



GraphicsMagick Bugs

Swiss army knife of image processing Brought to you by: bfriesen

#664 [bug] Heap buffer overflow when parsing MIFF

3

Milestone: v1.0 (example)

Status: closed-fixed

Owner: Bob Friesenhahn

Labels: <u>bug (4)</u> <u>vulnerability (1)</u>

Priority: 5

Updated: 2022-03-26

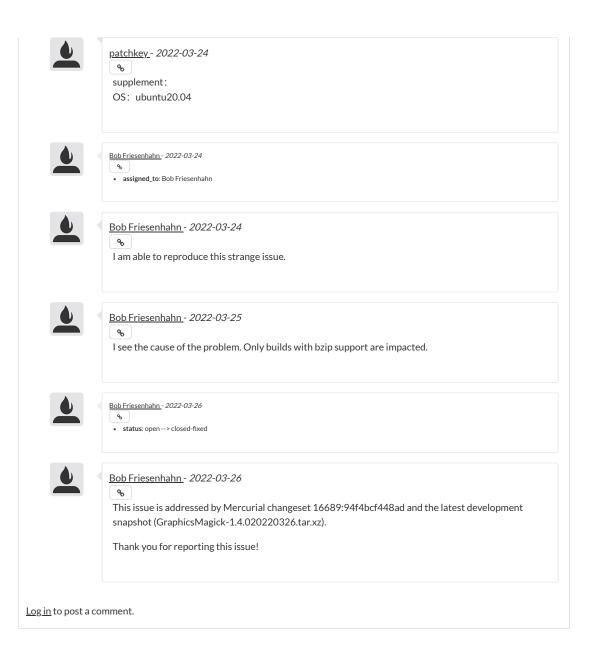
Created: 2022-03-24

Creator: patchkey

Private: No

Version: GraphicsMagick 1.4 snapshot-20220322

```
==3682383==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61700000032e at pc 0x6
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 PinqImage /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/comm.
   #8 0x51350f in GMCommand /home/user/test/GraphicsMagick-1.4.020220322/magick/command.c:
   #9 0x7ffff73030b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/csu/../csu/libc-s
   #10 0x3ab2fd in _start (/home/user/fuzzing_asanGrap/bin/gm+0x3ab2fd)
0x61700000032e is located 0 bytes to the right of 686-byte region [0x61700000080,0x61700000
allocated by thread TO here:
   #0 0x427da3 in realloc (/home/user/fuzzing asanGrap/bin/gm+0x427da3)
   #1 0x65f1dc in MagickReallocateResourceLimitedMemory /home/user/test/GraphicsMagick-1.
SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/user/fuzzing_asanGrap/bin/gm+0x3c4a8
Shadow bytes around the buggy address:
  =>0x0c2e7fff8060: 00 00 00 00 00[06]fa fa fa fa fa fa fa fa fa fa
  Shadow byte legend (one shadow byte represents 8 application bytes):
                   0.0
  Addressable:
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone: fa
  Freed heap region:
                    fd
  Stack left redzone:
                    f1
  Stack mid redzone:
  Stack right redzone:
                    f3
  Stack after return:
                    f5
  Stack use after scope: f8
  Global redzone:
                     f9
  Global init order:
  Poisoned by user:
  Container overflow:
                     fc
                     ac
 Array cookie:
 Intra object redzone: bb
  ASan internal:
                     fe
  Left alloca redzone:
  Right alloca redzone:
                     cb
4
command: ./gm identify example.miff
example.miff link:
https://drive.google.com/file/d/1kW2wd0S oCffl23eiRjwErAAMsb3muc-/view?usp=sharing
1 Attachments
example.miff
Discussion
```



SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

Team

SourceForge Headquarters

225 Broadway Suite 1600

San Diego, CA 92101

+1 (858) 454-5900

Resources

Support

Site Documentation



 $\hbox{@\,}2022\,\hbox{Slashdot}\,\hbox{Media.}\,\hbox{All}\,\hbox{Rights}\,\hbox{Reserved.}$

Terms

Privacy

Opt Out

Advertise