

[New issue](#)[Jump to bottom](#)

Multiple Segmentation fault in jhead via a crafted jpg file #17

🔒 Closed giantbranch opened this issue on Feb 26, 2021 · 3 comments

giantbranch commented on Feb 26, 2021

Description of problem:

Multiple Segmentation fault in jhead via a crafted jpg file

Version-Release number of selected component (if applicable):

I tested the following version:

Jhead version: 3.05

Jhead version: 3.04

How reproducible:

git clone --depth=1 <https://github.com/Matthias-Wandel/jhead.git> && cd jhead && make CC="clang" -e CFLAGS="-g -fsanitize=address" -e LDFLAGS="-g -fsanitize=address"

Steps to Reproduce:

1.just run the following command

Segmentation fault in ProcessCanonMakerNoteDir

```
./jhead -v ./tests_61418.jpg
```

Segmentation fault in Get16u

```
./jhead -v ./tests_61761.jpg
```

Segmentation fault in Get32s

```
./jhead -v ./tests_61763.jpg
```

poc:

[jhead-multi-seg.zip](#)

They are all because of wild-addr-read.

Actual results:

Segmentation fault in ProcessCanonMakerNoteDir

```
$ ./jhead -v ./tests_61418.jpg
Exif header 7166 bytes long
Exif section in Intel order
(dir has 9 entries)
  Make = "Canon"
  Model = "Canon DIGITAL IXUS?"
  Orientation = 1
  XResolution = 180/1
  YResolution = 180/1
  ResolutionUnit = 2
  DateTime = "2001:06:09 15:17:32"
  YCbCrPositioning = 1
  ExifOffset = 184
  Exif Dir:(dir has 27 entries)
    ExposureTime = 1/350
    FNumber = 40/10
    ExifVersion = "0210"
    DateTimeOriginal = "2001:06:09 15:17:32"
    DateTimeDigitized = "2001:06:09 15:17:32"
    ComponentsConfiguration = "?"
    CompressedBitsPerPixel = 3/1
    ShutterSpeedValue = 553859/65536
    ApertureValue = 262144/65536
    ExposureBiasValue = 0/3
    MaxApertureValue = 194698/65536
    SubjectDistance = 3750/1000
    MeteringMode = 2
    Flash = 0
    FocalLength = 346/32
    Maker note: (dir has 10 entries)
      Canon maker tag 0001 Value = 0, 1024, 6, 0, 9728, 512, 0, 768, 256, 0, 0, 256, 0, 256, 512, 256, ...
      Canon maker tag 0002 Value = 0, 0, 0, 256
      Canon maker tag 0003 Value = 512, 23040, 54017, 40448
      Canon maker tag 0004 Value = 0, 0, 0, 0, 7680, 0, 35840, 512, 32769, 3584, 1, 0, 0, 256, 1024
      Canon maker tag 0005 Value = 0, 0, 0, 512, 48, 0
      Canon maker tag 0006 Value = "IMG:JPEG file"
AddressSanitizer:DEADLYSIGNAL
=====
==25461==ERROR: AddressSanitizer: SEGV on unknown address 0x624100002100 (pc 0x0000004dfa3c bp 0x7ffe87bf3b0 sp 0x7ffe87baf2d0 T0)
==25461==The signal is caused by a READ memory access.
#0 0x4dfa3c in ProcessCanonMakerNoteDir /root/fuzz/jhead/makernote.c:105:29
#1 0x4df3ea in ProcessMakerNote /root/fuzz/jhead/makernote.c:189:9
#2 0x4d57e9 in ProcessExifDir /root/fuzz/jhead/exif.c:559:13
#3 0x4d7adf in ProcessExifDir /root/fuzz/jhead/exif.c:851:25
#4 0x4d494a in process_EXIF /root/fuzz/jhead/exif.c:1040:5
#5 0x4cf08d in ReadJpegSections /root/fuzz/jhead/jpgfile.c:289:25
#6 0x4cf096 in ReadJpegFile /root/fuzz/jhead/jpgfile.c:381:11
```

```
#7 0x4c8850 in ProcessFile /root/fuzz/jhead/jhead.c:908:10
#8 0x4c74e5 in main /root/fuzz/jhead/jhead.c:1759:13
#9 0x7fb2bd2083f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
#10 0x41b858 in _start (/root/fuzz/jhead/jhead+0x41b858)
```

AddressSanitizer can not provide additional info.

```
SUMMARY: AddressSanitizer: SEGV /root/fuzz/jhead/makernote.c:105:29 in ProcessCanonMakerNoteDir
==25461==ABORTING
```

Segmentation fault in Get16u

```
$ ./jhead -v ./tests_61761.jpg
Exif header 7166 bytes long
Exif section in Intel order
(dir has 213 entries)
  Make = "Canon"
```

```
Nonfatal Error : './tests_61761.jpg' Illegal value pointer for tag 0110 in Exif
Unknown Tag 6112 Value = 1
```

```
Nonfatal Error : './tests_61761.jpg' Illegal value pointer for tag e21a in Exif
```

```
Nonfatal Error : './tests_61761.jpg' Illegal value pointer for tag 011b in Exif
Unknown Tag 9e28 Value = 2
DateTime = "2001:06:09 1x:17:32"
YCbCrPositioning = 1
ExifOffset = 184
```

```
.....
.....
.....
.....
.....
.....
```

