michaelrsweet / htmldoc Public

Code Issues 20 Pull requests 1 Discussions Actions Projects ...

New issue Jump to bottom

Stack Buffer Overflow in gif_read_lzw #470

Closed Voiddy-Dev opened this issue on Jan 25 · 1 comment

Assignees

Labels bug priority-medium

Milestone Stable

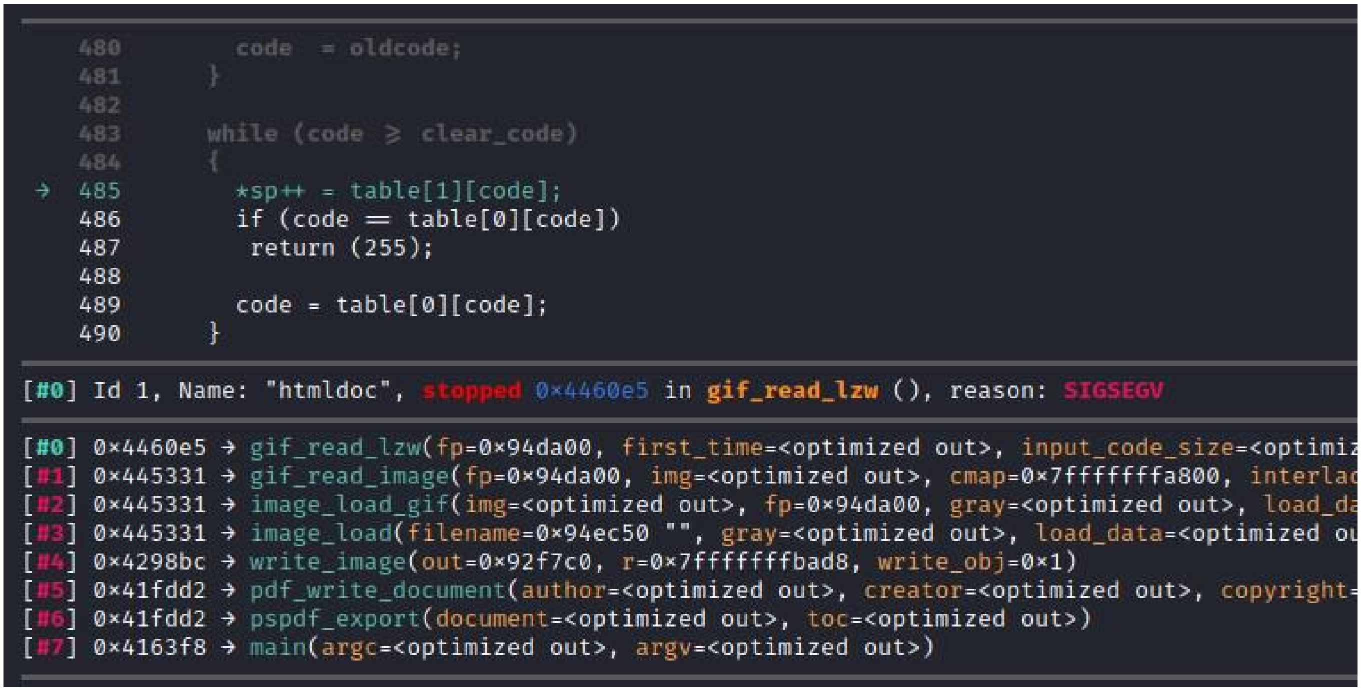
Voiddy-Dev commented on Jan 25

Due to an infinite loop in the `gif_read_lzw` function, the `sp` variable which belongs heap memory can be arbitrarily modified.

