

New issue

[Jump to bottom](#)

AddressSanitizer: heap-buffer-overflow on (write_header) /htmldoc/htmldoc/html.cxx:273 #425

✓ Closed

dramthy opened this issue on May 5, 2021 · 3 comments

Assignees



Labels

bug priority-high security

Milestone

📌 Stable

dramthy commented on May 5, 2021

No description provided.



dramthy closed this as completed on May 5, 2021



dramthy changed the title ~~htmlGetText~~ AddressSanitizer: AddressSanitizer: heap-buffer-overflow on (write_header) /htmldoc/htmldoc/html.cxx:273 on May 5, 2021

dramthy commented on May 5, 2021 • edited ▼

Author

Hello, While fuzzing htmldoc , I found a heap-buffer-overflow in write_header

Reporter:

dramthy from Topsec Alpha Lab

test platform:

htmldoc Version : current

OS :Ubuntu 20.04.1 LTS aarch64

kernel: 5.4.0-53-generic

compiler: cc (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0

reproduced:

(htmldoc with asan build option)

./htmldoc-with-asan ./poc.html

[poc.zip](#)

```
=====
==2609491==ERROR: AddressSanitizer: heap-buffer-overflow on address 0xfffff8cd0ca11 at pc
0xfffff92422fd0 bp 0xfffffef6e9d50 sp 0xfffffef6e9e00
READ of size 2 at 0xfffff8cd0ca11 thread T0
#0 0xfffff92422fcc (/lib/aarch64-linux-gnu/libasan.so.5+0x8efcc)
#1 0xfffff92423f8c in __interceptor_vfprintf (/lib/aarch64-linux-gnu/libasan.so.5+0x8ff8c)
#2 0xfffff924241a8 in __interceptor___fprintf_chk (/lib/aarch64-linux-gnu/libasan.so.5+0x901a8)
#3 0xaaaaae0238f30 in fprintf /usr/include/aarch64-linux-gnu/bits/stdio2.h:100
#4 0xaaaaae0238f30 in write_header /home/vm1/workspace/Projects/afl-
projects/001.htmldoc/htmldoc/htmldoc/html.cxx:273
#5 0xaaaaae023aa88 in html_export /home/vm1/workspace/Projects/afl-
projects/001.htmldoc/htmldoc/htmldoc/html.cxx:141
#6 0xaaaaae021f52c in main /home/vm1/workspace/Projects/afl-
projects/001.htmldoc/htmldoc/htmldoc/htmldoc.cxx:1291
#7 0xfffff91c4c08c in __libc_start_main (/lib/aarch64-linux-gnu/libc.so.6+0x2408c)
#8 0xaaaaae021f984 (/home/vm1/workspace/Projects/afl-projects/001.htmldoc/bin-with-
asan+0x4b984)

0xfffff8cd0ca11 is located 0 bytes to the right of 1-byte region [0xfffff8cd0ca10,0xfffff8cd0ca11)
allocated by thread T0 here:
#0 0xfffff92481a30 in __interceptor_malloc (/lib/aarch64-linux-gnu/libasan.so.5+0xeda30)
#1 0xaaaaae02892c4 in htmlGetText /home/vm1/workspace/Projects/afl-
projects/001.htmldoc/htmldoc/htmldoc/htmllib.cxx:2125
#2 0xaaaaae0238024 in get_title /home/vm1/workspace/Projects/afl-
projects/001.htmldoc/htmldoc/htmldoc/html.cxx:883
#3 0xaaaaae0238024 in get_title /home/vm1/workspace/Projects/afl-
projects/001.htmldoc/htmldoc/htmldoc/html.cxx:883
#4 0xaaaaae0238024 in get_title /home/vm1/workspace/Projects/afl-
projects/001.htmldoc/htmldoc/htmldoc/html.cxx:883
#5 0xaaaaae0238024 in get_title /home/vm1/workspace/Projects/afl-
projects/001.htmldoc/htmldoc/htmldoc/html.cxx:883
#6 0xaaaaae023a940 in html_export /home/vm1/workspace/Projects/afl-
projects/001.htmldoc/htmldoc/htmldoc/html.cxx:115
#7 0xaaaaae021f52c in main /home/vm1/workspace/Projects/afl-
projects/001.htmldoc/htmldoc/htmldoc/htmldoc.cxx:1291
#8 0xfffff91c4c08c in __libc_start_main (/lib/aarch64-linux-gnu/libc.so.6+0x2408c)
#9 0xaaaaae021f984 (/home/vm1/workspace/Projects/afl-projects/001.htmldoc/bin-with-
asan+0x4b984)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/lib/aarch64-linux-gnu/libasan.so.5+0x8efcc)
```

Maybe fix:

in htmlGetText(), the s2 is not init, if tlen ==0, malloc (1+0) and s2[tlen]='\0'.

```
if (tdata != NULL)
{
    // Add the text to this string...
```

```

tlen = strlen((char *)tdata);

if (s)
    s2 = (uchar *)realloc(s, 1 + slen + tlen);
else{
    s2 = (uchar *)malloc(1 + tlen); // error, s2 is not init
    s2[tlen] = '\0';
}



if (!s2)
    break;

s = s2;

memcpy((char *)s + slen, (char *)tdata, tlen);

```



 **dramthy** reopened this on May 5, 2021

  **dramthy** changed the title ~~AddressSanitizer: AddressSanitizer: heap-buffer-overflow on (write_header)~~ ~~/htmldoc/htmldoc/html.cxx:273~~ AddressSanitizer: heap-buffer-overflow on (write_header) ~~/htmldoc/htmldoc/html.cxx:273~~ on May 5, 2021

michaelsweet commented on May 7, 2021


Owner

Confirmed, investigating.

  **michaelsweet** self-assigned this on May 7, 2021

  **michaelsweet** added **bug** **priority-high** **security** labels on May 7, 2021

  **michaelsweet** added this to the **Stable** milestone on May 7, 2021

 **michaelsweet** added a commit that referenced this issue on May 7, 2021

 Fix a crash bug with empty titles (Issue [#425](#))

 [a0014be](#)

michaelsweet commented on May 7, 2021

Owner

[master [a0014be](#)] Fix a crash bug with empty titles (Issue [#425](#))



michaelrsweet closed this as completed on May 7, 2021

Assignees



michaelrsweet

Labels

bug **priority-high** **security**

Projects

None yet

Milestone

Stable

Development

No branches or pull requests

2 participants

