



Optical Character Recognition (GOCR) Bugs

Status: Alpha
Brought to you by: joerg10

#40 A use-after-free in pgm2asc.c:2857:51

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 ./use-after-free-context_correction-pgm2asc-2857

AddressSanitizer output

```
=====
==59747==ERROR: AddressSanitizer: heap-use-after-free on address 0x61a000012a4 at pc 0x0000000000000000
READ of size 4 at 0x61a000012a4 thread T0
#0 0x5456ee in context_correction /home/seviezhou/jocr/src/pgm2asc.c:2857:51
#1 0x54a291 in pgm2asc /home/seviezhou/jocr/src/pgm2asc.c:3427:28
#2 0x518776 in main /home/seviezhou/jocr/src/gocr.c:350:5
#3 0x7f4e7058983f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:308
#4 0x41a768 in _start (/home/seviezhou/jocr/src/gocr+0x41a768)

0x61a000012a4 is located 36 bytes inside of 1376-byte region [0x61a00001280,0x61a000017e0)
freed by thread T0 here:
#0 0x4de7b8 in __interceptor_cfree.localalias.0 /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_cfree.cpp:112
#1 0x54c1a7 in free_box /home/seviezhou/jocr/src/box.c:122:3

previously allocated by thread T0 here:
#0 0x4de978 in __interceptor_malloc /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:144
#1 0x54bdc2 in malloc_box /home/seviezhou/jocr/src/box.c:96:24

SUMMARY: AddressSanitizer: heap-use-after-free /home/seviezhou/jocr/src/pgm2asc.c:2857:51 in context_correction
Shadow bytes around the buggy address:
 0x0c347fff8200: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c347fff8210: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c347fff8220: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c347fff8230: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c347fff8240: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c347fff8250: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c347fff8260: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c347fff8270: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c347fff8280: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c347fff8290: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c347fff82a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
==59747==ABORTING
```

1 Attachments

[use-after-free-context_correction-pgm2asc-2857.zip](#)

Discussion

[Log in](#) to post a comment.

SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

Team

SourceForge Headquarters

225 Broadway Suite 1600

San Diego, CA 92101

+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status



© 2022 Slashdot Media. All Rights Reserved.

[Terms](#)

[Privacy](#)

[Opt Out](#)

[Advertise](#)