

The future of sharing is up to you! Join the FSF by Dec 31 to defend your freedom to share.

[READ MORE](#)

52

455 Members



PSPP - Bugs: bug #63000, heap-buffer-overflow in read_string

Not Logged in

[Login](#)

[New User](#)


This Page

[Language](#)

[Clean Reload](#)

[Printer Version](#)

Search

in [Projects](#) 

Hosted Projects

[Hosting requirements](#)

[Register New Project](#)

[Full List](#)

[Contributors Wanted](#)

[Statistics](#)

Site Help

[User Docs: FAQ](#)

[User Docs: In Depth Guide](#)

[Get Support](#)

[Contact Savannah](#)

GNU Project

[Help GNU](#)

[All GNU Packages](#)

[Dev Resources](#)

[License List](#)

[GNU Mirrors](#)

 **FREE SOFTWARE**
FOUNDATION
Help us protect your
freedom and the
rights of computer
users everywhere by
becoming a member

Group [Main](#) [Homepage](#) [Download](#) [Docs](#) [Mailing lists](#) [Source code](#)
[Bugs](#) [Patches](#) [News](#)

bug #63000: heap-buffer-overflow in read_string

Submitter: [han zheng <kdsj>](#)

[Submit Changes and Browse Items](#)

Submitted: Fri 02 Sep 2022 07:22:22 AM 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](#))

**Free Software
Foundation**

Coming Events
Free Software Directory
Cryptographic software
legal notice
Copyright infringement
notification

Related Forges

Savannah Non-GNU
Puszcza

Mon 19 Sep 2022 05:41:00 PM UTC, comment #1: **Quote**

I fixed it, by preventing the program from being installed:
<https://git.savannah.gnu.org/cgit/pspp.git/commit/?id=8596d6eb21e40ffaf9321d1cb779333de3126b50>.

Ben
Pfaff
<blp>

**Fri 02 Sep 2022 07:22:22 AM UTC, original submission:** **Quote**

```
## short summary
Hello, I was testing my fuzzer and find a heap buffer overflow in
read_string, pspp-1.6.2

## 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
=====
==2607491==ERROR: AddressSanitizer: heap-buffer-overflow on
address 0x602000000111 at pc 0x0000004d6a35 bp 0x7fffc66178b0 sp
0x7fffc66178a8
WRITE of size 1 at 0x602000000111 thread T0
    #0 0x4d6a34 in read_string
/home/kdsj/workspace/fuzz/verify/pspp-1.6.2/utilities/pspp-dump-
sav.c:1661:20
    #1 0x4d6a34 in read_character_encoding
/home/kdsj/workspace/fuzz/verify/pspp-1.6.2/utilities/pspp-dump-
sav.c:1020:3
    #2 0x4d6a34 in read_extension_record
/home/kdsj/workspace/fuzz/verify/pspp-1.6.2/utilities/pspp-dump-
sav.c:649:7
    #3 0x4d6a34 in main /home/kdsj/workspace/fuzz/verify/pspp-
1.6.2/utilities/pspp-dump-sav.c:219:15
    #4 0x7flbaa451fcf in __libc_start_call_main
csu/../sysdeps/nptl/libc_start_call_main.h:58:16
    #5 0x7flbaa45207c in __libc_start_main csu/../csu/libc-
start.c:409:3
    #6 0x41f384 in _start (/home/kdsj/workspace/fuzz/verify/pspp-
1.6.2/utilities/pspp-dump-sav+0x41f384)

0x602000000111 is located 0 bytes to the right of 1-byte region
[0x602000000110,0x602000000111)
allocated by thread T0 here:
    #0 0x49a3c2 in calloc /home/kdsj/workspace/llvm-
project/compiler-rt/lib/asan/asan_malloc_linux.cpp:154:3
    #1 0x4da045 in xmalloc /home/kdsj/workspace/fuzz/verify/pspp-
1.6.2/gl/xmalloc.c:297:19
    #2 0x7flbaa451fcf in __libc_start_call_main
csu/../sysdeps/nptl/libc_start_call_main.h:58:16

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/kdsj/workspace/fuzz/verify/pspp-1.6.2/utilities/pspp-dump-
```

han
zheng
<kdsj>

```

sav.c:1661:20 in read_string
Shadow bytes around the buggy address:
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff8000: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fa
  0x0c047fff8010: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fa
=>0x0c047fff8020: fa fa[01]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8070: 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
==2607491==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 #53649: poc4.zip added by kdsj (653B - application/x-zip-compressed)

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)

-email is unavailable- added by [kdsj](#) (Submitted the item)

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
2022-09-19	blp	Status	None		Fixed
		Open/Closed	Open		Closed
2022-09-02	kdsj	Attached File	-		Added poc4.zip, #53649

