nginx / njs Public

<> Code ⊙ Issues 41 Pull requests 2 Actions Security Insights

New issue

Jump to bottom

Patch bypass for njs_await_fulfilled, causing UAF again #469

Closed P1umer opened this issue on Feb 15 · 3 comments

Labels bug fuzzer

P1umer commented on Feb 15 • edited by xeioex

This UAF was introduced in a patch for a similar bug #451, which shows that njs_await_fulfilled is still flawed.

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  : 7bd570b39297d3d91902c93a624c89b08be7a6fe
Version : 0.7.2
Build   :
          NJS_CFLAGS="$NJS_CFLAGS -fsanitize=address"
          NJS_CFLAGS="$NJS_CFLAGS -fno-omit-frame-pointer"
```

Proof of concept

```
async function a0(v) {
    await 1;
    a0();
}
a0();
```

Stack dump

```
=================================================================
==2064567==ERROR: AddressSanitizer: heap-use-after-free on address 0x62500009da60 at pc
0x00000049595f bp 0x7ffdd8c90f20 sp 0x7ffdd8c906e8
WRITE of size 88 at 0x62500009da60 thread T0
```

```
    #0 0x49595e in __asan_memset (/home/p1umer/Documents/origin/njs/build/njs+0x49595e)
    #1 0x53947f in njs_function_frame_alloc
/home/p1umer/Documents/origin/njs/src/njs_function.c:574:5
    #2 0x5397a7 in njs_function_lambda_frame
/home/p1umer/Documents/origin/njs/src/njs_function.c:466:20
    #3 0x4eae3e in njs_function_frame /home/p1umer/Documents/origin/njs/src/njs_function.h:155:16
    #4 0x4eae3e in njs_function_frame_create
/home/p1umer/Documents/origin/njs/src/njs_vmcode.c:1740:16
    #5 0x4e32e8 in njs_vmcode_interpreter
/home/p1umer/Documents/origin/njs/src/njs_vmcode.c:736:23
    #6 0x605ecc in njs_await_fulfilled /home/p1umer/Documents/origin/njs/src/njs_async.c:96:11
    #7 0x53bf9c in njs_function_native_call
/home/p1umer/Documents/origin/njs/src/njs_function.c:739:11
    #8 0x53a5d9 in njs_function_frame_invoke
/home/p1umer/Documents/origin/njs/src/njs_function.c:777:16
    #9 0x53a5d9 in njs_function_call2 /home/p1umer/Documents/origin/njs/src/njs_function.c:600:11
    #10 0x5f53c7 in njs_function_call /home/p1umer/Documents/origin/njs/src/njs_function.h:180:12
    #11 0x5f53c7 in njs_promise_reaction_job
/home/p1umer/Documents/origin/njs/src/njs_promise.c:1171:15
    #12 0x53bf9c in njs_function_native_call
/home/p1umer/Documents/origin/njs/src/njs_function.c:739:11
    #13 0x4de620 in njs_vm_invoke /home/p1umer/Documents/origin/njs/src/njs_vm.c:375:12
    #14 0x4de620 in njs_vm_call /home/p1umer/Documents/origin/njs/src/njs_vm.c:359:12
    #15 0x4de620 in njs_vm_handle_events /home/p1umer/Documents/origin/njs/src/njs_vm.c:524:19
    #16 0x4de620 in njs_vm_run /home/p1umer/Documents/origin/njs/src/njs_vm.c:479:12
    #17 0x4c8407 in njs_process_script /home/p1umer/Documents/origin/njs/src/njs_shell.c:937:15
    #18 0x4c7484 in njs_process_file /home/p1umer/Documents/origin/njs/src/njs_shell.c:632:11
    #19 0x4c7484 in main /home/p1umer/Documents/origin/njs/src/njs_shell.c:316:15
    #20 0x7f03823f40b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #21 0x41dabd in _start (/home/p1umer/Documents/origin/njs/build/njs+0x41dabd)

