hzeller / timg Public

Code Issues 20 Pull requests Actions Projects Security ···

New issue Jump to bottom

Detected memory leaks 16 byte(s) leaked in 2 allocation(s) #92

Closed **yangfar** opened this issue on Oct 14 · 3 comments

yangfar commented on Oct 14 • edited

Version

timg v1.4.4
afl-clang
afl-clang++

Description

```
=================================================================
==15159==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 8 byte(s) in 1 object(s) allocated from:
#0 0x485b14 in strdup (/home/hjsz/fuzz_software/timg/build/src/timg+0x485b14)
#1 0x51afb7 in timg::QueryBackgroundColor() /home/hjsz/fuzz_software/timg/src/term-query.cc:177:12
#2 0x4d8802 in main::$_1::operator()() const /home/hjsz/fuzz_software/timg/src/timg.cc:775:43
#3 0x4d8802 in std::_Function_handler<timg::rgba_t (), main::$_1>::_M_invoke(std::_Any_data const&) /usr/bin/../lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/std_function.h:285:9
#4 0x4dd3a3 in std::function<void ()>::operator()() const /usr/bin/../lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/std_function.h:688:14
#5 0x4dd3a3 in timg::ThreadPool::Runner() /home/hjsz/fuzz_software/timg/src/thread-pool.h:76:13
#6 0x7f5c047dcde3 (/lib/x86_64-linux-gnu/libstdc++.so.6+0xd6de3)

Direct leak of 8 byte(s) in 1 object(s) allocated from:
#0 0x4c8edd in operator new(unsigned long) (/home/hjsz/fuzz_software/timg/build/src/timg+0x4c8edd)
#1 0x4f2477 in timg::BufferedWriteSequencer::BufferedWriteSequencer(int, bool, int, bool, int const volatile&) /home/hjsz/fuzz_software/timg/src/buffered-write-sequencer.cc:42:11
#2 0x4d26e2 in main /home/hjsz/fuzz_software/timg/src/timg.cc:826:34
#3 0x7f5c04399082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: 16 byte(s) leaked in 2 allocation(s).
```

Command

./timg some.jpg
./timg -g50x50 some.jpg
When I want to fuzz the software and make it by afl,crashes occur.

Poc

POC.zip

Thanks for your time !

Report of the Information Security Laboratory of Ocean University of China @OUC_ISLOUC @OUC_Blue_Whale

hzeller closed this as completed in `e9667ea` on Oct 14

hzeller commented on Oct 14 • edited ▾ Owner

Can you do your check with latest head ?

yangfar commented on Oct 14 Author

Sure，I will reply as soon as possible.

LeSuisse added a commit to LeSuisse/nixpkgs that referenced this issue 21 days ago

`timg: apply patch for CVE-2022-43151` … `bbb8622`

LeSuisse mentioned this issue 21 days ago

timg: apply patch for CVE-2022-43151 NixOS/nixpkgs#199726

Merged

13 tasks

github-actions bot pushed a commit to NixOS/nixpkgs that referenced this issue 21 days ago

`timg: apply patch for CVE-2022-43151` … ✓ `8619ea3`

vivlim pushed a commit to vivlim/nixpkgs that referenced this issue 19 days ago

`timg: apply patch for CVE-2022-43151` … `404faf5`

hzeller commented 12 days ago Owner

Fix included in release `v1.4.5`

Mic92 pushed a commit to Mic92/nixpkgs that referenced this issue 8 days ago

`timg: apply patch for CVE-2022-43151` … `c6aff38`

prtzl pushed a commit to prtzl/nixpkgs that referenced this issue 5 days ago

`timg: apply patch for CVE-2022-43151` … `f08492d`

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants