

CZ4062 Assignment

Fuzzing Report

Group 35

Calvin Che Zi Yi - U1522882K  
Nguyen Dang Duy Nghia - U1520536G  
Vu Duc Long - U1520526J

Contents

[2 Observations of Fuzzing Process 3](#_Toc530737125)

[2.1 cxxfilt\_1542666721080 3](#_Toc530737126)

[2.1.1 Execution Speed 3](#_Toc530737127)

[2.1.2 Paths Info 3](#_Toc530737128)

[2.1.3 Abnormal Info 4](#_Toc530737129)

[2.1.4 Findings of Mutation Operators 4](#_Toc530737130)

[2.2 strings\_1542666723047 5](#_Toc530737131)

[2.2.1 Execution Speed 5](#_Toc530737132)

[2.2.2 Paths Info 5](#_Toc530737133)

[2.2.3 Abnormal Info 6](#_Toc530737134)

[2.2.4 Findings of Mutation Operators 6](#_Toc530737135)

[3 Crash Analysis 7](#_Toc530737136)

[3.1 GNU c++filt 2.15 7](#_Toc530737137)

[3.1.1 A null pointer dereference in function work\_stuff\_copy\_to\_from()(cplus-dem.c:1208) 7](#_Toc530737138)

[3.1.2 A null pointer dereference in function cplus\_demangle\_type()(cp-demangle.c:1827) 7](#_Toc530737139)

[3.1.3 A read invalid address in function d\_name()(cp-demangle.c:1167) 8](#_Toc530737140)

[3.1.4 A null pointer dereference in function do\_type()(cplus-dem.c:3760) 9](#_Toc530737141)

[3.1.5 A read invalid address in function d\_substitution()(cp-demangle.c:2589) 10](#_Toc530737142)

[3.2 GNU strings 2.15 11](#_Toc530737143)

[3.2.1 A null pointer dereference in function bfd\_section\_from\_shdr()(elf.c:1657) 11](#_Toc530737144)

[3.2.2 A null pointer dereference in function bfd\_section\_from\_shdr()(elf.c:1652) 11](#_Toc530737145)

[3.2.3 A null pointer dereference in function bfd\_hash\_lookup()(hash.c:374) 12](#_Toc530737146)

[3.2.4 A read invalid address in function bfd\_alloc()(opncls.c:652) 12](#_Toc530737147)

[3.2.5 A null pointer dereference in \_bfd\_elf\_make\_section\_from\_shdr bfd\_alloc()(elf.c:746) 13](#_Toc530737148)

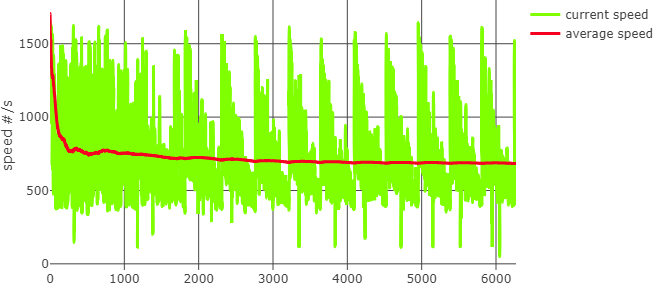
# Observations of Fuzzing Process

Fuzzing was performed on two of the provided programs, GNU c++filt 2.15 and GNU strings 2.15 over approximately 26 hours with 3 CPU cores each.

## cxxfilt\_1542666721080

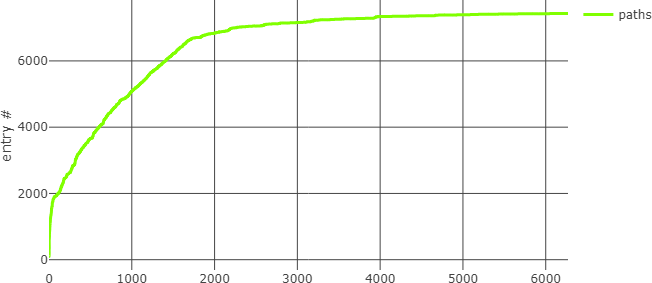
Fuzzing for GNU c++filt 2.15 started at 20/11/2018 6:32:01 and ended at 21/11/2018 8:39:30.

### Execution Speed



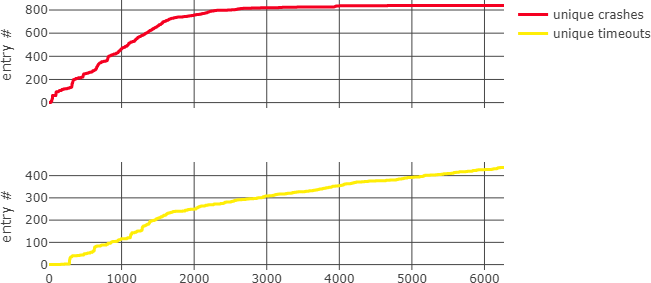
The average execution speed was around 700 per second, with a higher average speed of more than 1500 at the start and stabilizing at slightly less than 700. There is a clear pattern of the current speed throughout the fuzzing, showing the start and end of different stages.

### Paths Info



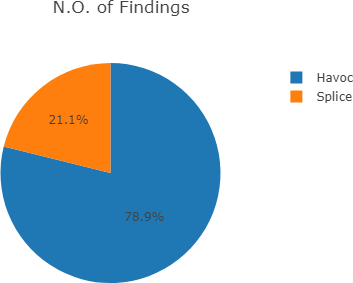
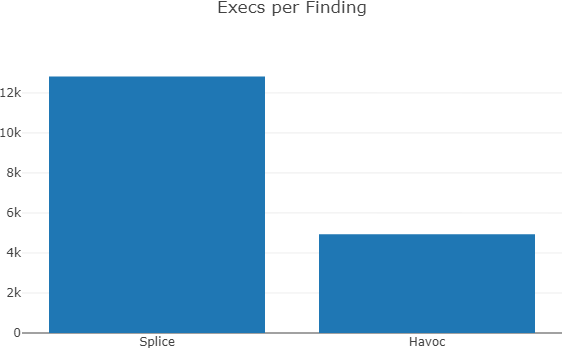
The fuzzing tool tested a total of 7429 paths, with lesser new paths found after about 8 hours.