0x62500009da60 is located 352 bytes inside of 8192-byte region [0x62500009d900,0x62500009f900)
freed by thread T0 here:
    #0 0x495f7d in free (/home/p1umer/Documents/origin/njs/build/njs+0x495f7d)
    #1 0x53c2c9 in njs_function_frame_free
/home/p1umer/Documents/origin/njs/src/njs_function.c:797:13
    #2 0x4e9817 in njs_vmcode_return /home/p1umer/Documents/origin/njs/src/njs_vmcode.c:1810:5
    #3 0x4e9817 in njs_vmcode_await /home/p1umer/Documents/origin/njs/src/njs_vmcode.c:1905:12
    #4 0x4e9817 in njs_vmcode_interpreter
/home/p1umer/Documents/origin/njs/src/njs_vmcode.c:831:24
    #5 0x53b43a in njs_function_lambda_call
/home/p1umer/Documents/origin/njs/src/njs_function.c:703:11
    #6 0x60595d in njs_async_function_frame_invoke
/home/p1umer/Documents/origin/njs/src/njs_async.c:32:11
    #7 0x4e47fa in njs_vmcode_interpreter
/home/p1umer/Documents/origin/njs/src/njs_vmcode.c:785:23
    #8 0x605ecc in njs_await_fulfilled /home/p1umer/Documents/origin/njs/src/njs_async.c:96:11
    #9 0x53bf9c in njs_function_native_call
/home/p1umer/Documents/origin/njs/src/njs_function.c:739:11
    #10 0x53a5d9 in njs_function_frame_invoke
/home/p1umer/Documents/origin/njs/src/njs_function.c:777:16
    #11 0x53a5d9 in njs_function_call2 /home/p1umer/Documents/origin/njs/src/njs_function.c:600:11
    #12 0x5f53c7 in njs_function_call /home/p1umer/Documents/origin/njs/src/njs_function.h:180:12
    #13 0x5f53c7 in njs_promise_reaction_job
/home/p1umer/Documents/origin/njs/src/njs_promise.c:1171:15
```

```
    #14 0x53bf9c in njs_function_native_call
/home/p1umer/Documents/origin/njs/src/njs_function.c:739:11
    #15 0x4de620 in njs_vm_invoke /home/p1umer/Documents/origin/njs/src/njs_vm.c:375:12
    #16 0x4de620 in njs_vm_call /home/p1umer/Documents/origin/njs/src/njs_vm.c:359:12
    #17 0x4de620 in njs_vm_handle_events /home/p1umer/Documents/origin/njs/src/njs_vm.c:524:19
    #18 0x4de620 in njs_vm_run /home/p1umer/Documents/origin/njs/src/njs_vm.c:479:12
    #19 0x4c8407 in njs_process_script /home/p1umer/Documents/origin/njs/src/njs_shell.c:937:15
    #20 0x4c7484 in njs_process_file /home/p1umer/Documents/origin/njs/src/njs_shell.c:632:11
    #21 0x4c7484 in main /home/p1umer/Documents/origin/njs/src/njs_shell.c:316:15
    #22 0x7f03823f40b2 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/p1umer/Documents/origin/njs/build/njs+0x496c97)
    #1 0x62044c in njs_memalign /home/p1umer/Documents/origin/njs/src/njs_malloc.c:39:11
    #2 0x4cf7ab in njs_mp_alloc_large /home/p1umer/Documents/origin/njs/src/njs_mp.c:577:13
    #3 0x5395b1 in njs_function_frame_alloc
/home/p1umer/Documents/origin/njs/src/njs_function.c:564:17
    #4 0x5397a7 in njs_function_lambda_frame
/home/p1umer/Documents/origin/njs/src/njs_function.c:466:20
    #5 0x4eae3e in njs_function_frame /home/p1umer/Documents/origin/njs/src/njs_function.h:155:16
    #6 0x4eae3e in njs_function_frame_create
/home/p1umer/Documents/origin/njs/src/njs_vmcode.c:1740:16
    #7 0x4e32e8 in njs_vmcode_interpreter
/home/p1umer/Documents/origin/njs/src/njs_vmcode.c:736:23
    #8 0x605ecc in njs_await_fulfilled /home/p1umer/Documents/origin/njs/src/njs_async.c:96:11
    #9 0x53bf9c in njs_function_native_call
/home/p1umer/Documents/origin/njs/src/njs_function.c:739:11
    #10 0x53a5d9 in njs_function_frame_invoke
/home/p1umer/Documents/origin/njs/src/njs_function.c:777:16
    #11 0x53a5d9 in njs_function_call2 /home/p1umer/Documents/origin/njs/src/njs_function.c:600:11
    #12 0x5f53c7 in njs_function_call /home/p1umer/Documents/origin/njs/src/njs_function.h:180:12
    #13 0x5f53c7 in njs_promise_reaction_job
/home/p1umer/Documents/origin/njs/src/njs_promise.c:1171:15
    #14 0x53bf9c in njs_function_native_call
/home/p1umer/Documents/origin/njs/src/njs_function.c:739:11
    #15 0x4de620 in njs_vm_invoke /home/p1umer/Documents/origin/njs/src/njs_vm.c:375:12
    #16 0x4de620 in njs_vm_call /home/p1umer/Documents/origin/njs/src/njs_vm.c:359:12
    #17 0x4de620 in njs_vm_handle_events /home/p1umer/Documents/origin/njs/src/njs_vm.c:524:19
    #18 0x4de620 in njs_vm_run /home/p1umer/Documents/origin/njs/src/njs_vm.c:479:12
    #19 0x4c8407 in njs_process_script /home/p1umer/Documents/origin/njs/src/njs_shell.c:937:15
    #20 0x4c7484 in njs_process_file /home/p1umer/Documents/origin/njs/src/njs_shell.c:632:11
    #21 0x4c7484 in main /home/p1umer/Documents/origin/njs/src/njs_shell.c:316:15
    #22 0x7f03823f40b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16