The crash happens in this loop:

```
      while (code >= clear_code)
      {
        *sp++ = table[1][code];
        if (code == table[0][code])
          return (255);

        code = table[0][code];
      }
```



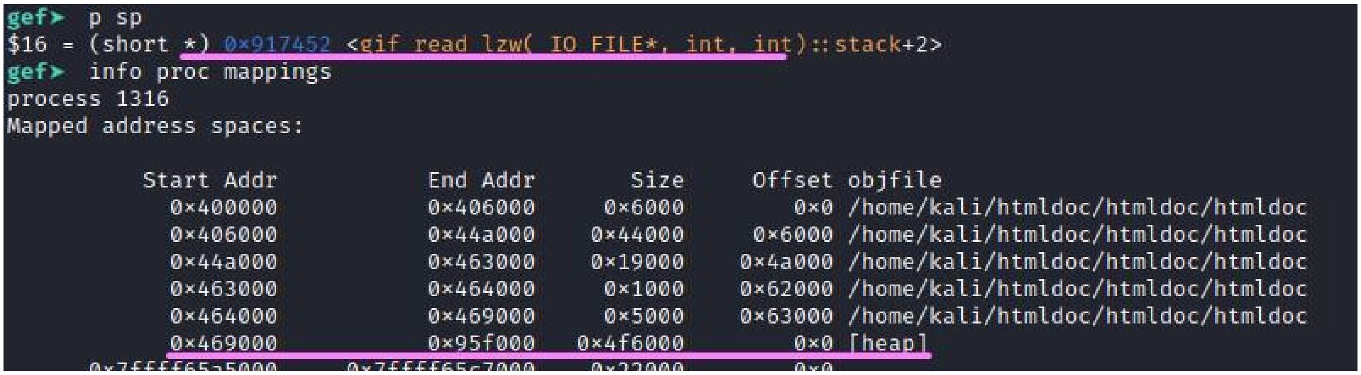
```
          code  = oldcode;
        }

        while (code >= clear_code)
        {
→         *sp++ = table[1][code];
          if (code == table[0][code])
           return (255);

          code = table[0][code];
        }
[#0] Id 1, Name: "htmldoc", stopped 0x4460e5 in gif_read_lzw (), reason: SIGSEGV
[#0] 0x4460e5 → gif_read_lzw(fp=0x94da00, first_time=<optimized out>, input_code_size=<optimiz
[#1] 0x445331 → gif_read_image(fp=0x94da00, img=<optimized out>, cmap=0x7fffffffa800, interlac
[#2] 0x445331 → image_load_gif(img=<optimized out>, fp=0x94da00, gray=<optimized out>, load_da
[#3] 0x445331 → image_load(filename=0x94ec50 "", gray=<optimized out>, load_data=<optimized ou
[#4] 0x4298bc → write_image(out=0x92f7c0, r=0x7fffffffbad8, write_obj=0x1)
[#5] 0x41fdd2 → pdf_write_document(author=<optimized out>, creator=<optimized out>, copyright=
[#6] 0x41fdd2 → pspdf_export(document=<optimized out>, toc=<optimized out>)
[#7] 0x4163f8 → main(argc=<optimized out>, argv=<optimized out>)
```

As `sp` is consistently incremented, it reaches out of heap memory which causes the crash:

