heap-buffer-overflow on jhead(v3.03, v3.04)/jpgqguess.c:109 process_DQT

Bug #1858744 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 while running jhead(v3.03, v3.04). I can not confirm
if this bug is needed to patch. Deatil log as follow: (POC in attachment)

lbb@lbb ./jhead/jhead ./input/id_m075

Nonfatal Error : './input/id_m075' Suspicious offset of first Exif IFD
value
Nonfatal Error : './input/id_m075' Illegally sized Exif subdirectory
(60138 entries)
Nonfatal Error : './input/id_m075' Extraneous 11 padding bytes before
section 03
Nonfatal Error : './input/id_m075' Extraneous 10 padding bytes before
section DB
Nonfatal Error : './input/id_m075' Extraneous 12 padding bytes before
section 03
Nonfatal Error : './input/id_m075' Extraneous 164 padding bytes before
section C4
Nonfatal Error : './input/id_m075' Extraneous 10 padding bytes before
section EA
Nonfatal Error : './input/id_m075' Extraneous 10 padding bytes before
section 03
Nonfatal Error : './input/id_m075' Extraneous 11 padding bytes before
section 03
Nonfatal Error : './input/id_m075' Extraneous 10 padding bytes before
section DB
=================================================================
==19742==ERROR: AddressSanitizer: heap-buffer-overflow on address
0x60700000ddc3 at pc 0x0000004e5c14 bp 0x7fff938f6490 sp 0x7fff938f6488
READ of size 1 at 0x60700000ddc3 thread T0
    #0 0x4e5c13 in process_DQT /home/lbb/afl-experient/Tests/ASAN/jhead-3.
04/jpgqguess.c:109:38
    #1 0x4e2d9c in ReadJpegSections /home/lbb/afl-experient/Tests/ASAN/
jhead-3.04/jpgfile.c:223:17
    #2 0x4e39c7 in ReadJpegFile /home/lbb/afl-experient/Tests/ASAN/jhead-
3.04/jpgfile.c:379:11
    #3 0x4dea31 in ProcessFile /home/lbb/afl-experient/Tests/ASAN/jhead-3.
04/jhead.c:905:10
    #4 0x4dea31 in main /home/lbb/afl-experient/Tests/ASAN/jhead-3.
04/jhead.c:1756
    #5 0x7f3ea4c5f82f in __libc_start_main /build/glibc-LK5gWL/glibc-2.
23/csu/../csu/libc-start.c:291
    #6 0x435e48 in _start (/home/lbb/afl-experient/Tests/ASAN/jhead-3.
04/jhead+0x435e48)

0x60700000ddc3 is located 0 bytes to the right of 67-byte region
[0x60700000dd80,0x60700000ddc3)
allocated by thread T0 here:
    #0 0x4bcdf2 in __interceptor_malloc (/home/lbb/afl-experient/
Tests/ASAN/jhead-3.04/jhead+0x4bcdf2)
    #1 0x4e291c in ReadJpegSections /home/lbb/afl-experient/Tests/ASAN/
jhead-3.04/jpgfile.c:173:25
    #2 0x4e39c7 in ReadJpegFile /home/lbb/afl-experient/Tests/ASAN/jhead-
3.04/jpgfile.c:379:11

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/lbb/afl-experient/
Tests/ASAN/jhead-3.04/jpgqguess.c:109 process_DQT
Shadow bytes around the buggy address:
  0x0c0e7fff9b60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff9b70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff9b80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff9b90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff9ba0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c0e7fff9bb0: 00 00 00 00 00 00 00 00[03]fa fa fa fa fa 00 00
  0x0c0e7fff9bc0: 00 00 00 00 00 00 03 fa fa fa fa fa 00 00 00 00
  0x0c0e7fff9bd0: 00 00 00 00 03 fa fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff9be0: 00 00 03 fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c0e7fff9bf0: 03 fa fa fa fa fa fd fd fd fd fd fd fd fd fd fd
  0x0c0e7fff9c00: 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
  Left alloca redzone: ca
  Right alloca redzone: cb
==19742==ABORTING
```

See original description

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

Tags: jhead stack-buffer-overflow

CVE References

2020-6624

Binbin Li (libbin) wrote on 2020-01-08:	#1
POC (102.7 KiB, application/octet-stream)	

description:updated

See full activity log

To post a comment you must log in.