SUMMARY: AddressSanitizer: heap-use-after-free
(/home/p1umer/Documents/origin/njs/build/njs+0x49595e) in __asan_memset
Shadow bytes around the buggy address:
  0x0c4a8000baf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a8000bb00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a8000bb10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a8000bb20: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a8000bb30: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c4a8000bb40: fd fd fd fd fd fd fd fd fd fd fd fd[fd]fd fd fd
  0x0c4a8000bb50: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a8000bb60: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a8000bb70: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a8000bb80: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a8000bb90: 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
==2064567==ABORTING
```

Credit

p1umer(**@P1umer**)

xeioex added bug fuzzer labels on Feb 15

xeioex commented on Feb 18 Contributor

The patch

```
# HG changeset patch
# User Dmitry Volyntsev <xeioex@nginx.com>
# Date 1645208528 0
#      Fri Feb 18 18:22:08 2022 +0000
# Node ID d3bd263c19c4e2bbf65ddae3764f3eae6f45648a
# Parent  b7a93f20410a99f186ca7c85f7c9187b8212474f
Fixed frame allocation from an awaited frame.

njs_function_frame_save() is used to save the awaited frame when "await"
instruction is encountered. The saving was done as a memcpy() of
existing runtime frame.
```

```
njs_function_frame_alloc() is used to alloc a new function frame, this
function tries to use a spare preallocated memory from the previous
frame first.  Previously, this function might result in "use-after-free"
when invoked from a restored frame saved with njs_function_frame_save().
Because njs_function_frame_save() left pointers to the spare memory of
the original frame which may be already free when saved frame is
restored.

The fix is to erase fields for the spare memory from the saved frame.

This closes #469 issue on Github.

diff --git a/src/njs_function.c b/src/njs_function.c
--- a/src/njs_function.c
+++ b/src/njs_function.c
@@ -811,9 +811,13 @@ njs_function_frame_save(njs_vm_t *vm, nj
     njs_native_frame_t  *active, *native;

     *frame = *vm->active_frame;
+
     frame->previous_active_frame = NULL;

     native = &frame->native;
+    native->size = 0;
+    native->free = NULL;
+    native->free_size = 0;

     active = &vm->active_frame->native;
     value_count = njs_function_frame_value_count(active);
diff --git a/test/js/async_recursive_large.t.js b/test/js/async_recursive_large.t.js
new file mode 100644
--- /dev/null
+++ b/test/js/async_recursive_large.t.js
@@ -0,0 +1,26 @@
+/*---
+includes: [compareArray.js]
+flags: [async]
+---*/
+
+let stages = [];
+
+async function f(v) {
+    if (v == 1000) {
+        return;
+    }
+
+    stages.push(`f>${v}`);
+
+    await "X";
+
+    await f(v + 1);
+
+    stages.push(`f<${v}`);
+}
+
+f(0)
```

```
+.then(v => {
+    assert.sameValue(stages.length, 2000);
+})
+.then($DONE, $DONE);
diff --git a/test/js/async_recursive_mid.t.js b/test/js/async_recursive_mid.t.js
--- a/test/js/async_recursive_mid.t.js
+++ b/test/js/async_recursive_mid.t.js
@@ -6,7 +6,7 @@ flags: [async]
 let stages = [];

 async function f(v) {
-    if (v == 3) {
+    if (v == 1000) {
         return;
     }
```

xeioex mentioned this issue on Feb 18

Worker process exited on signal 6 or 11 processing huge .js file #472

Closed

ViieeS commented on Feb 21

@xeioex May I know your plans for a new release including the patch?

nginx-hg-mirror closed this as completed in `ad48705` on Feb 21

xeioex commented on Feb 21 Contributor

Hi **@ViieeS**,

No specific plans yet. Approximately in two weeks.

👍 1

bmv126 mentioned this issue on Mar 22

Heap UAF in njs_await_fulfilled #451

Closed

Assignees

No one assigned

Labels

bug fuzzer

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants