New issue

Jump to bottom

The lack of a complete magic check leads to heap-buffer-overflow in pdf_get_version() #14

Closed yifengchen-cc opened this issue on Jul 23, 2020 · 2 comments

yifengchen-cc commented on Jul 23, 2020 • edited

commit 3dfc102

os version: ubuntu 16.04

```
//pdf.c:205:34
void[ pdf_get_version](url)(FILE *fp, pdf_t *pdf)
{
    char *header, *c;

    header = get_header(fp);

    /* Locate version string start and make sure we dont go past header */
    if ((c = strstr(header, "%PDF-")) &&
        (c + strlen("%PDF-M.m") + 2))
    {
        pdf->pdf_major_version = atoi(c + strlen("%PDF-"));
    --> pdf->pdf_minor_version = atoi(c + strlen("%PDF-M."));
    }

    free(header);
}
```

```
root@ubuntu:/home/fuzz/pdfresurrect# ./pdfresurrect poc
=================================================================
==12207==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000000981 at pc 0x0000004b27bc bp 0x7ffec7acc460 sp 0x7ffec7acbc00
READ of size 1 at 0x619000000981 thread T0
    #0 0x4b27bb in __interceptor_atoi (/home/fuzz/pdfresurrect/pdfresurrect+0x4b27bb)
    #1 0x4f9bf2 in pdf_get_version /home/fuzz/pdfresurrect/pdf.c:205:34
    #2 0x4f8aac in init_pdf /home/fuzz/pdfresurrect/main.c:205:5
    #3 0x4f84e3 in main /home/fuzz/pdfresurrect/main.c:279:17
    #4 0x7f7e5efd783f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #5 0x41ae18 in _start (/home/fuzz/pdfresurrect/pdfresurrect+0x41ae18)

0x619000000981 is located 1 bytes to the right of 1024-byte region [0x619000000580,0x619000000980)
allocated by thread T0 here:
    #0 0x4c6fca in calloc (/home/fuzz/pdfresurrect/pdfresurrect+0x4c6fca)
    #1 0x4f8254 in safe_calloc /home/fuzz/pdfresurrect/main.c:223:16
    #2 0x4f9ad0 in get_header /home/fuzz/pdfresurrect/pdf.c:1230:20
    #3 0x4f9ba1 in pdf_get_version /home/fuzz/pdfresurrect/pdf.c:198:14
    #4 0x4f8aac in init_pdf /home/fuzz/pdfresurrect/main.c:205:5
    #5 0x4f84e3 in main /home/fuzz/pdfresurrect/main.c:279:17
    #6 0x7f7e5efd783f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/fuzz/pdfresurrect/pdfresurrect+0x4b27bb) in __interceptor_atoi
Shadow bytes around the buggy address:
  0x0c327fff80e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff80f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff8130:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8160: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8170: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==12207==ABORTING
```

build arg:

```
export CC="clang-8"
export CXX="clang++-8"
export CFLAGS="-O1 -fno-omit-frame-pointer -gline-tables-only -DFUZZING_BUILD_MODE_UNSAFE_FOR_PRODUCTION -fsanitize=address -fsanitize-address-use-after-scope -fsanitize-coverage=trac
export CXXFLAGS="-O1 -fno-omit-frame-pointer -gline-tables-only -DFUZZING_BUILD_MODE_UNSAFE_FOR_PRODUCTION -fsanitize=address -fsanitize-address-use-after-scope -fsanitize-coverage=tr
./configure
LDFLAGS="$CXXFLAGS" make -j$(nproc)
```

poc1.gz

Credit: 1vanChen of NSFOCUS Security Team

enferex commented on Jul 24, 2020 — Owner

I can repro this on master, I've updated the header checks and gave you a shout-out in the AUTHORS file. Thanks!

👍 2

 **enferex** closed this as completed on Jul 24, 2020

yifengchen-cc commented on Apr 9, 2021 Author

This issue has been assigned CVE-2020-20740.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants