

[New issue](#)[Jump to bottom](#)

heap overflow in _dwarf_check_string_valid in dwarf_util.c #116

🔒 Closed sleिकासper opened this issue on May 26 · 1 comment

sleिकासper commented on May 26

There is a heap overflow in _dwarf_check_string_valid in dwarf_util.c. Depending on the usage of this library, this may cause code execution or deny of service.

reproduce steps:

1. compile libdwarf with address sanitizer
2. run dwarfdump with poc file

```
dwarfdump -vv -a ./poc
```

poc:

[poc.zip](#)

Address sanitizer output:

```
=====
==1464907==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6060000015bb at pc
0x00000083fa88 bp 0x7fff18213420 sp 0x7fff18213418
READ of size 1 at 0x6060000015bb thread T0
#0 0x83fa87 in _dwarf_check_string_valid
/home/casper/targets/struct/libdwarf/aflasan/SRC/src/lib/libdwarf/dwarf_util.c:938:13
#1 0x70192c in _dwarf_internal_get_pubnames_like_data
/home/casper/targets/struct/libdwarf/aflasan/SRC/src/lib/libdwarf/dwarf_global.c:560:19
#2 0x7e43be in dwarf_get_pubtypes
/home/casper/targets/struct/libdwarf/aflasan/SRC/src/lib/libdwarf/dwarf_pubtypes.c:63:11
#3 0x637fa0 in print_types
/home/casper/targets/struct/libdwarf/aflasan/SRC/src/bin/dwarfdump/print_types.c:90:13
#4 0x519257 in process_one_file
/home/casper/targets/struct/libdwarf/aflasan/SRC/src/bin/dwarfdump/dwarfdump.c:1242:16
#5 0x512ac7 in main
/home/casper/targets/struct/libdwarf/aflasan/SRC/src/bin/dwarfdump/dwarfdump.c:503:9
#6 0x7f1199de00b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/csu/../csu/libc-
start.c:308:16
#7 0x42848d in _start
```

```
(/home/casper/targets/struct/libdwarf/aflasan/fuzzrun/dwarfdump+0x42848d)
```

0x606000015bb is located 0 bytes to the right of 59-byte region [0x60600001580,0x606000015bb) allocated by thread T0 here:

```
#0 0x4cd59f in malloc /home/casper/fuzz/fuzzdeps/llvm-project-11.0.0/compiler-rt/lib/asan/asan_malloc_linux.cpp:145:3
```

```
#1 0x870cd5 in elf_load_nolibelf_section  
/home/casper/targets/struct/libdwarf/aflasan/SRC/src/lib/libdwarf/dwarf_elfread.c:229:26
```

```
#2 0x4969e5 in vprintf /home/casper/fuzz/fuzzdeps/llvm-project-11.0.0/compiler-rt/lib/asan/./sanitizer_common/sanitizer_common_interceptors.inc:1641:1
```

SUMMARY: AddressSanitizer: heap-buffer-overflow

/home/casper/targets/struct/libdwarf/aflasan/SRC/src/lib/libdwarf/dwarf_util.c:938:13 in _dwarf_check_string_valid

Shadow bytes around the buggy address:

```
0x0c0c7fff8260: fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd fa  
0x0c0c7fff8270: fa fa fa fa fd fd fd fd fd fd fd fa fa fa fa fa  
0x0c0c7fff8280: 00 00 00 00 00 00 00 00 fa fa fa fa 00 00 00 00  
0x0c0c7fff8290: 00 00 00 00 fa fa fa fa 00 00 00 00 00 00 00 00  
0x0c0c7fff82a0: fa fa fa fa 00 00 00 00 00 00 00 00 00 fa fa fa fa  
=>0x0c0c7fff82b0: 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa fa fa  
0x0c0c7fff82c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c0c7fff82d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c0c7fff82e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c0c7fff82f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c0c7fff8300: 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

davea42 commented on May 29

Owner

Thank you for the report and test case. I assigned this libdwarf vulnerability as DW202205-001 and have pushed the fix .

View the vulnerability on www.prevanders.net/dwarfbug.html



davea42 closed this as completed on May 29

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

