Summary

There is a memory leak vulnerability in apng2gif-1.7.1.

https://apng2gif.sourceforge.net/

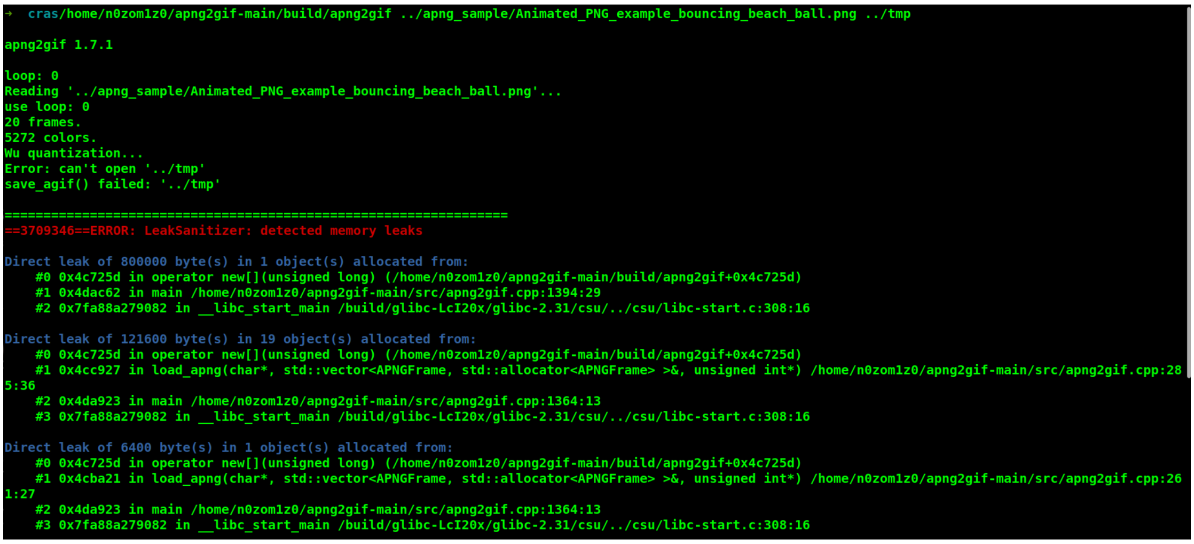
https://github.com/zyzsdy/apng2gif

Details

When I compiled it with ASAN, and ran apng2gif in this way:

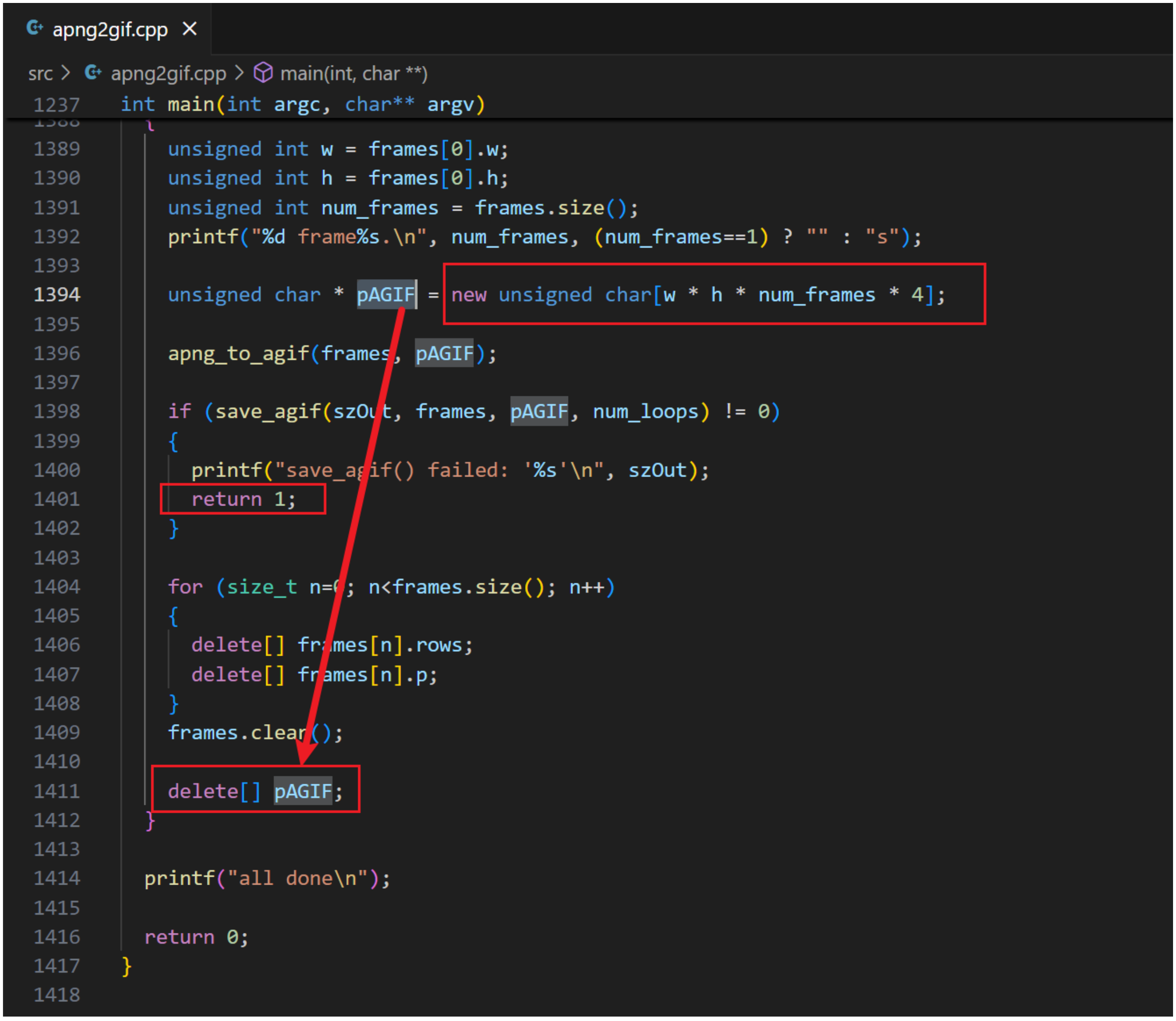
```
/home/n0zom1z0/apng2gif-main/build/apng2gif
../apng_sample/Animated_PNG_example_bouncing_beach_ball.png ../tmp
```

