New issue

Jump to bottom

[Security] heap-buffer-overflow of exif.c in function Get16u #33

Closed NigelX opened this issue on Apr 12, 2021 · 2 comments

NigelX commented on Apr 12, 2021 • edited

Hi jhead Team
I found an overflow error.

System info:
Ubuntu 20.04 : clang 10.0.0 , gcc 9.3.0
Fedora 33: clang 11.0.0 , gcc 10.2.1

jhead version 3.06 commit `871e319`

file: jhead_poc.zip

Verification steps:
1.Get the source code of jhead

Edit file makefile

```
OBJ=obj
SRC=.
CFLAGS:=$(shell dpkg-buildflags --get CFLAGS) -fsanitize=address
LDFLAGS:=$(shell dpkg-buildflags --get LDFLAGS) -fsanitize=address
...
```

2.Compile the jhead

```
$ make
```

3.run jhead

```
$ ./jhead poc.jpg
```

asan info

```
Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Illegal value pointer for tag 0110 in Exif

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Illegal number format 232 for tag 0300 in Exif

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 11000004

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Illegal value pointer for tag 9004 in Exif

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 3639b234

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Illegal number format 25724 for tag dc6e in Exif

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Illegal number format 255 for tag 9bb0 in Exif

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 30002

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 30003

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 39404

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 30000

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 20006

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 20007

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 40008

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 20009

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 40010

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Illegal Exif number format 1540 for maker tag 0000

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 14000001

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 20001

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 9e00d3

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Illegal Exif number format 160 for maker tag 0062

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count ab0000

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Illegal Exif number format 37779 for maker tag 9393

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 66204745

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 69460000

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 7f02061

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 51f87089
Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Illegal Exif number format 47318 for maker tag 937a

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count ce0009

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 40000

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 383952

Nonfatal Error : 'crashes/id:000000,sig:06,src:001187,time:15492164,op:havoc,rep:8' Bad components count 30303130
=================================================================
==4037677==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61a000000515 at pc 0x0000004ce2aa bp 0x7fffe9e82350 sp 0x7fffe9e82348
READ of size 1 at 0x61a000000515 thread T0
    #0 0x4ce2a9 in Get16u exif.c
    #1 0x4d78c0 in ProcessCanonMakerNoteDir makernote.c:128:27
    #2 0x4d78c0 in ProcessMakerNote makernote.c:189:9
    #3 0x4d0d4a in ProcessExifDir exif.c:578:13
    #4 0x4d1a46 in ProcessExifDir exif.c:870:25
    #5 0x4cfde3 in process_EXIF exif.c:1060:5
    #6 0x4ca981 in ReadJpegSections jpgfile.c:289:25
    #7 0x4cb257 in ReadJpegFile jpgfile.c:381:11
    #8 0x4c6274 in ProcessFile jhead.c:914:10
    #9 0x4c6274 in main jhead.c:1770:13
    #10 0x7fb64aa370b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
    #11 0x41c45d in _start (/home/hh/Downloads/jhead/jhead+0x41c45d)

0x61a000000515 is located 9 bytes to the right of 1164-byte region [0x61a000000080,0x61a00000050c)
allocated by thread T0 here:
    #0 0x494b9d in malloc (/home/hh/Downloads/jhead/jhead+0x494b9d)
    #1 0x4ca120 in ReadJpegSections jpgfile.c:175:25
    #2 0x4cb257 in ReadJpegFile jpgfile.c:381:11

SUMMARY: AddressSanitizer: heap-buffer-overflow exif.c in Get16u
Shadow bytes around the buggy address:
  0x0c347fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fff8090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c347fff80a0: 00 04[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fff80f0: 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
==4037677==ABORTING
```

Tanks

HX from **Topsec alpha Security Team**

carnil commented on Apr 14, 2021

This issue appears to have been assigned CVE-2021-3496.

Matthias-Wandel commented on Apr 14, 2021

Owner

Fixed by `ca2973f`

Matthias-Wandel closed this as completed on Apr 14, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants