# Optical Character Recognition (GOCR) Bugs

**Status: Alpha**
**Brought to you by: joerg10**

## #42 A stack-buffer-overflow in pgm2asc.c:2648:39

**Status:** open **Owner:** nobody **Labels:** None
**Priority:** 5
**Updated:** 2020-08-03 **Created:** 2020-08-03 **Creator:** zhouan **Private:** No

### System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), gocr (latest jocr-dev 0.53-20200802)

### Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" ./configure

### Command line

./src/gocr -m 4 ./stack-overflow-try_to_divide_boxes-pgm2asc-2648

### AddressSanitizer output

```
=================================================================
==35440==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffeaa63b3fc at pc 0x0
READ of size 4 at 0x7ffeaa63b3fc thread T0
    #0 0x53d701 in try_to_divide_boxes /home/seviezhou/jocr/src/pgm2asc.c:2648:39
    #1 0x54a14d in pgm2asc /home/seviezhou/jocr/src/pgm2asc.c:3415:3
    #2 0x518776 in main /home/seviezhou/jocr/src/gocr.c:350:5
    #3 0x7fad0439d83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-s
    #4 0x41a768 in _start (/home/seviezhou/gocr/src/gocr+0x41a768)

Address 0x7ffeaa63b3fc is located in stack of thread T0 at offset 3100 in frame
    #0 0x5388df in try_to_divide_boxes /home/seviezhou/jocr/src/pgm2asc.c:2377

  This frame has 8 object(s):
    [32, 1408) 'boxa' (line 2378)
    [1536, 2912) 'boxb' (line 2378)
    [3040, 3072) 'a2' (line 2380)
    [3104, 3136) 'ci' (line 2383) <== Memory access at offset 3100 underflows this variable
    [3168, 3232) 's1' (line 2383)
    [3264, 3300) 'xi' (line 2386)
    [3344, 3352) 'buf' (line 2438)
    [3376, 3440) 'buf351' (line 2475)
HINT: this may be a false positive if your program uses some custom stack unwind mechanism
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/seviezhou/jocr/src/pgm2asc.c:2648:39
Shadow bytes around the buggy address:
  0x1000554bf620: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000554bf630: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000554bf640: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000554bf650: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000554bf660: 00 00 00 00 00 00 00 00 f2 f2 f2 f2 f2 f2 f2 f2
=>0x1000554bf670: f2 f2 f2 f2 f2 f2 f2 f2 00 00 00 00 f2 f2 f2[f2]
  0x1000554bf680: 00 00 00 00 f2 f2 f2 f2 00 00 00 00 00 00 00 00
  0x1000554bf690: f2 f2 f2 f2 00 00 00 00 04 f2 f2 f2 f2 f2 f8 f2
  0x1000554bf6a0: f2 f2 00 00 00 00 00 00 00 00 f3 f3 f3 f3 f3 f3
  0x1000554bf6b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000554bf6c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  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
==35440==ABORTING
```

**1 Attachments**

stack-overflow-try_to_divide_boxes-pgm2asc-2648.zip

### Discussion

Log in to post a comment.