

New issue

[Jump to bottom](#)

AddressSanitizer: double-free in function pspdf_export ps-pdf.cxx:945:7 #414

Closed chibataiki opened this issue on Jan 26, 2021 · 3 comments

Assignees
Labels **bug** priority-high
Milestone **Stable**

chibataiki commented on Jan 26, 2021 • edited

Hello, While fuzzing htmldoc, I found a double-free in pspdf_export

test platform
htmldoc Version 1.9.12 git [master 6898d0a]
OS:Ubuntu 20.04.1 LTS x86_64
kernel: 5.4.0-53-generic
compiler: clang version 10.0.0-4ubuntu1

reproduced:

htmldoc -f demo.pdf poc3.html
poc(zipped for update):
[poc3.zip](#)

```
==38152==ERROR: AddressSanitizer: attempting double-free on 0x603000000280 in thread T0:
#0 0x4ee210 in free /home/goushi/work/libfuzzer-workshop/src/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:124
#1 0x550309 in pspdf_export /home/htmldoc_sani/htmldoc/ps-pdf.cxx:945:7
#2 0x53c845 in main /home/htmldoc_sani/htmldoc/htmldoc.cxx:1291:3
#3 0x7ff6f7d10b2 in __libc_start_main /build/glibc-eXltMB/glibc-2.31/csu/../csu/libc-start.c:308:16
#4 0x41f8bd in _start (/home/htmldoc_sani/htmldoc/htmldoc+0x41f8bd)




0x603000000280 is located 0 bytes inside of 18-byte region [0x603000000280,0x603000000292)
freed by thread T0 here:
#0 0x4ee210 in free /home/goushi/work/libfuzzer-workshop/src/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:124
#1 0x550309 in pspdf_export /home/htmldoc_sani/htmldoc/ps-pdf.cxx:945:7
#2 0x53c845 in main /home/htmldoc_sani/htmldoc/htmldoc.cxx:1291:3
#3 0x7ff6f7d10b2 in __libc_start_main /build/glibc-eXltMB/glibc-2.31/csu/../csu/libc-start.c:308:16

previously allocated by thread T0 here:
#0 0x4ee5df in __interceptor_malloc /home/goushi/work/libfuzzer-workshop/src/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:146
#1 0x5ab666 in htmlGetText /home/htmldoc_sani/htmldoc/htmllib.cxx:2125:23

SUMMARY: AddressSanitizer: double-free /home/goushi/work/libfuzzer-workshop/src/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:124 in free
==38152==ABORTING

gef> bt
#0 __GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:50
#1 0x0000ffff79ba859 in __GI_abort () at abort.c:79
#2 0x0000ffff7a253ee in __libc_message (action=action@entry=do_abort, fmt=fmt@entry=0x7ffff7b4f285 "%s\n") at ../sysdeps/posix/libc_fatal.c:155
#3 0x0000ffff7a2d47c in malloc_printerr (str=str@entry=0x7ffff7b51278 "malloc_consolidate(): invalid chunk size") at malloc.c:5347
#4 0x0000ffff7a2dc58 in malloc_consolidate (av=av@entry=0x7ffff7b80b80 <main_arena>) at malloc.c:4477
#5 0x0000ffff7a2f160 in _int_free (av=0x7ffff7b80b80 <main_arena>, p=0x9249a0, have_lock=<optimized out>) at malloc.c:4400
#6 0x0000000004138a4 in pspdf_export (document=<optimized out>, toc=<optimized out>) at ps-pdf.cxx:994
#7 0x000000000408e89 in main (argc=<optimized out>, argv=<optimized out>) at htmldoc.cxx:1291
```

reporter: chiba of topsec alphalab


-  **michaelsweet** self-assigned this on Jan 26, 2021
-  **michaelsweet** added **bug** priority-high labels on Jan 26, 2021
-  **michaelsweet** added this to the **Stable** milestone on Jan 26, 2021

michaelsweet commented on Jan 26, 2021 Owner

Confirmed, investigating...

michaelsweet commented on Apr 1, 2021 Owner

This seems to have been fixed with the changes for #415.

 **michaelsweet** closed this as completed on Apr 1, 2021

 **michaelsweet** mentioned this issue on Apr 1, 2021

 Closed

chibataiki commented on Feb 21

Author

[CVE-2021-23158](#) assigned

Assignees

 michaelrsweet

Labels

bug priority-high

Projects

None yet

Milestone

Stable

Development

No branches or pull requests

2 participants

