

New issue

[Jump to bottom](#)

stack-buffer-overflow at /coders/xpm.c:232 in ReadXPMImage #1895



peanuts62 opened this issue on Apr 14, 2020 · 9 comments

peanuts62 commented on Apr 14, 2020

Prerequisites

- ☒ I have written a descriptive issue title
- ☒ I have verified that I am using the latest version of ImageMagick
- ☒ I have searched [open](#) and [closed](#) issues to ensure it has not already been reported

Description

There's a stack buffer overflow at /coders/xpm.c:232 in ReadXPMImage

[poc](#)

Steps to Reproduce

run_cmd

```
magick convert ./afl-Ima/sync_dir/fuzzer2/crashes/id\:000000\,sig\:06\,src\:009314\,op\:havoc\,rep\:16 t.png
```

Here's ASAN log.

```
==22728==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7fff34696d60 at pc 0x7fb49cb4a648 bp 0x7fff34694c80 sp 0x7fff34694c70
READ of size 1 at 0x7fff34696d60 thread T0
#0 0x7fb49cb4a647 in ParseXPMColor /home/afl-Ima/ImageMagick/coders/xpm.c:232
#1 0x7fb49cb3d610 in ReadXPMImage /home/afl-Ima/ImageMagick/coders/xpm.c:425
#2 0x7fb49beeb03c9 in ReadImage /home/afl-Ima/ImageMagick/MagickCore/constitute.c:553
#3 0x7fb49beeb4d46 in ReadImages /home/afl-Ima/ImageMagick/MagickCore/constitute.c:941
#4 0x7fb49b594ed2 in ConvertImageCommand /home/afl-Ima/ImageMagick/MagickWand/convert.c:606
#5 0x7fb49b6cd098 in MagickCommandGenesis /home/afl-Ima/ImageMagick/MagickWand/mogrify.c:186
#6 0x55be14ba8ec0 in MagickMain utilities/magick.c:149
#7 0x55be14ba9146 in main utilities/magick.c:180
#8 0x7fb49ae56b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#9 0x55be14ba8939 in _start (/home/ImageMagick/utilities/.libs/magick+0x1939)
```

Address 0x7fff34696d60 is located in stack of thread T0 at offset 8352 in frame
#0 0x7fb49cb3ade7 in ReadXPMImage /home/afl-Ima/ImageMagick/coders/xpm.c:250

```
This frame has 7 object(s):
[32, 4128] 'key:251'
[4256, 8352] 'target:251' <== Memory access at offset 8352 overflows this variable
[8480, 8488] 'colors:286'
[8512, 8520] 'columns:286'
[8544, 8552] 'rows:286'
[8576, 8584] 'width:286'
[8608, 12704] 'symbolic:398'
```

HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swapcontext
(longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/afl-Ima/ImageMagick/coders/xpm.c:232 in ParseXPMColor
Shadow bytes around the buggy address:

```
0x1000668cad50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1000668cad60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1000668cad70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1000668cad80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1000668cad90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x1000668cada0: 00 00 00 00 00 00 00 00 00 00 00 00 00[f2]f2 f2 f2
0x1000668cadb0: f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2
0x1000668cadc0: 00 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 00 00 00
0x1000668cadd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1000668cade0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1000668cadf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

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
==22728==ABORTING
```

System Configuration

- ImageMagick version:
Version: ImageMagick 7.0.10-7 Q16 x86_64 2020-04-10 <https://imagemagick.org>
Copyright: © 1999-2020 ImageMagick Studio LLC
License: <https://imagemagick.org/script/license.php>

- Features: Cipher DPC HDRI OpenMP(3.1)
Delegates (built-in): zlib
- Environment (Operating system, version and so on):
Description: Ubuntu 18.04.1 LTS
 - Additional information:

```
root@VM-0-15-ubuntu:/home# ./ImageMagick/utilities/.libs/magick identify -list policy
```

```
Path: /usr/local/etc/ImageMagick-7/policy.xml
```

```
Policy: Resource
name: list-length
value: 128
```

```
Policy: Resource
name: file
value: 768
```

```
Policy: Resource
name: disk
value: 16EiB
```

```
Policy: Resource
name: map
value: 4GiB
```

```
Policy: Resource
name: area
value: 100MP
```

```
Policy: Resource
name: height
value: 10KP
```

```
Policy: Resource
name: width
value: 10KP
```


```
Path: [built-in]
Policy: Undefined
rights: None
```

edit by peanuts
, and Is it possible to request a cve id?

 **urban-warrior** pushed a commit to ImageMagick/ImageMagick6 that referenced this issue on Apr 14, 2020

<https://github.com/ImageMagick/ImageMagick/issues/1895>

2653866

 **urban-warrior** pushed a commit that referenced this issue on Apr 14, 2020

<https://github.com/ImageMagick/ImageMagick/issues/1895>

5462fd4

urban-warrior commented on Apr 14, 2020

Contributor

ASAN does not return a stack issue for us. We're using ASAN with gcc 9.3.1. However, valgrind returned a unconditional jump. We added a patch.

peanuts62 commented on Apr 14, 2020

Author

Thank you.

peanuts62 commented on Apr 14, 2020

Author

Can I request a CVE ID?

urban-warrior commented on Apr 14, 2020

Contributor

Not sure what you're asking. Anyone can request a CVE ID. We rely on the user community to post CVE's due to our small development team and lack of time to address all issues associated with ImageMagick.

peanuts62 commented on Apr 14, 2020

Author

thank you ,
I hope this question can be assigned CVE

thesamesam commented on Apr 22, 2020

Contributor

@minghangshen You need to request a CVE from an authority like MITRE: https://cve.mitre.org/cve/request_id.html. Please let us know if you do.

peanuts62 commented on Apr 22, 2020

Author

@thesamesam I have submitted the form in https://cve.mitre.org/cve/request_id.html , and I have received an automatic response, but no response since

peanuts62 commented on Apr 22, 2020

Author

@thesamesam Auto-reply title : CVE Request 878017 for CVE ID Request

 **netbsd-srcmastr** pushed a commit to NetBSD/pkgsrc that referenced this issue on Apr 24, 2020

 ImageMagick6: Update to 6.9.11.7 ...

07ad2ed

 **netbsd-srcmastr** pushed a commit to NetBSD/pkgsrc that referenced this issue on Apr 28, 2020


ImageMagick: update to 7.0.10.8. ...

9b8a7f2

 **bmwiedemann** added a commit to bmwiedemann/openSUSE that referenced this issue on May 7, 2020


 Update ImageMagick to rev 206 via SR 800017 ...

4f6a933

 **dlemstra** closed this as completed on Jun 9, 2020

carnil commented on Nov 21, 2020

The correct CVE id seems though to be <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-19667>

  **itewqq** mentioned this issue on May 7, 2021

Cannot reproduce poc2 peanuts62/bug_poc#1

 Open

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants

