New issue

Jump to bottom

AddressSanitizer: SEGV in file_extension file.c:337:29 #418

Closed **chibataiki** opened this issue on Jan 26, 2021 · 2 comments

Assignees

Labels bug priority-high

Milestone Stable

chibataiki commented on Jan 26, 2021 • edited

Hello, While fuzzing htmldoc , I found aSEGV in file_extension function in file.c:337:29

- 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 poc8.html
poc(zipped for update):
poc8.zip

```
=================================================================
==38294==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000059da5a bp 0x7fff321dba90 sp 0x7fff321d9150 T0)
==38294==The signal is caused by a WRITE memory access.
==38294==Hint: address points to the zero page.
    #0 0x59da59 in file_extension /home//htmldoc_sani/htmldoc/file.c:337:29
    #1 0x5521fc in pdf_write_links(_IO_FILE*) /home//htmldoc_sani/htmldoc/ps-pdf.cxx:3424:26
    #2 0x5521fc in pdf_write_document(unsigned char*, unsigned char*, unsigned char*, unsigned char*, unsigned char*, unsigned char*, tree_str*, tree_str*)
/home//htmldoc_sani/htmldoc/ps-pdf.cxx:2295
    #3 0x5521fc in pspdf_export /home//htmldoc_sani/htmldoc/ps-pdf.cxx:910
    #4 0x53c845 in main /home//htmldoc_sani/htmldoc/htmldoc.cxx:1291:3
    #5 0x7f91f2fee0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
    #6 0x41f8bd in _start (/home//htmldoc_sani/htmldoc/htmldoc+0x41f8bd)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home//htmldoc_sani/htmldoc/file.c:337:29 in file_extension
==38294==ABORTING
```

```
 — source:file.c+337 ———
    332    if (strchr(extension, '#') == NULL)
    333      return (extension);
    334
    335    strlcpy(buf, extension, sizeof(buf));
    336
           // buf=0x00000000004602f0  →  "<P>Click on this image: <A HRnnnnnnnnnnnnnnnnnnn"
 →  337    *(char *)strchr(buf, '#') = '\0';
    338
    339    return (buf);
    340  }
    341
    342
 —— threads ———
[#0] Id 1, Name: "htmldoc", stopped 0x42a338 in file_extension (), reason: SIGSEGV
 ——— trace ———
[#0] 0x42a338 → file_extension(s=<optimized out>)
[#1] 0x412309 → pdf_write_links(out=<optimized out>)
[#2] 0x412309 → pdf_write_document(author=<optimized out>, creator=<optimized out>, copyright=<optimized out>, keywords=<optimized out>, subject=<optimized out>, lang=<optimized
out>, doc=<optimized out>, toc=<optimized out>)
[#3] 0x412309 → pspdf_export(document=<optimized out>, toc=<optimized out>)
[#4] 0x408e89 → main(argc=<optimized out>, argv=<optimized out>)
```

reporter: chiba of topsec alphalab

michaelrsweet added a commit that referenced this issue on Jan 26, 2021

`Fix a crash bug with malformed URIs (Issue #418)` 19c582f

michaelrsweet commented on Jan 26, 2021 Owner

[master 19c582f] Fix a crash bug with malformed URIs (Issue #418)

michaelrsweet closed this as completed on Jan 26, 2021

michaelrsweet self-assigned this on Jan 26, 2021

michaelrsweet added bug priority-high labels on Jan 26, 2021

michaelrsweet added this to the **Stable** milestone on Jan 26, 2021

chibataiki commented on Feb 21 — Author

CVE-2021-23180 assigned

Assignees

michaelrsweet

Labels

bug priority-high

Projects

None yet

Milestone

Stable

Development

No branches or pull requests

2 participants