

New issue

Jump to bottom

AddressSanitizer: stack-overflow at mjs.c:14225 #106

Open hongxuchen opened this issue on Jul 3, 2018 · 2 comments

hongxuchen commented on Jul 3, 2018

POCs:

https://github.com/ntu-sec/pocs/blob/master/mjs-8d847f2/crashes/so_mjs.c%3A14225_1.js
https://github.com/ntu-sec/pocs/blob/master/mjs-8d847f2/crashes/so_mjs.c%3A14225_2.js

ASAN output:

```
AddressSanitizer:DEADLYSIGNAL
=====
==31959==ERROR: AddressSanitizer: stack-overflow at address 0x7ffd3bc1af08 (pc 0x0000004d8a4c bp 0x7ffd3bc1b770 sp 0x7ffd3bc1af00 T0)
#0 0x4d8a4b in __asan_memcpy (/home/hongxu/FOT/mjs-asan/mjs.out+0x4d8a4b)
#1 0x544dc1 in mjs_mk_string /home/hongxu/FOT/mjs-asan/mjs.c:14225:9
#2 0x5436cb in mjs_get_own_property /home/hongxu/FOT/mjs-asan/mjs.c:12687:20
#3 0x545c5d in mjs_set_internal /home/hongxu/FOT/mjs-asan/mjs.c:12804:7
#4 0x534f61 in mjs_set /home/hongxu/FOT/mjs-asan/mjs.c:12772:10
#5 0x57bd68 in frozen_cb /home/hongxu/FOT/mjs-asan/mjs.c:12434:9
#6 0x54e48b in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6311:3
#7 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#8 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#9 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
...
#228 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#229 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#230 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#231 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#232 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#233 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#234 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#235 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#236 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#237 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#238 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#239 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#240 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#241 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#242 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#243 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#244 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#245 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#246 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#247 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7
#248 0x54e858 in parse_array /home/hongxu/FOT/mjs-asan/mjs.c:6323:9
#249 0x54c4e1 in parse_value /home/hongxu/FOT/mjs-asan/mjs.c:6363:7

SUMMARY: AddressSanitizer: stack-overflow (/home/hongxu/FOT/mjs-asan/mjs.out+0x4d8a4b) in __asan_memcpy
==31959==ABORTING
```

OS-WS commented on May 30, 2021

Hi,
This issue was assigned with [CVE-2020-36366](#) & [CVE-2020-18392](#).
Was it ever addressed?
Was it fixed?
If so, in what commit?

Thanks in advance!!

rojer commented on Jun 1, 2021

Collaborator

i don't believe so. PoCs are no longer available

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

