New issue

Jump to bottom

SEGV on unknown address 0x000000000000 #410

Closed chibataiki opened this issue on Jan 22, 2021 · 2 comments

Assignees

Labels bug priority-high

Milestone Stable

chibataiki commented on Jan 22, 2021 • edited

While fuzzing htmldoc I found a segmentation fault in the copy_image() function, in epub.cxx:1221

testcase:(zipped so GitHub accepts it)
crash01.html.zip

reproduced by running:

```
htmldoc -f demo.epub  crash01.html
```

htmldoc Version v1.9.11 git [master 0f9d20]
tested on:

OS :Ubuntu 20.04.1 LTS
kernel: 5.4.0-53-generic
compiler: clang version 10.0.0-4ubuntu1
Target: x86_64-pc-linux-gnu

OS : macOS Catalina 10.15.5(19F101) MacBook Pro (Retina, 13-inch, Early 2015)
compiler: Apple clang version 11.0.0 (clang-1100.0.33.17)

Install from snap or download mac dmg don't crash for this testcase.

- addresssanitizer

```
==3252595==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000042fc30 bp 0x7ffe6ab48d00 sp 0x7ffe6ab484a0 T0)
==3252595==The signal is caused by a READ memory access.
==3252595==Hint: address points to the zero page.
    #0 0x42fc30 in strcmp (/home/chiba/check_crash/htmldoc/htmldoc/htmldoc+0x42fc30)
    #1 0x7f70ce1fd7c7 in bsearch /build/glibc-ZN95T4/glibc-2.31/stdlib/../bits/stdlib-bsearch.h:33:23
    #2 0x4c81b0 in copy_image(_zipc_s*, char const*) /home/chiba/check_crash/htmldoc/htmldoc/epub.cxx:1221:25
    #3 0x4c8434 in copy_images(_zipc_s*, tree_str*) /home/chiba/check_crash/htmldoc/htmldoc/epub.cxx:1288:11
    #4 0x4c71c5 in epub_export /home/chiba/check_crash/htmldoc/htmldoc/epub.cxx:211:13
    #5 0x4d0f13 in main /home/chiba/check_crash/htmldoc/htmldoc/htmldoc.cxx:1291:3
    #6 0x7f70ce1dd0b2 in __libc_start_main /build/glibc-ZN95T4/glibc-2.31/csu/../csu/libc-start.c:308:16
    #7 0x41c5fd in _start (/home/chiba/check_crash/htmldoc/htmldoc/htmldoc+0x41c5fd)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/chiba/check_crash/htmldoc/htmldoc/htmldoc+0x42fc30) in strcmp
==3252595==ABORTING
```

