New issue

Jump to bottom

# Use of uninitialized value in the md_analyze_line() function #155

Closed bsdb0y opened this issue on Mar 27, 2021 · 2 comments

Labels bug

**bsdb0y** commented on Mar 27, 2021

Hi,

While fuzzing md4c 0.4.7 with AFL++ and MSAN, I found out that the md_analyze_line() function may use uninitialized memory.

Attaching a reproducer (gzipped so GitHub accepts it): input01.md.gz

Issue can be reproduced by running:

```
md2html input01.md


  ==2793660==WARNING: MemorySanitizer: use-of-uninitialized-value
      #0 0x7f021124c622 in md_analyze_line /home/bsdboy/md/md4c-release-0.4.7/src/md4c.c:5985:12
      #1 0x7f021122ee27 in md_process_doc /home/bsdboy/md/md4c-release-0.4.7/src/md4c.c:6254:9
      #2 0x7f021122dca5 in md_parse /home/bsdboy/md/md4c-release-0.4.7/src/md4c.c:6332:11
      #3 0x7f02112fd66b in md_html /home/bsdboy/md/md4c-release-0.4.7/src/md4c-html.c:571:12
      #4 0x4989fb in process_file /home/bsdboy/md/md4c-release-0.4.7/md2html/md2html.c:144:11
      #5 0x4989fb in main /home/bsdboy/md/md4c-release-0.4.7/md2html/md2html.c:368:11
      #6 0x7f0210e580b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
      #7 0x41c29d in _start (/home/bsdboy/md/md4c-release-0.4.7/build/md2html/md2html+0x41c29d)

  SUMMARY: MemorySanitizer: use-of-uninitialized-value /home/bsdboy/md/md4c-release-0.4.7/src/md4c.c:5985:12 in md_analyze_line
```

with memory origin tracking option `-fsanitize-memory-track-origins`

```
  ==2793563==WARNING: MemorySanitizer: use-of-uninitialized-value
      #0 0x7ffb9423f84f in md_analyze_line /home/bsdboy/md/md4c-release-0.4.7/src/md4c.c:5985:12
      #1 0x7ffb9421a49b in md_process_doc /home/bsdboy/md/md4c-release-0.4.7/src/md4c.c:6254:9
      #2 0x7ffb94218d8f in md_parse /home/bsdboy/md/md4c-release-0.4.7/src/md4c.c:6332:11
      #3 0x7ffb9430c7c4 in md_html /home/bsdboy/md/md4c-release-0.4.7/src/md4c-html.c:571:12
      #4 0x49972f in process_file /home/bsdboy/md/md4c-release-0.4.7/md2html/md2html.c:144:11
      #5 0x49972f in main /home/bsdboy/md/md4c-release-0.4.7/md2html/md2html.c:368:11
      #6 0x7ffb93e430b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
      #7 0x41c29d in _start (/home/bsdboy/md/md4c-release-0.4.7/build/md2html/md2html+0x41c29d)

    Uninitialized value was created by a heap allocation
      #0 0x42847d in malloc (/home/bsdboy/md/md4c-release-0.4.7/build/md2html/md2html+0x42847d)
      #1 0x49ab35 in membuf_init /home/bsdboy/md/md4c-release-0.4.7/md2html/md2html.c:69:17

  SUMMARY: MemorySanitizer: use-of-uninitialized-value /home/bsdboy/md/md4c-release-0.4.7/src/md4c.c:5985:12 in md_analyze_line
```

**mity** closed this as completed in `4fc808d` on Mar 29, 2021

**mity** commented on Mar 29, 2021 Owner

Thanks for reporting, should be now fixed.

**mity** added the bug label on Mar 29, 2021

**carnil** commented on Apr 29, 2021

The issue was apparently assigned CVE-2021-30027.

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants