# Optical Character Recognition (GOCR) Bugs

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

## #39 A stack-buffer-underflow in pgm2asc.c:1689:24

**Status:** open **Owner:** nobody **Labels:** bug (3)
**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 @@

## AddressSanitizer output

```
=================================================================
==38065==ERROR: AddressSanitizer: stack-buffer-underflow on address 0x7ffe7647eb3c at pc 0x
READ of size 4 at 0x7ffe7647eb3c thread T0
    #0 0x52ddfe in measure_pitch /home/seviezhou/jocr/src/pgm2asc.c:1689:24
    #1 0x549a9f in pgm2asc /home/seviezhou/jocr/src/pgm2asc.c:3377:3
    #2 0x518776 in main /home/seviezhou/jocr/src/gocr.c:350:5
    #3 0x7ff058f3083f 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 0x7ffe7647eb3c is located in stack of thread T0 at offset 28 in frame
    #0 0x529aaf in measure_pitch /home/seviezhou/jocr/src/pgm2asc.c:1455

  This frame has 1 object(s):
    [32, 4128) 'pdists' (line 1456) <== Memory access at offset 28 underflows this variable
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-underflow /home/seviezhou/jocr/src/pgm2asc.c:1689:2
Shadow bytes around the buggy address:
  0x10004ec87d10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10004ec87d20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10004ec87d30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10004ec87d40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10004ec87d50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10004ec87d60: 00 00 00 00 f1 f1 f1[f1]00 00 00 00 00 00 00 00
  0x10004ec87d70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10004ec87d80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10004ec87d90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10004ec87da0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10004ec87db0: 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
==38065==ABORTING
```

**1 Attachments**

stack-underflow-measure_pitch-pgm2asc-1689.zip

## Discussion

Log in to post a comment.