14isnot40 / vul_discovery Public

Code Issues Pull requests Actions Projects Security Insights

06d04dbbc6

vul_discovery / poc / bit2spr vulnerability discovery.md.pdf

14isnot40 Add files via upload History

1 contributor

443 KB

bit2spr vulnerability discovery

0x1 bit2spr introduction

This bit2spr converts bitmaps in X-bitmap format to the format used by the sprite package.

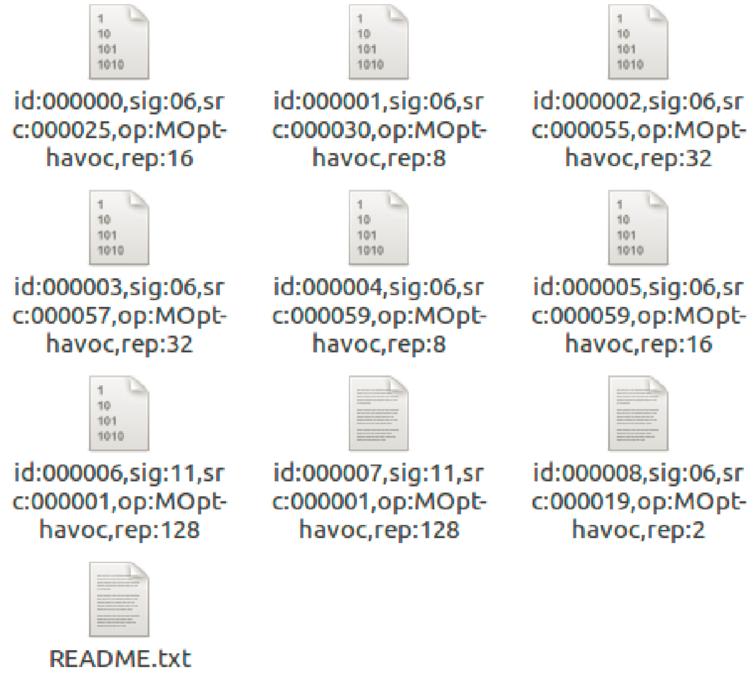
bit2spr is a ctan graphics package, widely used in texlive, ctex.

0x2 Fuzzing results

By using the modified AFL tools in 24hs, we found crashes with the cmd:

```
-i /fuzz_test/in -o /fuzz_test/out bit2spr @@ /dev/null
```

some poc can be produced in the output/crashes/



id:000000,sig:06,src:000025,op:MOpt-havoc,rep:16

id:000001,sig:06,src:000030,op:MOpt-havoc,rep:8

id:000002,sig:06,src:000055,op:MOpt-havoc,rep:32

id:000003,sig:06,src:000057,op:MOpt-havoc,rep:32

id:000004,sig:06,src:000059,op:MOpt-havoc,rep:8

id:000005,sig:06,src:000059,op:MOpt-havoc,rep:16

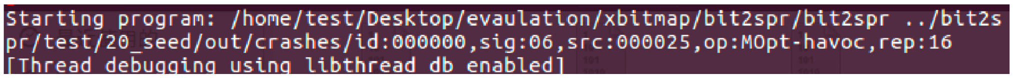
id:000006,sig:11,src:000001,op:MOpt-havoc,rep:128

id:000007,sig:11,src:000001,op:MOpt-havoc,rep:128

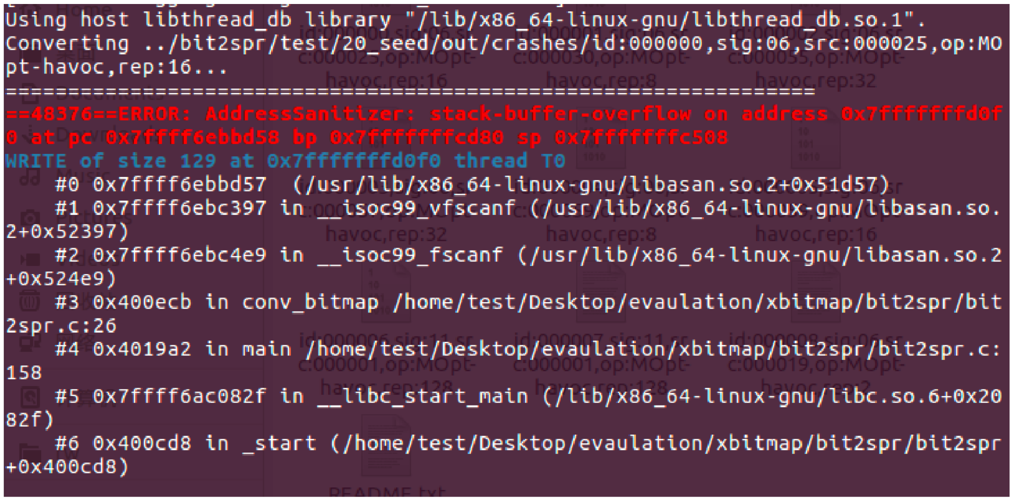
id:000008,sig:06,src:000019,op:MOpt-havoc,rep:2

README.txt

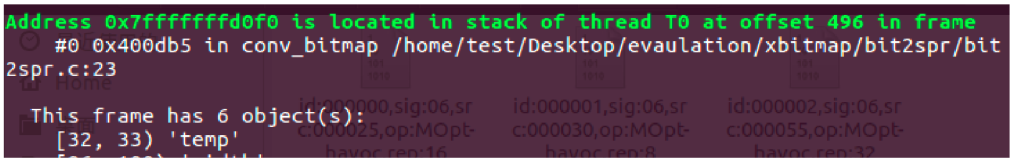
Add the address sanitizer option when compiling bit2spr using gcc, and then run the sample under the crashes folder



```
Starting program: /home/test/Desktop/evaulation/xbitmap/bit2spr/bit2spr ../bit2spr/test/20_seed/out/crashes/id:000000,sig:06,src:000025,op:MOpt-havoc,rep:16
[Thread debugging using libthread_db enabled]
```



```
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Converting ../bit2spr/test/20_seed/out/crashes/id:000000,sig:06,src:000025,op:MO
pt-havoc,rep:16...
=================================================================
==48376==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7fffffffd0f
0 at pc 0x7ffff6ebbd58 bp 0x7fffffffcd80 sp 0x7fffffffc508
WRITE of size 129 at 0x7fffffffd0f0 thread T0
    #0 0x7ffff6ebbd57  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x51d57)
    #1 0x7ffff6ebc397 in __isoc99_vfscanf (/usr/lib/x86_64-linux-gnu/libasan.so.
2+0x52397)
    #2 0x7ffff6ebc4e9 in __isoc99_fscanf (/usr/lib/x86_64-linux-gnu/libasan.so.2
+0x524e9)
    #3 0x400ecb in conv_bitmap /home/test/Desktop/evaulation/xbitmap/bit2spr/bit
2spr.c:26
    #4 0x4019a2 in main /home/test/Desktop/evaulation/xbitmap/bit2spr/bit2spr.c:
158
    #5 0x7ffff6ac082f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x20
82f)
    #6 0x400cd8 in _start (/home/test/Desktop/evaulation/xbitmap/bit2spr/bit2spr
+0x400cd8)
```



```
Address 0x7fffffffd0f0 is located in stack of thread T0 at offset 496 in frame
    #0 0x400db5 in conv_bitmap /home/test/Desktop/evaulation/xbitmap/bit2spr/bit
2spr.c:23

  This frame has 6 object(s):
    [32, 33) 'temp'
```