

heap-buffer-overflow on jhead-3.04/jpgfile.c:285 ReadJpegSections

Moderate F-ZhaoYang published GHSA-7pr6-xq4f-qhgc on Oct 30, 2020

Package	
jhead	
Affected versions	Patched versions
<3.04	None

Description

Impact

heap-buffer-overflow on jhead-3.04/jpgfile.c:285 ReadJpegSections
poc: <https://bugs.launchpad.net/ubuntu/+source/jhead/+bug/1900821/+attachment/5424955/+files/poc%20%282%29>

```
fstark@fstark-virtual-machine:~/jhead$ ./jhead fuzz1\;id\;000015\,sig\;06\,src\;000476\,time\;412880\,op\;arith8\,pos\;31\,val\;+29
=====
==957==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000efd2 at pc 0x7f6d38f94676 bp 0x7ffd0abe47d0 sp 0x7ffd0abe3f78
READ of size 4 at 0x60200000efd2 thread T0
#0 0x7f6d38f94675 in memcmp (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x77675)
#1 0x40e810 in ReadJpegSections /home/fstark/jhead/jpgfile.c:285
#2 0x410e86 in ReadJpegSections /home/fstark/jhead/jpgfile.c:125
#3 0x410e86 in ReadJpegFile /home/fstark/jhead/jpgfile.c:378
#4 0x40858b in ProcessFile /home/fstark/jhead/jhead.c:905
#5 0x402f2c in main /home/fstark/jhead/jhead.c:1756
#6 0x7f6d3886a83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
#7 0x406708 in _start (/home/fstark/jhead/jhead+0x406708)

0x60200000efd2 is located 0 bytes to the right of 2-byte region [0x60200000efd0,0x60200000efd2)
allocated by thread T0 here:
#0 0x7f6d38fb5602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
#1 0x40e4a8 in ReadJpegSections /home/fstark/jhead/jpgfile.c:172

SUMMARY: AddressSanitizer: heap-buffer-overflow ??? memcmp
Shadow bytes around the buggy address:
 0x0c047fff9da0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9db0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9dc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9dd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9de0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c047fff9df0: fa fa fa fa fa fa fa fa fa fa[02]fa fa fa 02 fa
 0x0c047fff9e00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9e10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9e20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9e30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9e40: 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
==957==ABORTING
```

Patches

Fixed by 5186ddc
[Matthias-Wandel@ 5186ddc](#)

References

[Matthias-Wandel#7](#)

Severity

Moderate

CVE ID

No known CVE

Weaknesses

No CWEs