/njs_process_script_fuzzer+0x4ffe8e)
    #4 0x4ff759 in LLVMFuzzerTestOneInput (/out/njs_process_script_fuzzer+0x4ff759)
    #5 0x4e0b39 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long)
(/out/njs_process_script_fuzzer+0x4e0b39)
    #6 0x4cba49 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long)
(/out/njs_process_script_fuzzer+0x4cba49)
    #7 0x4d0952 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned
long)) (/out/njs_process_script_fuzzer+0x4d0952)
```

```
    #8 0x4cb7d2 in main (/out/njs_process_script_fuzzer+0x4cb7d2)
    #9 0x7ffff77050b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #10 0x42101d in _start (/out/njs_process_script_fuzzer+0x42101d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /src/njs/src/njs_vmcode.c:1049:17 in njs_vmcode_array
==1324882==ABORTING
```

I attach the crashing testcase in a tar.gz, you can run it simply giving the testcase as first argument to the harness.

id:000002,sig:06,src:001260+005121,time:65254059,op:splice,rep:2,trial:1496856.tar.gz

xeioex added bug fuzzer labels on Feb 17

nginx-hg-mirror closed this as completed in `f65981b` on Feb 21

Assignees

No one assigned

Labels

bug fuzzer

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants