Fix 3 security problems found by fuzzer #23

Open everestsummer wants to merge 6 commits into `lecram:master` from `everestsummer:master`

Conversation 3 Commits 6 Checks 0 Files changed 1

everestsummer commented on Aug 20

The following sample generated by fuzzer may cause a SIGSEGV in gifdec.

The root cause is variable "key" may be a larger value than count of entries, causing program accesses out-of-bounds heap buffer.

```
Program received signal SIGSEGV, Segmentation fault.
0x0000555555558280 in read_image_data (interlace=64, gif=0x55555555d2a0) at gifdec.c:395
395 entry = table->entries[entry.prefix];
(gdb) bt
#0 0x0000555555558280 in read_image_data (interlace=64, gif=0x55555555d2a0) at gifdec.c:395
#1 read_image (gif=0x55555555d2a0) at gifdec.c:441
#2 gd_get_frame (gif=gif@entry=0x55555555d2a0) at gifdec.c:500
#3 0x00005555555554b4 in main (argc=, argv=0x7fffffffe1a8) at example2.c:38
```

crash-1.zip

everestsummer added 3 commits 3 months ago

```
Fix: Security: Uninitialized variables may cause SIGSEGV                          777d74f
Fix: Security: 'key' maybe a value bigger than table->nentries, causi…  …         f29dc41
Fix: Security: entry.prefix may be a bigger value than table->nentrie…  …         9705582
```

everestsummer commented on Aug 20 Author

crash-3.zip

`9705582`

Fixed another problem, entry.prefix will be 4096 in this case(crash-3.zip), causing an OOB read.

everestsummer changed the title ~~Fix 2 security problems found by fuzzer~~ **Fix 3 security problems found by fuzzer** on Aug 20

everestsummer added 3 commits 3 months ago

`Fix: Security: Infinite loop in discard_sub_blocks` bdfad6b

`Fix: Security: Infinite loop in read_ext` 271d1d2

`Fix: Security: Prevent i from being overflowed to negative value (and…` … b17f410

TinyNiko commented on Oct 16 • edited

`

```
==69822==ERROR: AddressSanitizer: heap-use-after-free on address 0x61c00000c0c1 at pc 0x00000051898b
bp 0x7fffffffcd10 sp 0x7fffffffcd08
WRITE of size 1 at 0x61c00000c0c1 thread T0
#0 0x51898a in read_image_data /home/niko/gitrepo/gifdec/gifdec.c:409:66
#1 0x51570d in read_image /home/niko/gitrepo/gifdec/gifdec.c:462:12
#2 0x513f2a in gd_get_frame /home/niko/gitrepo/gifdec/gifdec.c:521:9
#3 0x51b2b1 in main /home/niko/gitrepo/gifdec/example.c:84:15
#4 0x7ffff6af0c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310
#5 0x41a609 in _start (/home/niko/gitrepo/gifdec/example+0x41a609)

0x61c00000c0c1 is located 65 bytes inside of 1800-byte region [0x61c00000c080,0x61c00000c788)
freed by thread T0 here:
#0 0x4da2f0 in __interceptor_free.localalias.0 (/home/niko/gitrepo/gifdec/example+0x4da2f0)
#1 0x7fffea7b7d1a (/usr/lib/x86_64-linux-gnu/dri/vmwgfx_dri.so+0x464d1a)

previously allocated by thread T0 here:
#0 0x4da4c0 in __interceptor_malloc (/home/niko/gitrepo/gifdec/example+0x4da4c0)
#1 0x7fffea7ba11c (/usr/lib/x86_64-linux-gnu/dri/vmwgfx_dri.so+0x46711c)
```

```
SUMMARY: AddressSanitizer: heap-use-after-free /home/niko/gitrepo/gifdec/gifdec.c:409:66 in
read_image_data
Shadow bytes around the buggy address:
0x0c387fff97c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c387fff97d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c387fff97e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c387fff97f0: fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c387fff9800: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c387fff9810: fd fd fd fd fd fd fd fd[fd]fd fd fd fd fd fd fd
0x0c387fff9820: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c387fff9830: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c387fff9840: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c387fff9850: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c387fff9860: fd 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
==69822==ABORTING
`
```

TinyNiko commented 18 days ago

@everestsummer CVE-2022-43359 assigned

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants