GraphicsMagick Bugs

Swiss army knife of image processing

Brought to you by: bfriesen

#664 [bug]Heap buffer overflow when parsing MIFF

Milestone: v1.0 (example)	**Status:** closed-fixed	**Owner:** Bob Friesenhahn	**Labels:** bug (4) vulnerability (1)
Priority: 5			
Updated: 2022-03-26	**Created:** 2022-03-24	**Creator:** patchkey	**Private:** No

Version: GraphicsMagick 1.4 snapshot-20220322

```
==3682383==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61700000032e at pc 0x0
WRITE of size 6146 at 0x61700000032e thread T0
    #0 0x3c4a8d in fread (/home/user/fuzzing_asanGrap/bin/gm+0x3c4a8d)
    #1 0x52bb62 in ReadBlob /home/user/test/GraphicsMagick-1.4.020220322/magick/blob.c:3228
    #2 0xc1f532 in ReadMIFFImage /home/user/test/GraphicsMagick-1.4.020220322/coders/miff.c
    #3 0x5b092e in ReadImage /home/user/test/GraphicsMagick-1.4.020220322/magick/constitute
    #4 0x5af68b in PingImage /home/user/test/GraphicsMagick-1.4.020220322/magick/constitute
    #5 0x4b4ef9 in IdentifyImageCommand /home/user/test/GraphicsMagick-1.4.020220322/magick/
    #6 0x4ed162 in MagickCommand /home/user/test/GraphicsMagick-1.4.020220322/magick/command
    #7 0x514b89 in GMCommandSingle /home/user/test/GraphicsMagick-1.4.020220322/magick/comma
    #8 0x51350f in GMCommand /home/user/test/GraphicsMagick-1.4.020220322/magick/command.c:1
    #9 0x7ffff73030b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/csu/../csu/libc-st
    #10 0x3ab2fd in _start (/home/user/fuzzing_asanGrap/bin/gm+0x3ab2fd)

0x61700000032e is located 0 bytes to the right of 686-byte region [0x617000000080,0x61700000
allocated by thread T0 here:
    #0 0x427da3 in realloc (/home/user/fuzzing_asanGrap/bin/gm+0x427da3)
    #1 0x65f1dc in _MagickReallocateResourceLimitedMemory /home/user/test/GraphicsMagick-1.4

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/user/fuzzing_asanGrap/bin/gm+0x3c4a8d
Shadow bytes around the buggy address:
  0x0c2e7fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff8020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff8030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2e7fff8060: 00 00 00 00 00[06]fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
```

command: `./gm identify example.miff`

example.miff link:

https://drive.google.com/file/d/1kW2wd0S_oCffl23eiRjwErAAMsb3muc-/view?usp=sharing

1 Attachments

example.miff

Discussion

patchkey - *2022-03-24*

supplement：
OS： ubuntu20.04

Bob Friesenhahn - *2022-03-24*

- **assigned_to**: Bob Friesenhahn

Bob Friesenhahn - *2022-03-24*

I am able to reproduce this strange issue.

Bob Friesenhahn - *2022-03-25*

I see the cause of the problem. Only builds with bzip support are impacted.

Bob Friesenhahn - *2022-03-26*

- **status**: open --> closed-fixed

Bob Friesenhahn - *2022-03-26*

This issue is addressed by Mercurial changeset 16689:94f4bcf448ad and the latest development snapshot (GraphicsMagick-1.4.020220326.tar.xz).

Thank you for reporting this issue!

Log in to post a comment.

Site Status