libpano13-bin: out of bounds read in PTinfo

74 views

pola lemu Apr 22, 2021, 1:04:58 PM

to hugin and other free panoramic software

In libpano13-2.9.20, there is an out-of-bounds read bug.
The bug in function panoParserFindOLine() in parser.c.

line 2494 called strchr, the return pointer is null and then `ptr++` to 0x1.

```
     2494     ptr = strchr(ptr, '\n');
           // ptr=0x00007fffffffe1f8  →  0x0000000000000000
 → 2495     ptr++;
```

So at line 2467, the *ptr(0x01) cannot access and resulted in an out of bounds read and crash.

```
// ptr=0x00007fffffffe1f8  →  0x0000000000000001
 → 2466     while (ptr != NULL) {
●  2467      if (*ptr == 'o') {
```

the backtrace: