Closed Issue created 7 months ago by **Loeng**

GIMP 2.10.30 crashed when allocate large memory

Environment/Versions

- GIMP version:2.10.30 and 2.99.10
- Package: https://download.gimp.org/pub/gimp/v2.10/gimp-2.10.30.tar.bz2

https://download.gimp.org/pub/gimp/v2.99/gimp-2.99.10.tar.bz2

- Operating System: Ubuntu 21.10

Description of the bug

Through a crafted XCF file, the program will allocate for a huge amount of memory, resulting in insufficient memory or program crash. This ASAN report:

==286446==ERROR: AddressSanitizer: allocator is out of memory trying to allocate 0xab9e16000 bytes

```
#0 0x7f0dfc859a37 in __interceptor_calloc ../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:15

#1 0x7f0dfbbd45b0 in g_malloc0 (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x5e5b0)

#2 0x562b862c20a7 in xcf_load_old_paths /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/xcf/xcf-load.

#3 0x562b862b8ca6 in xcf_load_image_props /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/xcf/xcf-loa

#4 0x562b862b4586 in xcf_load_image /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/xcf/xcf-load.c:25

#5 0x562b862b267e in xcf_load_stream /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/xcf/xcf.c:315

#6 0x562b862b3630 in xcf_load_invoker /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/xcf/xcf.c:445

#7 0x562b863c33ac in gimp_procedure_real_execute /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/pdb/

#8 0x562b863eda5d in gimp_plug_in_procedure_execute /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/p

#9 0x562b863c50d0 in gimp_procedure_execute /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/pdb/gimpp

#10 0x562b863b6325 in gimp_pdb_execute_procedure_by_name_args /home/leung/fuzzing_gimp/test/gimp-2.1

#11 0x562b863b77d0 in gimp_pdb_execute_procedure_by_name /home/leung/fuzzing_gimp/test/gimp-2.10.30/

#12 0x562b866a9998 in file_open_image /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/file/file-open.

#13 0x562b866ab9db in file_open_with_proc_and_display /home/leung/fuzzing_gimp/test/gimp-2.10.30/app

#14 0x562b866ab2f2 in file_open_with_display /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/file/fil

#15 0x562b866acc28 in file_open_from_command_line /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/fil

#16 0x562b862aa21a in app_run /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/app.c:417

#17 0x562b862b0bc1 in main /home/leung/fuzzing_gimp/test/gimp-2.10.30/app/main.c:656

#18 0x7f0dfb7d7fcf in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
```

==286446==HINT: if you don't care about these errors you may set allocator_may_return_null=1

SUMMARY: AddressSanitizer: out-of-memory ../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:154 in __interceptor_calloc

==286446==ABORTING

The reason: Missing size check for num_points

```
//gimp-2.10.30/app/xcf/xcf-load.c:2755
xcf_read_int32  (info, &num_points, 1);
```

```
....
//gimp-2.10.30/app/xcf/xcf-load.c:2780
if (num_points == 0)
    {
      g_free (name);
      return FALSE;
    }

  points = g_new0 (GimpVectorsCompatPoint, num_points);
```

Thread 1 "gimp-console-2." hit Breakpoint 1, xcf_load_old_path (image=0x555555a16860, info=0x7fffffffda90) at xcf-load.c:2787 2787 points = g_new0 (GimpVectorsCompatPoint, num_points); (gdb) p/x num_points $1 = 0x72696400 (gdb) n

(gimp-console-2.10:287033): GLib-ERROR **: 19:00:44.570: ../../../glib/gmem.c:142: failed to allocate 46068228096 bytes

Reproduction

Is the bug reproducible? Always Reproduction steps:

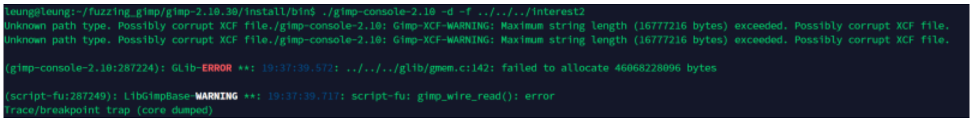
1. download the crafted XCF file:[https://github.com/leung-yao/poc/raw/main/poc%20for%20gimp poc for gimp](https://github.com/leung-yao/poc/raw/main/poc%20for%20gimp)
2. compiler gimp 2.10.30 with console, my compiler command：

```
PKG_CONFIG_PATH=$PKG_CONFIG_PATH:$HOME/fuzzing_gimp/gegl-0.4.36/  ./configure --disable-gtktest --di
make
make install
```

3. use gimp console
4. ./gimp-console-2.10 -d -f [poc file]

Expected result:normal

Actual result:crash



```
leung@leung:~/fuzzing_gimp/gimp-2.10.30/install/bin$ ./gimp-console-2.10 -d -f ../../../interest2
Unknown path type. Possibly corrupt XCF file./gimp-console-2.10: Gimp-XCF-WARNING: Maximum string length (16777216 bytes) exceeded. Possibly corrupt XCF file.
Unknown path type. Possibly corrupt XCF file./gimp-console-2.10: Gimp-XCF-WARNING: Maximum string length (16777216 bytes) exceeded. Possibly corrupt XCF file.

(gimp-console-2.10:287224): GLib-ERROR **: 19:37:39.572: ../../../glib/gmem.c:142: failed to allocate 46068228096 bytes

(script-fu:287249): LibGimpBase-WARNING **: 19:37:39.717: script-fu: gimp_wire_read(): error
Trace/breakpoint trap (core dumped)
```

Additional information

gimp2.99.10 also will crashed by this xcf file.

Drag your designs here or click to upload.

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 1

CVE-2022-30067 patch?

#8222

Activity

Loeng @gdmzyzl · 7 months ago Author

please reply me,thx.

Jacob Boerema @Wormnest · 6 months ago Developer

@gdmzyzl We are all volunteers here. Sometimes it takes time to look at all issues.

That said, I can reproduce the problem, thanks for reporting. I will work on fixing it.

Jacob Boerema changed milestone to %2.10.32 6 months ago

Jacob Boerema added 1. Crash 2.10.30 2.99.10 labels 6 months ago

Jacob Boerema closed via commit 4f99f1fc 6 months ago

Jacob Boerema mentioned in commit 8cd6d052 6 months ago

Jacob Boerema @Wormnest · 6 months ago Developer

Should be fixed now in both master and the next stable release.

```
app: fix #8120 GIMP 2.10.30 crashed when allocate large memory

GIMP could crash if the information regarding old path properties read
from XCF was incorrect. It did not check if xcf_old_path succeeded and
kept trying to load more paths even if the last one failed to load.

Instead we now stop loading paths as soon as that function fails.
In case we have a failure here we also try to skip to the next property
based on the size of the path property, in hopes that the only problem
was this property.
```

Jacob Boerema mentioned in commit 4f99f1fc 6 months ago

Loeng @gdmzyzl · 6 months ago Author

The vulnerability was found by Ziliang Yao, Haoshan Xu, Anlin Yu, Hui Lu, Zhihong Tian from Guangzhou University.

Nikc marked #8222 (closed) as a duplicate of this issue 5 months ago

Nikc marked this issue as related to #8222 (closed) 5 months ago

Nikc mentioned in issue #8222 (closed) 5 months ago

Jacob Boerema @Wormnest · 5 months ago Developer

I guess they requested a CVE for this issue, without telling us. @gdmzyzl Next time please tell us, you intend to open a CVE and make the issue confidential. That is standard practice for these kind of issues.

CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30067

Jehan mentioned in issue Infrastructure/gimp-web#262 (closed) 5 months ago

Please register or sign in to reply