- gdb

```
─[ DISASM ]─
 ► 0x7ffff7de1ed7 <__strcmp_avx2+887>    vmovdqu ymm1, ymmword ptr [rdi + rdx]
   0x7ffff7de1edc <__strcmp_avx2+892>    vpcmpeqb ymm0, ymm1, ymmword ptr [rsi + rdx]
   0x7ffff7de1ee1 <__strcmp_avx2+897>    vpminub ymm0, ymm0, ymm1
   0x7ffff7de1ee5 <__strcmp_avx2+901>    vpcmpeqb ymm0, ymm0, ymm7
   0x7ffff7de1ee9 <__strcmp_avx2+905>    vpmovmskb ecx, ymm0
   0x7ffff7de1eed <__strcmp_avx2+909>    test   ecx, ecx
   0x7ffff7de1eef <__strcmp_avx2+911>    jne    __strcmp_avx2+848 <__strcmp_avx2+848>
    ↓
   0x7ffff7de1eb0 <__strcmp_avx2+848>    add    rdi, rdx
   0x7ffff7de1eb3 <__strcmp_avx2+851>    add    rsi, rdx
   0x7ffff7de1eb6 <__strcmp_avx2+854>    tzcnt  edx, ecx
   0x7ffff7de1eba <__strcmp_avx2+858>    movzx  eax, byte ptr [rdi + rdx]
─[ STACK ]──
00:0000│ rsp  0x7fffffffd948 —▸ 0x7ffff7ca27c8 (bsearch+88) ◂— test   eax, eax
01:0008│      0x7fffffffd950 —▸ 0x555555aa6bc0 —▸ 0x555555aa6fd0 —▸ 0x7ffff7e47000 (main_arena+1152) —▸ 0x7ffff7e46ff0 (main_arena+1136) ◂— ...
02:0010│      0x7fffffffd958 ◂— 0x8
03:0018│      0x7fffffffd960 ◂— 0x0
04:0020│      0x7fffffffd968 —▸ 0x555555aa8bf0 —▸ 0x555555aa8af0 —▸ 0x555555aa7f40 —▸ 0x555555aa65c0 ◂— ...
05:0028│      0x7fffffffd970 —▸ 0x555555aa9200 —▸ 0x555555aa6340 ◂— 0x5555fbad2480
06:0030│      0x7fffffffd978 —▸ 0x555555aa8fe0 ◂— 0x616d693a61746164 ('data:ima')
07:0038│      0x7fffffffd980 —▸ 0x5555555cd04b ◂— 0x22263e3c00435253 /* 'SRC' */

pwndbg> bt
#0  __strcmp_avx2 () at ../sysdeps/x86_64/multiarch/strcmp-avx2.S:736
#1  0x00007ffff7ca27c8 in __GI_bsearch (__key=0x7fffffffd9a0, __base=0x555555aa6bc0, __nmemb=<optimized out>, __size=8, __compar=0x55555555d609 <compare_images(char**, char**)>) at
../bits/stdlib-bsearch.h:33
#2  0x0000555555555d6ed in copy_image (zipc=zipc@entry=0x555555aa9200, filename=filename@entry=0x555555aa8fe0
",B1BMVEUAAAD///+l2Z/dAAAAM0lEQVR4nGP4/5/h/1+G/58ZDrAz3D/McH8yw83NDDeNGe4Ug9CLzwz3gVLMDA/A6P9/#FGGF\207jOXZtQAAAAA
at epub.cxx:1235
#3  0x000055555555d81c in copy_images (zipc=zipc@entry=0x555555aa9200, t=0x555555aa8bf0, t@entry=0x555555aa65c0) at epub.cxx:1288
#4  0x000055555555e813 in epub_export (document=0x555555aa65c0, toc=0x555555aa6760) at epub.cxx:211
#5  0x0000555555555d448 in main (argc=<optimized out>, argc@entry=4, argv=argv@entry=0x7fffffffe4e8) at htmldoc.cxx:1291
#6  0x00007ffff7c820b3 in __libc_start_main (main=0x55555555af20 <main(int, char**)>, argc=4, argv=0x7fffffffe4e8, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized
out>, stack_end=0x7fffffffe4d8) at ../csu/libc-start.c:308
#7  0x0000555555555d54e in _start () at htmldoc.cxx:1315
```

The bug locate in epub.cxx:1221 compare_images. The arguments of compare_images didn't checked so strcmp() lead a segfault due to to null pointer.

Reporter: chiba of topsec alphalab

michaelrsweet added a commit that referenced this issue on Jan 23, 2021

`Fix crash bug with data: URIs (Issue #410)` ··· ✕ `008861d`

michaelrsweet commented on Jan 23, 2021 Owner

[master `008861d`] Fix crash bug with data: URIs (Issue #410)

michaelrsweet closed this as completed on Jan 23, 2021

---

michaelrsweet self-assigned this on Jan 23, 2021

michaelrsweet added bug priority-high labels on Jan 23, 2021

michaelrsweet added this to the Stable milestone on Jan 23, 2021

michaelrsweet mentioned this issue on Jan 23, 2021

break url to pdf/ps #409

Closed

chibataiki commented on Feb 21 Author

CVE-2021-26948 assigned

Assignees

michaelrsweet

Labels

bug priority-high

Projects

None yet

Milestone

Stable

Development

No branches or pull requests

2 participants