heap-buffer-overflow on jhead-3.04/exif.c:336 Get32s

Bug #1858746 reported by Binbin Li on 2020-01-08

This bug affects 1 person 8

Affects	Status	Importance	Assigned to	Milestone
jhead (Ubuntu)	New	Undecided	Unassigned	

Bug Description

heap-buffer-overflow on jhead-3.04/exif.c:336 Get32s when we run ./jhead ./input/poc.

```
lbb@lbb ./jhead ./input/id_043
Nonfatal Error : './input/id_043' Suspicious offset of first Exif IFD
value
Nonfatal Error : './input/id_043' Maximum Exif directory nesting exceeded
(corrupt Exif header)
Nonfatal Error : './input/id_043' Illegal number format 32768 for tag 1000
in Exif
Nonfatal Error : './input/id_043' Maximum Exif directory nesting exceeded
(corrupt Exif header)
Nonfatal Error : './input/id_043' Illegal number format 95 for Exif gps
tag 002a
Nonfatal Error : './input/id_043' Illegal number format 62152 for Exif gps
tag 91bf
Nonfatal Error : './input/id_043' Illegal number format 65529 for Exif gps
tag ffff
Nonfatal Error : './input/id_043' Illegal number format 0 for Exif gps tag
00ff
Nonfatal Error : './input/id_043' Illegal number format 0 for Exif gps tag
7c00
Nonfatal Error : './input/id_043' Inappropriate format (4) for Exif GPS
coordinates!
Nonfatal Error : './input/id_043' Illegal number format 65535 for Exif gps
tag 1f00
Nonfatal Error : './input/id_043' Illegal number format 128 for Exif gps
tag 0010
Nonfatal Error : './input/id_043' Illegal number format 0 for Exif gps tag
0087
Nonfatal Error : './input/id_043' Illegal number format 128 for Exif gps
tag 0010
Nonfatal Error : './input/id_043' Illegal number format 0 for Exif gps tag
0087
Nonfatal Error : './input/id_043' Illegal number format 0 for Exif gps tag
0092
Nonfatal Error : './input/id_043' Illegal number format 0 for Exif gps tag
0088
Nonfatal Error : './input/id_043' Illegal number format 257 for Exif gps
tag 2d00
Nonfatal Error : './input/id_043' Illegal number format 23110 for Exif gps
tag 4146
Nonfatal Error : './input/id_043' Inappropriate format (12) for Exif GPS
coordinates!
=================================================================
==25863==ERROR: AddressSanitizer: heap-buffer-overflow on address
0x611000009fdd at pc 0x00000040aeff bp 0x7ffe1a579f50 sp 0x7ffe1a579f40
READ of size 1 at 0x611000009fdd thread T0
    #0 0x40aefe in Get32s /home/lbb/afl-experient/Tests/ASAN/jhead-3.
04/exif.c:336
    #1 0x4115dc in ProcessGpsInfo /home/lbb/afl-experient/Tests/ASAN/
jhead-3.04/gpsinfo.c:138
    #2 0x40d9a3 in ProcessExifDir /home/lbb/afl-experient/Tests/ASAN/
jhead-3.04/exif.c:866
    #3 0x40d91c in ProcessExifDir /home/lbb/afl-experient/Tests/ASAN/
jhead-3.04/exif.c:852
    #4 0x40d91c in ProcessExifDir /home/lbb/afl-experient/Tests/ASAN/
jhead-3.04/exif.c:852
    #5 0x40d91c in ProcessExifDir /home/lbb/afl-experient/Tests/ASAN/
jhead-3.04/exif.c:852
    #6 0x40d91c in ProcessExifDir /home/lbb/afl-experient/Tests/ASAN/
jhead-3.04/exif.c:852
    #7 0x40e09a in process_EXIF /home/lbb/afl-experient/Tests/ASAN/jhead-
3.04/exif.c:1041
    #8 0x408318 in ReadJpegSections /home/lbb/afl-experient/Tests/ASAN/
jhead-3.04/jpgfile.c:287
    #9 0x408581 in ReadJpegFile /home/lbb/afl-experient/Tests/ASAN/jhead-
3.04/jpgfile.c:379
    #10 0x405039 in ProcessFile /home/lbb/afl-experient/Tests/ASAN/jhead-
3.04/jhead.c:905
    #11 0x40267d in main /home/lbb/afl-experient/Tests/ASAN/jhead-3.
04/jhead.c:1756
    #12 0x7ff18ec8a82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.
so.6+0x2082f)
    #13 0x403c38 in _start (/home/lbb/afl-experient/Tests/ASAN/jhead-3.
04/jhead+0x403c38)

0x611000009fdd is located 3 bytes to the right of 218-byte region
[0x611000009f00,0x611000009fda)
allocated by thread T0 here:
    #0 0x7ff18f3d5602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.
so.2+0x98602)
    #1 0x40798b in ReadJpegSections /home/lbb/afl-experient/Tests/ASAN/
jhead-3.04/jpgfile.c:173
    #2 0x408581 in ReadJpegFile /home/lbb/afl-experient/Tests/ASAN/jhead-
3.04/jpgfile.c:379
    #3 0x405039 in ProcessFile /home/lbb/afl-experient/Tests/ASAN/jhead-3.
04/jhead.c:905
    #4 0x40267d in main /home/lbb/afl-experient/Tests/ASAN/jhead-3.
04/jhead.c:1756
    #5 0x7ff18ec8a82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.
so.6+0x2082f)
```

Report a bug

This report contains **Public** information
Everyone can see this information.

You are not directly subscribed to this bug's notifications.

Edit bug mail

Other bug subscribers

Subscribe someone else

Notified of all changes

Binbin Li
Salvatore Bonaccorso

May be notified

Alejandro J. Alva...
Ashani Holland
Bruno Garcia
CRC
Charlie_Smotherman
Debian PTS
Doraann2
Franko Fang
HaySayCheese
Hidagawa
Jesse Jones
José Alfonso
Matt j
Mr. MInhaj
Name Changed
PCTeacher012
Paolo Topa
Peter Bullert
Punnsa
Richard Seguin
Richard Williams
Tom Weiss
Vasanth
Vic Parker
ahepas
basilisgabri
dsfkj dfjx
eoininmoran
ganesh
linuxgijs
nikonikic42
projevie@hotmail.com
qadir
sankaran
van

Bug attachments

POC

Add attachment

```
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/lbb/afl-experient/
Tests/ASAN/jhead-3.04/exif.c:336 Get32s
Shadow bytes around the buggy address:
  0x0c227fff93a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff93b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff93c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff93d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff93e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c227fff93f0: 00 00 00 00 00 00 00 00 00 00 00[02]fa fa fa fa
  0x0c227fff9400: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff9410: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff9420: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff9430: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff9440: 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
  Heap right redzone: fb
  Freed heap region: fd
  Stack left redzone: f1
  Stack mid redzone: f2
  Stack right redzone: f3
  Stack partial redzone: f4
  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
==25863==ABORTING
```

Tags: heap-buffer-overflow jhead

CVE References

2020-6625

Binbin Li (libbin) wrote on 2020-01-08:	#1
POC (240 bytes, application/octet-stream)	

See full activity log

To post a comment you must log in.