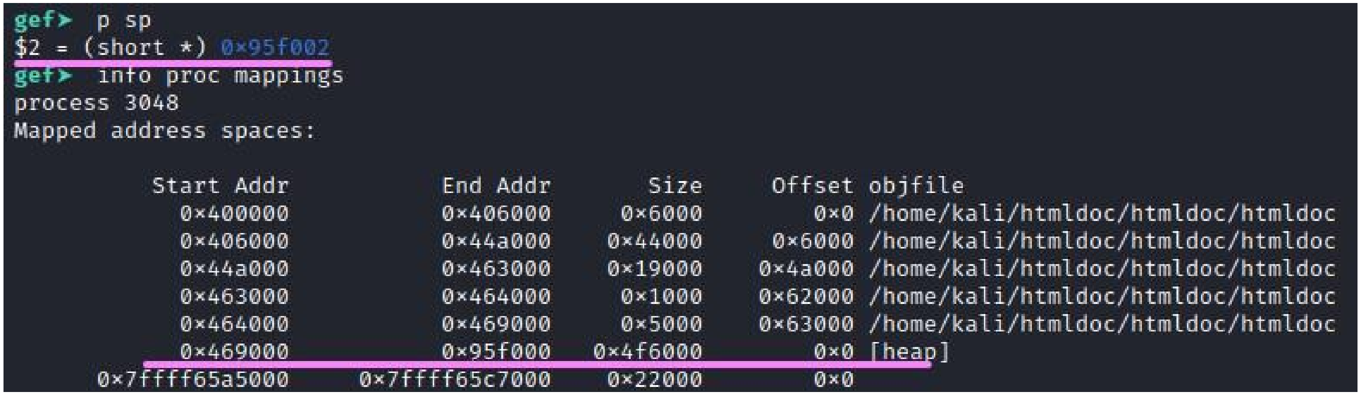
`sp` towards the start of execution:



```
gef➤  p sp
$16 = (short *) 0x917452 <gif_read_lzw(_IO_FILE*, int, int)::stack+2>
gef➤  info proc mappings
process 1316
Mapped address spaces:

          Start Addr           End Addr       Size     Offset objfile
            0x400000           0x406000     0x6000        0x0 /home/kali/htmldoc/htmldoc/htmldoc
            0x406000           0x44a000    0x44000     0x6000 /home/kali/htmldoc/htmldoc/htmldoc
            0x44a000           0x463000    0x19000    0x4a000 /home/kali/htmldoc/htmldoc/htmldoc
            0x463000           0x464000     0x1000    0x62000 /home/kali/htmldoc/htmldoc/htmldoc
            0x464000           0x469000     0x5000    0x63000 /home/kali/htmldoc/htmldoc/htmldoc
            0x469000           0x95f000   0x4f6000        0x0 [heap]
      0x7ffff65a5000     0x7ffff65c7000    0x22000        0x0
```

`sp` once the crash happened:



```
gef➤  p sp
$2 = (short *) 0x95f002
gef➤  info proc mappings
process 3048
Mapped address spaces:

          Start Addr           End Addr       Size     Offset objfile
            0x400000           0x406000     0x6000        0x0 /home/kali/htmldoc/htmldoc/htmldoc
            0x406000           0x44a000    0x44000     0x6000 /home/kali/htmldoc/htmldoc/htmldoc
            0x44a000           0x463000    0x19000    0x4a000 /home/kali/htmldoc/htmldoc/htmldoc
            0x463000           0x464000     0x1000    0x62000 /home/kali/htmldoc/htmldoc/htmldoc
            0x464000           0x469000     0x5000    0x63000 /home/kali/htmldoc/htmldoc/htmldoc
            0x469000           0x95f000   0x4f6000        0x0 [heap]
      0x7ffff65a5000     0x7ffff65c7000    0x22000        0x0
```

You can download and attempt the following POC:

```
htmldoc --webpage -f out.pdf ./crash.html
```

poc.zip

michaelrsweet added a commit that referenced this issue on Jan 25

`Fix a potential stack overflow bug with GIF images (Issue #470)` ✗ fb0334a

michaelrsweet commented on Jan 25 Owner

[master `fb0334a`] Fix a potential stack overflow bug with GIF images (Issue #470)

michaelrsweet closed this as completed on Jan 25

---

michaelrsweet self-assigned this on Jan 25

michaelrsweet added **bug** **priority-medium** labels on Jan 25

michaelrsweet added this to the **Stable** milestone on Jan 25

Voiddy-Dev changed the title ~~Heap Overflow in gif_read_lzw~~ Stack Buffer Overflow in gif_read_lzw on Jan 26

Assignees

michaelrsweet

Labels

bug **priority-medium**

Projects

None yet

Milestone

Stable

Development

No branches or pull requests

2 participants