Error occurred:



```
→  cras/home/n0zom1z0/apng2gif-main/build/apng2gif ../apng_sample/Animated_PNG_example_bouncing_beach_ball.png ../tmp

apng2gif 1.7.1

loop: 0
Reading '../apng_sample/Animated_PNG_example_bouncing_beach_ball.png'...
use loop: 0
20 frames.
5272 colors.
Wu quantization...
Error: can't open '../tmp'
save_agif() failed: '../tmp'

=================================================================
==3709346==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 800000 byte(s) in 1 object(s) allocated from:
    #0 0x4c725d in operator new[](unsigned long) (/home/n0zom1z0/apng2gif-main/build/apng2gif+0x4c725d)
    #1 0x4dac62 in main /home/n0zom1z0/apng2gif-main/src/apng2gif.cpp:1394:29
    #2 0x7fa88a279082 in __libc_start_main /build/glibc-LcI20x/glibc-2.31/csu/../csu/libc-start.c:308:16

Direct leak of 121600 byte(s) in 19 object(s) allocated from:
    #0 0x4c725d in operator new[](unsigned long) (/home/n0zom1z0/apng2gif-main/build/apng2gif+0x4c725d)
    #1 0x4cc927 in load_apng(char*, std::vector<APNGFrame, std::allocator<APNGFrame> >&, unsigned int*) /home/n0zom1z0/apng2gif-main/src/apng2gif.cpp:28
5:36
    #2 0x4da923 in main /home/n0zom1z0/apng2gif-main/src/apng2gif.cpp:1364:13
    #3 0x7fa88a279082 in __libc_start_main /build/glibc-LcI20x/glibc-2.31/csu/../csu/libc-start.c:308:16

Direct leak of 6400 byte(s) in 1 object(s) allocated from:
    #0 0x4c725d in operator new[](unsigned long) (/home/n0zom1z0/apng2gif-main/build/apng2gif+0x4c725d)
    #1 0x4cba21 in load_apng(char*, std::vector<APNGFrame, std::allocator<APNGFrame> >&, unsigned int*) /home/n0zom1z0/apng2gif-main/src/apng2gif.cpp:26
1:27
    #2 0x4da923 in main /home/n0zom1z0/apng2gif-main/src/apng2gif.cpp:1364:13
    #3 0x7fa88a279082 in __libc_start_main /build/glibc-LcI20x/glibc-2.31/csu/../csu/libc-start.c:308:16
```

