



PSPP - Bugs: bug #67074, Heap Buffer Overflow in PSPP...

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

Not Logged in

[Login](#)

[New User](#)

This Page

[Language](#)

[Clean Reload](#)

Search

Area to search in
[Groups](#) 

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](#)



Help us protect your freedom and the rights of computer users everywhere by becoming a member of the FSF.

Join Now!

Free Software Foundation

[Coming Events](#)

[Free Software Directory](#)

[Cryptographic software legal notice](#)

[Copyright infringement notification](#)

Related Forges

[Savannah Non-GNU](#)

bug #67074: Heap Buffer Overflow in PSPP Output Directory Processing

Submitter: [Nez <xu_dawn>](#)

Submitted: Sat 03 May 2025 11:49:54 AM UTC

[Submit changes and browse items](#)

[Submit changes and return to this item](#)

[Preview](#)

Category: None

Status: None

Open/Closed: Open

Effort: 0.00

Severity: 5 - Average

Assigned to: None

Release: None

* Mandatory Fields

(+) **Post a Comment**

(-) **Discussion**

Sat 03 May 2025 11:49:54 AM UTC, **original submission**:

[Quote](#)

Nez
<xu_dawn>

Summary

Heap Buffer Overflow in PSPP Output Directory Processing

Environment

PSPP version: master in Git

Repository[commit:82fb509fb2fedd33e7ac0c46ca99e108bb3bdfbf]

OS: Ubuntu 20.04.6 LTS

Compiler: Clang-12.0.1

Steps to reproduce

```
# export CFLAGS="-g -O0 -fno-inline -fno-lto -fsanitize=address"
# export CXXFLAGS="-g -O0 -fno-inline -fno-lto -fsanitize=address"
# ./configure --prefix=$INSTALL_DIR --without-gui --disable-shared --without-perl-module
# make -j64 & make install
```

```
root@9c4de30a2a30:./pspp-output dir POC -O format=pdf
```

```
=====
==81148==ERROR: AddressSanitizer: heap-buffer-overflow on address
0x621000007590 at pc 0x00000043c8be bp 0x7ffelfcc20e0 sp 0x7ffelfcc18a8
WRITE of size 7653 at 0x621000007590 thread T0
    #0 0x43c8bd in fread (/new-test/fuzzdir/fuz-pspp-output_dir/pspp-
output+0x43c8bd)
    #1 0x6c7a49 in inflate_read /new-test/program/download/pspp-
2.0.1/src/libpspp/zip-reader.c:747:20
    #2 0x6c3bc4 in zip_member_read /new-test/program/download/pspp-
```

```

2.0.1/src/libpspp/zip-reader.c:238:20
    #3 0x55b900 in spv_read_xml_member /new-test/program/download/pspp-
2.0.1/src/output/spv/spv.c:433:20
    #4 0x55d1d7 in spv_heading_read /new-test/program/download/pspp-
2.0.1/src/output/spv/spv.c:768:17
    #5 0x55cbf2 in spv_read /new-test/program/download/pspp-
2.0.1/src/output/spv/spv.c:867:9
    #6 0x4d44e6 in read_and_filter_spv /new-test/program/download/pspp-
2.0.1/utilities/pspp-output.c:195:15
    #7 0x4d2378 in run_directory /new-test/program/download/pspp-
2.0.1/utilities/pspp-output.c:204:30
    #8 0x4d1329 in main /new-test/program/download/pspp-
2.0.1/utilities/pspp-output.c:856:3
    #9 0x7f00ff4cdd8f in __libc_start_call_main
csu/../sysdeps/nptl/libc_start_call_main.h:58:16
    #10 0x7f00ff4cde3f in __libc_start_main csu/../csu/libc-
start.c:392:3
    #11 0x4250b4 in _start (/new-test/fuzzdir/fuz-pspp-output_dir/pspp-
output+0x4250b4)

```

0x621000007590 is located 0 bytes to the right of 4240-byte region
[0x621000006500,0x621000007590)

allocated by thread T0 here:

```

    #0 0x4a00f2 in calloc (/new-test/fuzzdir/fuz-pspp-output_dir/pspp-
output+0x4a00f2)
    #1 0x6c75e1 in inflate_init /new-test/program/download/pspp-
2.0.1/src/libpspp/zip-reader.c:686:26

```

SUMMARY: AddressSanitizer: heap-buffer-overflow (/new-test/fuzzdir/fuz-
pspp-output_dir/pspp-output+0x43c8bd) in fread

Shadow bytes around the buggy address:

```

0x0c427fff8e60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c427fff8e70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c427fff8e80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c427fff8e90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c427fff8ea0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c427fff8eb0: 00 00[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c427fff8ec0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c427fff8ed0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c427fff8ee0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c427fff8ef0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c427fff8f00: fa 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

```

==81148==ABORTING

POC

<https://drive.google.com/file/d/1yDmRKzWMQpLpiKDpvv1Yhl8UETBKCTDb/view?usp=sharing>

Credit

(-) Attached Files

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

Attach Files:

No file chosen

No file chosen

No file chosen

No file chosen

Comment:

No files currently attached

(-) Dependencies

Depends on the following items: None found

Items that depend on this one: None found

(+) Mail Notification Carbon-Copy List

(+) Votes

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

(+) History