AddressSanitizer: DEADLY SIGNAL

```
=====
==25463==ERROR: AddressSanitizer: SEGV on unknown address 0x6241000011b7 (pc 0x0000004d399c bp 0x7ffc7716b130 sp 0x7ffc7716b0e0 T0)
==25463==The signal is caused by a READ memory access.
```

```
#0 0x4d399c in Get16u /root/fuzz/jhead/exif.c:323:17
#1 0x4d40e1 in PrintFormatNumber /root/fuzz/jhead/exif.c:378:45
#2 0x4dfbdd in ProcessCanonMakerNoteDir /root/fuzz/jhead/makernote.c:123:21
#3 0x4df3ea in ProcessMakerNote /root/fuzz/jhead/makernote.c:189:9
#4 0x4d57e9 in ProcessExifDir /root/fuzz/jhead/exif.c:559:13
#5 0x4d7adf in ProcessExifDir /root/fuzz/jhead/exif.c:851:25
#6 0x4d7adf in ProcessExifDir /root/fuzz/jhead/exif.c:851:25
#7 0x4d494a in process_EXIF /root/fuzz/jhead/exif.c:1040:5
#8 0x4cf08d in ReadJpegSections /root/fuzz/jhead/jpgfile.c:289:25
#9 0x4cf096 in ReadJpegFile /root/fuzz/jhead/jpgfile.c:381:11
#10 0x4c8850 in ProcessFile /root/fuzz/jhead/jhead.c:908:10
#11 0x4c74e5 in main /root/fuzz/jhead/jhead.c:1759:13
#12 0x7f45bf8ba83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
#13 0x41b858 in _start (/root/fuzz/jhead/jhead+0x41b858)
```

AddressSanitizer can not provide additional info.

```
SUMMARY: AddressSanitizer: SEGV /root/fuzz/jhead/exif.c:323:17 in Get16u
==25463==ABORTING
```

Segmentation fault in Get32s

```
$ ./jhead -v ./tests_61763.jpg
Exif header 7166 bytes long
Exif section in Intel order
(dir has 42 entries)
  Make = "Canon"
  Model = "?anon DIGITAL IXUS?"
  Orientation = 1
  XResolution = 180/1
  YResolution = 180/1
  ResolutionUnit = 2
  DateTime = "2001:06:09 15:17:32"
  YCbCrPositioning = 1
  ExifOffset = 184
  Exif Dir:(dir has 27 e
```

```
.....
.....
.....
.....
.....
.....
```

AddressSanitizer: DEADLY SIGNAL

```
=====
==25465==ERROR: AddressSanitizer: SEGV on unknown address 0x62410000200b (pc 0x0000004d3bc8 bp 0x7ffe1275af10 sp 0x7ffe1275ae80 T0)
==25465==The signal is caused by a READ memory access.
```

```
#0 0x4d3bc8 in Get32s /root/fuzz/jhead/exif.c:336:18
#1 0x4d419b in PrintFormatNumber /root/fuzz/jhead/exif.c:388:32
#2 0x4dfbdd in ProcessCanonMakerNoteDir /root/fuzz/jhead/makernote.c:123:21
#3 0x4df3ea in ProcessMakerNote /root/fuzz/jhead/makernote.c:189:9
#4 0x4d57e9 in ProcessExifDir /root/fuzz/jhead/exif.c:559:13
#5 0x4d7adf in ProcessExifDir /root/fuzz/jhead/exif.c:851:25
#6 0x4d494a in process_EXIF /root/fuzz/jhead/exif.c:1040:5
#7 0x4cf08d in ReadJpegSections /root/fuzz/jhead/jpgfile.c:289:25
#8 0x4cf096 in ReadJpegFile /root/fuzz/jhead/jpgfile.c:381:11
#9 0x4c8850 in ProcessFile /root/fuzz/jhead/jhead.c:908:10
#10 0x4c74e5 in main /root/fuzz/jhead/jhead.c:1759:13
#11 0x7f88040ac83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
#12 0x41b858 in _start (/root/fuzz/jhead/jhead+0x41b858)
```


AddressSanitizer can not provide additional info.

```
SUMMARY: AddressSanitizer: SEGV /root/fuzz/jhead/exif.c:336:18 in Get32s
==25465==ABORTING
```

Additional info:

Founder: giantbranch of NSFOCUS Security Team

Fixed by [a50953a](#)

 **Matthias-Wandel** closed this as completed on Mar 4, 2021

akhuettel commented on Oct 18

This (the segfault in Get32s) looks like it's identical to <https://bugs.launchpad.net/ubuntu/+source/jhead/+bug/1858746>
Can you confirm this?

 **Matthias-Wandel** commented on Oct 18

Owner

I will look at it next time I find time to work on jhead. Don't know when that is.

----- Original Message -----

From: "Andreas K. Hüttel" ***@*** **>

To: "Matthias-Wandel/jhead" ***@*** **>

Cc: "Matthias Wandel" ***@***.***>; "State change"

@ **>

Sent: 10/18/2022 6:58:05 PM

Subject: Re: [Matthias-Wandel/jhead] Multiple Segmentation fault in jhead via a crafted jpg file (#17)

This (the segfault in Get32s) looks like it's identical to

<https://bugs.launchpad.net/ubuntu/+source/jhead/+bug/1858746>

Can you confirm this?

—

Reply to this email directly, view it on GitHub

<[#17 \(comment\)](#)>,

or unsubscribe

<<https://github.com/notifications/unsubscribe-auth/AOSCO3HJNMVROAVRGISNV5DWD4MO3ANCNFSM4YH7XISA>>.

You are receiving this because you modified the open/close

state.Message ID:

@ **>

...

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