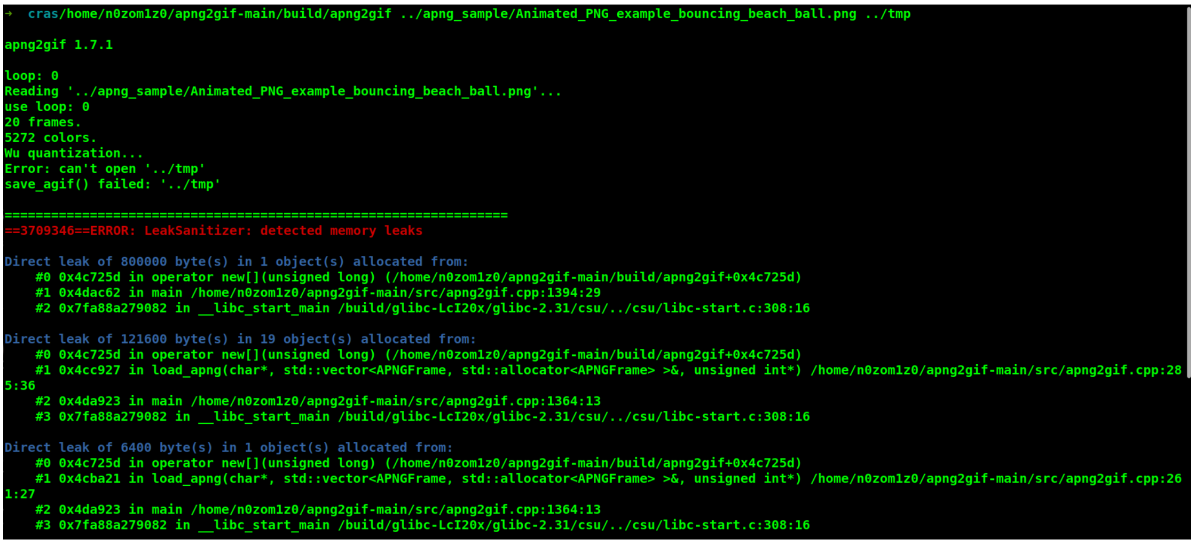
It seems that when it comes to error in saving `pAGIF` into `szOut`, the commited memory `pAGIF` will not be deleted properly.



```
int main(int argc, char** argv)
  {
    unsigned int w = frames[0].w;
    unsigned int h = frames[0].h;
    unsigned int num_frames = frames.size();
    printf("%d frame%s.\n", num_frames, (num_frames==1) ? "" : "s");

    unsigned char * pAGIF = new unsigned char[w * h * num_frames * 4];

    apng_to_agif(frames, pAGIF);

    if (save_agif(szOut, frames, pAGIF, num_loops) != 0)
    {
      printf("save_agif() failed: '%s'\n", szOut);
      return 1;
    }

    for (size_t n=0; n<frames.size(); n++)
    {
      delete[] frames[n].rows;
      delete[] frames[n].p;
    }
    frames.clear();

    delete[] pAGIF;
  }

  printf("all done\n");

  return 0;
}
```

PoC

```
/home/n0zom1z0/apng2gif-main/build/apng2gif
../apng_sample/Animated_PNG_example_bouncing_beach_ball.png ../tmp
```



```
→  cras/home/n0zom1z0/apng2gif-main/build/apng2gif ../apng_sample/Animated_PNG_example_bouncing_beach_ball.png ../tmp

apng2gif 1.7.1

loop: 0
Reading '../apng_sample/Animated_PNG_example_bouncing_beach_ball.png'...
use loop: 0
20 frames.
5272 colors.
Wu quantization...
Error: can't open '../tmp'
save_agif() failed: '../tmp'

=================================================================
==3709346==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 800000 byte(s) in 1 object(s) allocated from:
    #0 0x4c725d in operator new[](unsigned long) (/home/n0zom1z0/apng2gif-main/build/apng2gif+0x4c725d)
    #1 0x4dac62 in main /home/n0zom1z0/apng2gif-main/src/apng2gif.cpp:1394:29
    #2 0x7fa88a279082 in __libc_start_main /build/glibc-LcI20x/glibc-2.31/csu/../csu/libc-start.c:308:16

Direct leak of 121600 byte(s) in 19 object(s) allocated from:
    #0 0x4c725d in operator new[](unsigned long) (/home/n0zom1z0/apng2gif-main/build/apng2gif+0x4c725d)
    #1 0x4cc927 in load_apng(char*, std::vector<APNGFrame, std::allocator<APNGFrame> >&, unsigned int*) /home/n0zom1z0/apng2gif-main/src/apng2gif.cpp:28
5:36
    #2 0x4da923 in main /home/n0zom1z0/apng2gif-main/src/apng2gif.cpp:1364:13
    #3 0x7fa88a279082 in __libc_start_main /build/glibc-LcI20x/glibc-2.31/csu/../csu/libc-start.c:308:16

Direct leak of 6400 byte(s) in 1 object(s) allocated from:
    #0 0x4c725d in operator new[](unsigned long) (/home/n0zom1z0/apng2gif-main/build/apng2gif+0x4c725d)
    #1 0x4cba21 in load_apng(char*, std::vector<APNGFrame, std::allocator<APNGFrame> >&, unsigned int*) /home/n0zom1z0/apng2gif-main/src/apng2gif.cpp:26
1:27
    #2 0x4da923 in main /home/n0zom1z0/apng2gif-main/src/apng2gif.cpp:1364:13
    #3 0x7fa88a279082 in __libc_start_main /build/glibc-LcI20x/glibc-2.31/csu/../csu/libc-start.c:308:16
```