New issue

Jump to bottom

SEGV (stack overflow) on vfprintf #24

Open **strongcourage** opened this issue on May 27, 2019 · 0 comments

strongcourage commented on May 27, 2019 • edited

Hi,

Our fuzzer found a crash due to a stack overflow bug on the function vfprintf (the latest commit `b671b64` on master - version 0.70).

PoC_so_vfprintf: https://github.com/strongcourage/PoCs/blob/master/pdf2json_b671b64/PoC_so_vfprintf

Valgrind says:

```
valgrind pdf2json PoC_so_vfprintf /dev/null
==8530== Memcheck, a memory error detector
==8530== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
==8530== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
==8530== Command: ./pdf2json PoC_so_vfprintf /dev/null
==8530==
Error: PDF file is damaged - attempting to reconstruct xref table...
Error (13719): Illegal character <8e> in hex string
Error (13778): Illegal character <db> in hex string
Error (13781): Illegal character <94> in hex string
Error (13782): Illegal character <02> in hex string
Error (13783): Illegal character <a2> in hex string
Error: End of file inside array
Error: End of file inside dictionary
Error (193): Illegal character '>'
Error (195): Dictionary key must be a name object
Error (203): Dictionary key must be a name object
Error (229): Dictionary key must be a name object
Error (232): Dictionary key must be a name object
Error (491): Illegal character <01> in hex string
Error (496): Illegal character <6e> in hex string
Error (498): Illegal character <6f> in hex string
Error (500): Illegal character <6a> in hex string
Error (506): Illegal character <6f> in hex string
Error (508): Illegal character <6a> in hex string
Error (510): Illegal character <3c> in hex string
Error (511): Illegal character <3c> in hex string
Error (513): Illegal character <2f> in hex string
...
Error (8023): Dictionary key must be a name object
==8530== Stack overflow in thread #1: can't grow stack to 0xffe801000
==8530==
==8530== Process terminating with default action of signal 11 (SIGSEGV)
==8530==  Access not within mapped region at address 0xFFE801FF8
==8530== Stack overflow in thread #1: can't grow stack to 0xffe801000
==8530==    at 0x5756642: _IO_default_xsputn (genops.c:422)
==8530==  If you believe this happened as a result of a stack
==8530==  overflow in your program's main thread (unlikely but
==8530==  possible), you can try to increase the size of the
==8530==  main thread stack using the --main-stacksize= flag.
==8530==  The main thread stack size used in this run was 8388608.
==8530== Stack overflow in thread #1: can't grow stack to 0xffe801000
==8530==
==8530== Process terminating with default action of signal 11 (SIGSEGV)
==8530==  Access not within mapped region at address 0xFFE801FF0
==8530== Stack overflow in thread #1: can't grow stack to 0xffe801000
==8530==    at 0x4A28680: _vgnU_freeres (in /usr/lib/valgrind/vgpreload_core-amd64-linux.so)
==8530==  If you believe this happened as a result of a stack
==8530==  overflow in your program's main thread (unlikely but
==8530==  possible), you can try to increase the size of the
==8530==  main thread stack using the --main-stacksize= flag.
==8530==  The main thread stack size used in this run was 8388608.
==8530==
==8530== HEAP SUMMARY:
==8530==     in use at exit: 15,497,401 bytes in 256,831 blocks
==8530==   total heap usage: 435,600 allocs, 178,769 frees, 16,602,462 bytes allocated
==8530==
==8530== LEAK SUMMARY:
==8530==    definitely lost: 0 bytes in 0 blocks
==8530==    indirectly lost: 0 bytes in 0 blocks
==8530==      possibly lost: 0 bytes in 0 blocks
==8530==    still reachable: 15,497,401 bytes in 256,831 blocks
==8530==         suppressed: 0 bytes in 0 blocks
==8530== Rerun with --leak-check=full to see details of leaked memory
==8530==
==8530== For counts of detected and suppressed errors, rerun with: -v
==8530== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
Segmentation fault
```

Thanks,
Manh Dung

strongcourage changed the title ~~Segmentation fault (stack overflow) on vfprintf~~ **SEGV (stack overflow) on vfprintf** on May 29, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant