New issue Jump to bottom

AddressSanitizer: heap-buffer-overflow on render_table_row() ps-pdf.cxx:6123:34 #417

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

Assignees

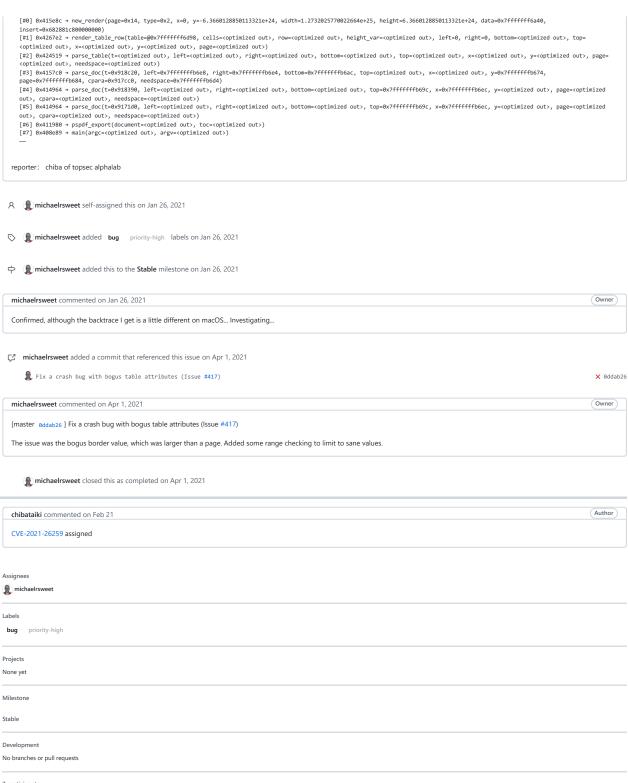
Labels

bug priority-high

Milestone

\$\frac{1}{2}\$ Stable

```
chibataiki commented on Jan 26, 2021 • edited 🕶
Hello, While fuzzing htmldoc, I found a heap-buffer-overflow in the render_table_row() ps-pdf.cxx:6123:34
       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
htmldoc -f demo.pdf poc7.html
poc(zipped for update):
poc7.zip
   ==38248==\text{ERROR: AddressSanitizer: heap-buffer-overflow on address } 0x625000002100 \text{ at pc } 0x00000059260e \text{ bp } 0x7fffa3362670 \text{ sp } 0x7fffa3362668 \text{ READ of size } 8 \text{ at } 0x625000002100 \text{ thread } T0
          We 0x59260d in render_table_row(hotable_t8, tree_str***, int, unsigned char*, float, float, float, float, float, float*, float*, int*) /home//htmldoc_sani/htmldoc/ps-pdf.cxx:6123:34
#1 0x588630 in parse_table(tree_str*, float, float, float, float, float*, float*, int*, int) /home//htmldoc_sani/htmldoc/ps-pdf.cxx:7081:5
#2 0x558013 in parse_doc(tree_str*, float*, float*, float*, float*, float*, float*, int*, tree_str*, int*) /home//htmldoc_sani/htmldoc/ps-pdf.cxx:4081:9
#3 0x556564 in parse_doc(tree_str*, float*, 
          #5 0x54f90e in pspdf_export /home//htmldoc_sani/htmldoc/ps-pdf.cxx:803:3 #6 0x53c845 in main /home//htmldoc_sani/htmldoc.cxx:1291:3
           #7 0x7f52a6b3e0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
          #8 0x41f8bd in start (/home//htmldoc sani/htmldoc/htmldoc+0x41f8bd)
    0x625000002100 is located 32 bytes to the right of 8160-byte region [0x625000000100,0x6250000020e0)
   allocated by thread T0 here:
#0 0x4eea4e in realloc /home/goushi/work/libfuzzer-workshop/src/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:165
           #1 0x55d96b in check_pages(int) /home//htmldoc_sani/htmldoc/ps-pdf.cxx:8804:24
    SUMMARY: AddressSanitizer: heap-buffer-overflow /home//htmldoc_sani/htmldoc/ps-pdf.cxx:6123:34 in render_table_row(hdtable_t&, tree_str***, int, unsigned char*, float, float,
    float, float, float*, float*, int*)
Shadow bytes around the buggy address:
       Shadow byte legend (one shadow byte represents 8 application bytes): Addressable: 00
       Partially addressable: 01 02 03 04 05 06 07
        Heap left redzone:
       Freed heap region:
        Stack left redzone:
        Stack mid redzone:
       Stack right redzone:
       Stack after return:
        Stack use after scope:
       Global redzone:
       Global init order:
        Poisoned by user:
       Container overflow:
       Intra object redzone:
       ASan internal:
       Left alloca redzone:
       Right alloca redzone:
    Shadow gap:
==38248==ABORTING
              source:ps-pdf.cxx+8754 ----
         8749
                               break;
         8750
         8751
         8752
                     if (insert)
         8753
      → 8754
8755
                        if (insert->prev)
                             insert->prev->next = r;
         8756
                            pages[page].start = r;
         8758
                                             = insert->prev;
         threads ·
    [#0] Id 1, Name: "htmldoc", stopped 0x415e8c in new_render (), reason: SIGSEGV
         trace
```



2 participants

