

New issue

[Jump to bottom](#)

## Read out of bound in TGA files #697

Closed

meweez opened this issue on Apr 30, 2021 · 13 comments

meweez commented on Apr 30, 2021

Contributor

hello,

[this issue](#) is showing a read out of bound for a corrupted TGA [test.txt](#) which is patched by adding some checks for `gdGetBuf` .

although the patch prevents occurring this vulnerability I saw that this function ( `gdGetBuf` ) is used in `read_header_tga` too which there is no check for its return value again.

I changed the header of the file which was used for the previous [CVE-2016-6132](#). In fact, I changed the first byte to `ff` which is assigned to `tga->identsize` .

[file\(it is a tga, not a really a txt\)](#)

```
...
tga->identsize = header[0];
...
gdGetBuf(tga->ident, tga->identsize, ctx);
...
```

when I run the test with this input file ASAN shows this:

```
AddressSanitizer: DEADLY SIGNAL
=====
==12378==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f685ae4a7a0 bp 0x7fff6bb8b740 sp 0x7fff6bb8b720 T0)
==12378==The signal is caused by a READ memory access.
==12378==Hint: address points to the zero page.
#0 0x7f685ae4a79f in gdImageDestroy /tmp/libgd/src/gd.c:390
#1 0x55c05b670432 in main /tmp/libgd/tests/tga/bug00084.c:11
#2 0x7f685aa3709a in __libc_start_main ../csu/libc-start.c:308
#3 0x55c05b670339 in _start (/tmp/libgd/build/Bin/test_tga_bug00084+0x2339)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /tmp/libgd/src/gd.c:390 in gdImageDestroy
==12378==ABORTING
```

Is it showing another vulnerability?

meweez commented on May 31, 2021

Contributor

Author

any comment?

cmb69 commented on May 31, 2021

Contributor

There might be a bug there, but who needs to read TGAs in ... checks calendar ... 2021?

pierrejoye commented on Jul 2, 2021

Contributor

@me22bee could you upload the full test case or do you use only bug00084.c?

meweez commented on Jul 2, 2021

Contributor

Author

do you use only bug00084.c?

yes.

pierrejoye commented on Jul 19, 2021

Contributor

@me22bee could you attach the patched test file? Should be an easy fix. TGA is still used, indeed not for web but our targets go further than web devs :)

 meweez mentioned this issue on Jul 19, 2021**fix read out-of-bounds in reading tga header file #711**

Merged

meweez commented on Jul 19, 2021 • edited

Contributor

Author

could you attach the patched test file?


I have sent a pull request and also attached the patch file here.

[0001-fix-read-out-of-bands-in-reading-tga-header-file.patch.txt](#)

pierrejoye commented on Jul 19, 2021

Contributor

Thank you @me22bee :)

 pierrejoye closed this as completed on Jul 19, 2021

meweez commented on Jul 19, 2021

Contributor Author

your welcome,  
Don't you assign a CVE number to it?  
@pierrejoye

 pierrejoye commented on Jul 19, 2021

Contributor

let me check with the \*\*\*@\*\*\*.\*\*\*, we have access ;)  
...



meweez commented on Jul 25, 2021 • edited

Contributor Author

| let me check with  
any update?  
@pierrejoye

carnil commented on Aug 5, 2021

[CVE-2021-38115](#) seems to have been assigned for this issue.



mshah-aiondigital commented on Sep 2, 2021

Will a release be provided with this security fix?

 meweez mentioned this issue on Sep 5, 2021

**gdPutBuf return value check #750**



oerdnj commented on Jul 6

Contributor

| Will a release be provided with this security fix?  
FTR the fix has been released in 2.3.3

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

6 participants

