💣 PSPP - Bugs: bug #62977, heap-buffer-overflow in...

Group		Main	Homepage	Download	Docs	Mailing lists	Source code	Bugs
		Patches	News					

bug #62977: heap-buffer-overflow in read_bytes_internal, different from CVE-2018-20230

Submitter:	None		**Submit Changes and Browse Items**	
Submitted:	Mon 29 Aug 2022 12:30:22 PM UTC		Submit Changes and Return to this Item	

Category:	None		*Severity:*	5 - Average
Status:	Fixed		*Assigned to:*	None
Open/Closed:	Closed		*Release:*	None
Effort:	0.00			

* Mandatory Fields

Add a New Comment (🖉Rich Markup) [Preview]

Comment Type & Canned Response:

None ⌄   None ⌄

Mon 05 Sep 2022 05:11:09 PM UTC, comment #1: | Quote |

Ben Pfaff
<blp>

I fixed it, by preventing the program from being installed:
https://git.savannah.gnu.org/cgit/pspp.git/commit/?
id=8596d6eb21e40ffaf9321d1cb779333de3126b50. Maybe people will fuzz
things that are worthwhile now rather than a program that no one uses.

*Mon 29 Aug 2022 12:30:22 PM UTC, **original submission:*** | Quote |

Anonymous

```
## short summary

Hello, I was testing my fuzzer and find a heap buffer overflow in
read_bytes_internal, pspp-1.6.2, which is different from  CVE-2018-20230.
(The poc of CVE-2018-20230 cannot be reproduced in this version)

## Environment
Ubuntu 21.10
gcc 11.2.0
pspp-1.6.2

## step to reproduce
./configure --disable-shared --without-gui && make -j$(nproc)

./pspp-dump-sav $POC

## ASan output

=================================================================
==3455132==ERROR: AddressSanitizer: heap-buffer-overflow on address
0x602000000f71 at pc 0x000000499f5e bp 0x7fff77164110 sp 0x7fff771638d8
WRITE of size 5 at 0x602000000f71 thread T0
    #0 0x499f5d in fread /home/kdsj/workspace/llvm-project/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:1029:16
    #1 0x41fc97 in read_bytes_internal
(/home/kdsj/workspace/fuzz/libpspp/pspp-dump-sav/pspp-dump-sav+0x41fc97)
    #2 0x41fb79 in read_bytes (/home/kdsj/workspace/fuzz/libpspp/pspp-
dump-sav/pspp-dump-sav+0x41fb79)
    #3 0x42621b in read_string (/home/kdsj/workspace/fuzz/libpspp/pspp-
dump-sav/pspp-dump-sav+0x42621b)
    #4 0x4237ce in read_character_encoding
(/home/kdsj/workspace/fuzz/libpspp/pspp-dump-sav/pspp-dump-sav+0x4237ce)
    #5 0x41d7b9 in read_extension_record
(/home/kdsj/workspace/fuzz/libpspp/pspp-dump-sav/pspp-dump-sav+0x41d7b9)
    #6 0x417ac0 in main (/home/kdsj/workspace/fuzz/libpspp/pspp-dump-
sav/pspp-dump-sav+0x417ac0)
    #7 0x7f8cc1e41fcf in __libc_start_call_main
csu/../sysdeps/nptl/libc_start_call_main.h:58:16
    #8 0x7f8cc1e4207c in __libc_start_main csu/../csu/libc-start.c:409:3
    #9 0x407444 in _start (/home/kdsj/workspace/fuzz/libpspp/pspp-dump-
sav/pspp-dump-sav+0x407444)

0x602000000f71 is located 0 bytes to the right of 1-byte region
[0x602000000f70,0x602000000f71)
allocated by thread T0 here:
    #0 0x4fd792 in calloc /home/kdsj/workspace/llvm-project/compiler-
rt/lib/asan/asan_malloc_linux.cpp:154:3
    #1 0x42fabb in xcalloc (/home/kdsj/workspace/fuzz/libpspp/pspp-dump-
sav/pspp-dump-sav+0x42fabb)
    #2 0x4237b5 in read_character_encoding
(/home/kdsj/workspace/fuzz/libpspp/pspp-dump-sav/pspp-dump-sav+0x4237b5)
    #3 0x41d7b9 in read_extension_record
(/home/kdsj/workspace/fuzz/libpspp/pspp-dump-sav/pspp-dump-sav+0x41d7b9)
    #4 0x417ac0 in main (/home/kdsj/workspace/fuzz/libpspp/pspp-dump-
sav/pspp-dump-sav+0x417ac0)
    #5 0x7f8cc1e41fcf in __libc_start_call_main
csu/../sysdeps/nptl/libc_start_call_main.h:58:16

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/kdsj/workspace/llvm-project/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:1029:16
in fread
Shadow bytes around the buggy address:
  0x0c047fff8190: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 fa
```

```
   0x0c047fff81a0: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fa
   0x0c047fff81b0: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fa
   0x0c047fff81c0: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fa
   0x0c047fff81d0: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fa
=>0x0c047fff81e0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa[01]fa
   0x0c047fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c047fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c047fff8210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c047fff8220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c047fff8230: 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
   Shadow gap:              cc
==3455132==ABORTING

## Credit
Han Zheng(NCNIPC of China, Hexhive)
```

(Note: upload size limit is set to 16384 kB, after insertion of the required escape characters.)

Attach Files:

| Choose File | No file chosen | | Choose File | No file chosen |
| Choose File | No file chosen | | Choose File | No file chosen |

Comment:

| |

Attached Files

file #53626: poc0.zip added by kdsj (653B - application/x-zip-compressed - poc)

Depends on the following items: None found

Items that depend on this one: None found

Carbon-Copy List

-email is unavailable- added by blp (Posted a comment)

There are 0 votes so far. Votes easily highlight which items people would like to see resolved in priority, independently of the priority of the item set by tracker managers.

Only logged-in users can vote.

Please enter the title of George Orwell's famous dystopian book (it's a date):

| Submit Changes and Browse Items | Submit Changes and Return to this Item |

Follow 3 latest changes.

Date	Changed by	Updated Field	Previous Value	=>	Replaced by
2022-09-05	blp	Status	None	➡	Fixed
		Open/Closed	Open	➡	Closed
2022-08-29	kdsj	Attached File	-	➡	Added poc0.zip, #53626