allocator is out of memory(OOM in pdftoppm)

Post Reply Search this topic… 6 posts • Page **1** of **1**

elvadisas

allocator is out of memory(OOM in pdftoppm)

Thu Apr 28, 2022 6:40 am

Hello,
i had a crash when i did a fuzzing test in xpdf.
Description:
Memory Allocation with Excessive Size Value
run poc:

```
/home/elva/fuzzing_xpdf/install/bin/pdftoppm ./poc /home/elva/fuzzing_xpdf/out
```

asan :

```
Syntax Error (8241): Too few (1) args to 'c' operator
Syntax Error (8252): Too few (4) args to 'c' operator
Syntax Error (8267): Too few (5) args to 'cm' operator
Syntax Error (8274): Unknown operator 'rg69122'
Syntax Error (8274): Unknown operator 'c464.34084'
Syntax Error (8274): Too few (1) args to 'c' operator
Syntax Error (8274): Unknown operator 'T'
Syntax Error (8274): Unknown operator 'T000069127.734.3436812812.3000085.rg'
Syntax Error (8274): Unknown operator 'T'
Syntax Error (8274): Arg #0 to 'J' operator is wrong type (real)
Syntax Error (8277): Too few (2) args to 'c' operator
Syntax Error (8277): Unknown operator 'c46978425992'
Syntax Error (8277): Arg #0 to 'Tf' operator is wrong type (real)
Syntax Error (8277): Unknown operator 'E25992'
Syntax Error (8277): Too few (1) args to 'c' operator
Syntax Error (8277): Arg #0 to 'Tf' operator is wrong type (integer)
Syntax Error (8277): Too few (2) args to 'rg' operator
Syntax Error (8277): Too few (4) args to 'c' operator
Syntax Error (8277): Too few (1) args to 'cm' operator
Syntax Error (8277): Too few (1) args to 'c' operator
Syntax Error (8293): Unknown operator 'q5685700398103000'
Syntax Error (8328): Unknown operator 'T252000'
Syntax Error (8344): Too few (5) args to 'c' operator
Syntax Error (8355): Too few (1) args to 'c' operator
Syntax Error (8367): Unknown operator 'T'
Syntax Error (8397): Too few (1) args to 'c' operator
Syntax Error (8408): Unknown operator 'BT831'
Syntax Error (8439): Unknown operator 'm0'
Syntax Error (8442): Too few (0) args to 'c' operator
Syntax Error (8456): Unknown operator 'cm1184'
```

```
=================================================================
==486377==ERROR: AddressSanitizer: requested allocation size 0x26bfff68a20 (0x26bfff69a20 after adjustments for alignment, red zones etc.) exceeds maximum supported size of 0x10000000000 (thread T0)
#0 0x4ce7cd in malloc (/home/elva/fuzzing_xpdf/install/bin/pdftoppm+0x4ce7cd)
#1 0x7fe487 in gmalloc64(unsigned long) /home/elva/fuzzing_xpdf/xpdf-4.04/goo/gmem.cc:271:13
#2 0x7fe487 in gmallocn64(int, unsigned long) /home/elva/fuzzing_xpdf/xpdf-4.04/goo/gmem.cc:288:10

==486377==HINT: if you don't care about these errors you may set allocator_may_return_null=1
SUMMARY: AddressSanitizer: allocation-size-too-big (/home/elva/fuzzing_xpdf/install/bin/pdftoppm+0x4ce7cd) in malloc
==486377==ABORTING
```

POC is in ATTACHMENT.
Thank you.

ATTACHMENTS

poc.rar
(31 KiB) Downloaded 77 times

derekn

Re: allocator is out of memory(OOM in pdftoppm)

Mon May 02, 2022 9:11 pm

I can't reproduce this problem. Can you double-check that you attached the correct POC PDF file?

Which compiler and version are you using?

Thanks.

elvadisas

Re: allocator is out of memory(OOM in pdftoppm)

Thu May 05, 2022 2:01 am

hello,thank you for your reply:-)
My testing enviorment:
--Tested on Ubuntu 20.04.2 LTS x86_64,AFL++
--gcc version 9.3.0
--xpdf version xpdf 4.04
https://dl.xpdfreader.com/xpdf-4.04.tar.gz

POC is in the ATTACHMENT.
Screenshot is also in the ATTACHMENT.
Pls double-check~~~
Thanks.

ATTACHMENTS

screenshot.rar
(76.09 KiB) Downloaded 64 times

poc.rar
(31 KiB) Downloaded 67 times

derekn

Re: allocator is out of memory(OOM in pdftoppm)

Wed May 11, 2022 10:26 pm

I've tried with gcc 5.5.0 and gcc 11.2.0 (that's what I have on my dev machines), with asan, and I'm still not seeing a crash.

What was your cmake command to configure xpdf before compiling?

elvadisas

Re: allocator is out of memory(OOM in pdftoppm)

Thu May 12, 2022 2:18 am

Hello,derekn

you can reproduced the bug by the following steps:

```
mkdir build_asan
cd build_asan

cmake -DCMAKE_BUILD_TYPE=Debug $HOME/fuzzing_xpdf/xpdf-4.04 -DCMAKE_INSTALL_PREFIX=$HOME/fuzzing_xpdf/install/ -DCMAKE_CXX_COMPILER=afl-clang-fast++

AFL_USE_ASAN=1 make
sudo AFL_USE_ASAN=1 make install

$HOME/fuzzing_xpdf/install/bin/pdftoppm -f 1 $HOME/fuzzing_xpdf/poc $HOME/fuzzing_xpdf/output
```

POC file and more screenshots are in the ATTACHMENTS.

My Testing Enviroments:
--Tested on Ubuntu 20.04.2 LTS x86_64,AFL++
--gcc version 9.3.0
--xpdf version xpdf 4.04
https://dl.xpdfreader.com/xpdf-4.04.tar.gz

you can try it:-)

ATTACHMENTS

screenshot.rar
(76.09 KiB) Downloaded 57 times

poc.rar
(31 KiB) Downloaded 75 times

derekn

Re: allocator is out of memory(OOM in pdftoppm)

Thu May 12, 2022 11:03 pm

Ah, you're building with clang, not gcc. And the AFL stuff apparently sets the options to "-O3".

I was able to reproduce this, and I'll have it fixed in the next release.

Post Reply

6 posts • Page **1** of **1**

Return to “Xpdf open source”

Jump to

Board index

Delete cookies All times are UTC