

New issue

Jump to bottom

Use of uninitialized value in the md_push_block_bytes() function #130

Closed fcambus opened this issue on Sep 29, 2020 · 5 comments

Labels bug

fcambus commented on Sep 29, 2020

Hi,

While fuzzing md4c 0.4.5 with Honggfuzz, I found out that the md_push_block_bytes() function may use uninitialized memory.

Attaching a reproducer (gzipped so GitHub accepts it): [test01.md.gz](#)

Issue can be reproduced by running:

```
md2html test01.md

==257142==WARNING: MemorySanitizer: use-of-uninitialized-value
#0 0x7f6d02f3e5ed in md_push_block_bytes /home/fcambus/md4c-release-0.4.5/src/md4c.c:4848:12
#1 0x7f6d02f3e5ed in md_start_new_block /home/fcambus/md4c-release-0.4.5/src/md4c.c:4868:25
#2 0x7f6d02f3e5ed in md_process_line /home/fcambus/md4c-release-0.4.5/src/md4c.c:6147:9
#3 0x7f6d02f3e5ed in md_process_doc /home/fcambus/md4c-release-0.4.5/src/md4c.c:6218:9
#4 0x7f6d02f337e5 in md_parse /home/fcambus/md4c-release-0.4.5/src/md4c.c:6295:11
#5 0x7f6d02f6f5c2 in md_html /home/fcambus/md4c-release-0.4.5/src/md4c-html.c:571:12
#6 0x4964a9 in process_file /home/fcambus/md4c-release-0.4.5/md2html/md2html.c:144:11
#7 0x4964a9 in main /home/fcambus/md4c-release-0.4.5/md2html/md2html.c:368:11
#8 0x7f6d02bac0b2 in __libc_start_main /build/glibc-ZN95T4/glibc-2.31/csu/../csu/libc-start.c:308:16
#9 0x41c29d in _start (/home/fcambus/md4c-release-0.4.5/md2html/md2html+0x41c29d)


SUMMARY: MemorySanitizer: use-of-uninitialized-value /home/fcambus/md4c-release-0.4.5/src/md4c.c:4848:12 in md_push_block_bytes
```

mity commented on Sep 29, 2020

Owner

Ack. In debug build, it even leads to an assertion.

Thanks for reporting it.

 mity added the bug label on Sep 29, 2020

 mity closed this as completed in [22ca89a](#) on Sep 29, 2020

mity commented on Sep 29, 2020

Owner

I'm now sitting at a Windows machine and cannot really use memory sanitizer here, but the commit fixed the assertion in the debug build. I believe it is just another manifestation of the same bug.

Feel free to reopen if you still see the same trouble with it.

fcambus commented on Sep 29, 2020

Author

This issue has been assigned [CVE-2020-26148](#).

fcambus commented on Sep 29, 2020

Author

Looks good to me, I can confirm commit [22ca89a](#) fixes the issue. Thanks!

mity commented on Sep 29, 2020

Owner

For the sake of completeness, this bash command triggers it too in 0.4.5:

```
$ printf '\0x\n' | md2html
```

Assignees
No one assigned

Labels
bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