### Abnormal Info



There was a total of 840 unique crashes and 437 unique timeouts found. The unique crashes curve closely mirrors the paths curve, as only with new paths are unique crashes and timeouts discovered.

### Findings of Mutation Operators

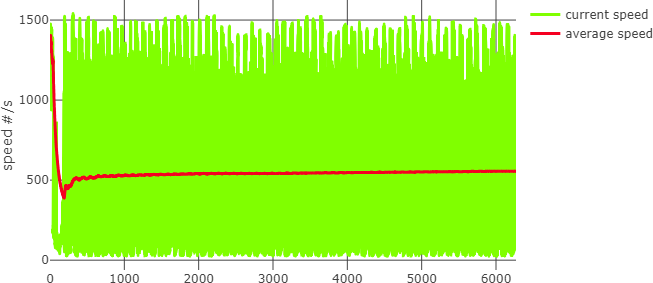
 

The Havoc mutation operator is more prevalent than Splice in the fuzzing of the program.

## strings\_1542666723047

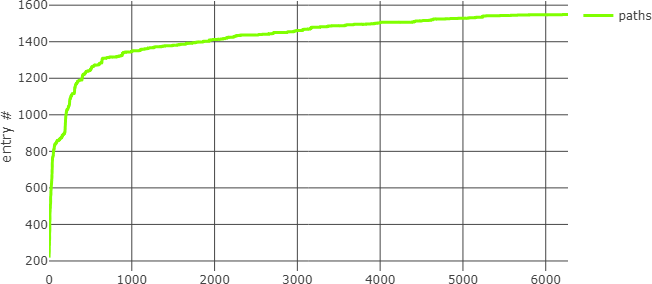
Fuzzing for GNU strings 2.15 started at 20/11/2018 6:32:03 and ended at 21/11/2018 8:39:31.

### Execution Speed



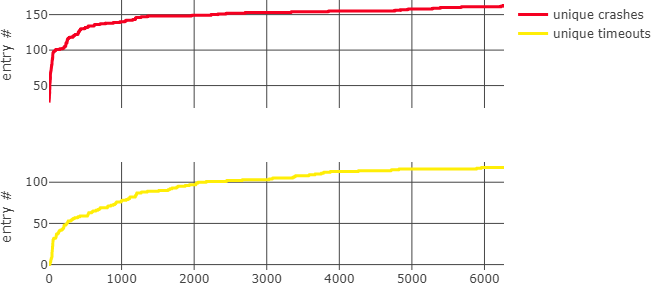
The average execution speed was around 550 per second, with a higher average speed of more than 1400 at the start and stabilizing at around 550.

### Paths Info



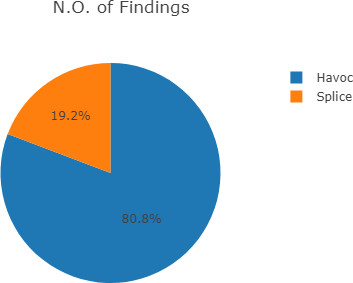
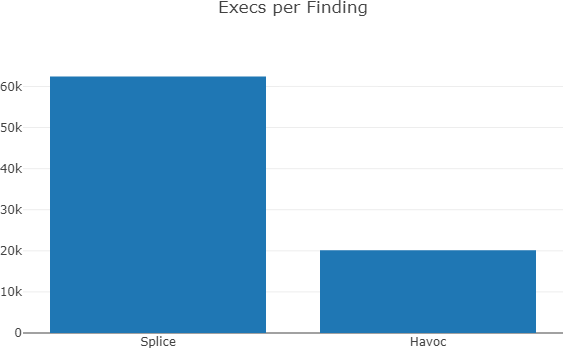
The fuzzing tool tested a total of 1549 paths, with lesser new paths found after about 4 hours.

### Abnormal Info



There was a total of 163 unique crashes and 118 unique timeouts found. These curves closely mirror the paths curve, as only with new paths are unique crashes and timeouts discovered.

### Findings of Mutation Operators

The Havoc mutation operator is more prevalent than Splice in the fuzzing of the program.

# Crash Analysis

Crashes from GNU c++filt 2.15 and GNU strings 2.15 were triaged and analysed using GDB.

## GNU c++filt 2.15

The source of GNU c++filt 2.15 was obtained from <http://ftp.gnu.org/gnu/binutils/binutils-2.15.tar.bz2>.

### A null pointer dereference in function work\_stuff\_copy\_to\_from()(cplus-dem.c:1208)

Input File: w01\_000000,sig:11,Havoc:5594:27520,src:w01\_000115

|  |
| --- |
| Program received signal SIGSEGV, Segmentation fault.  strlen () at ../sysdeps/x86\_64/strlen.S:106  106 ../sysdeps/x86\_64/strlen.S: No such file or directory.  (gdb) bt  #0 strlen () at ../sysdeps/x86\_64/strlen.S:106  #1 0x00000000004f1f7c in work\_stuff\_copy\_to\_from (to=0x7fffffffe430, from=0x7fffffffe570)  at ../../libiberty/cplus-dem.c:1208  #2 0x00000000004ef73c in iterate\_demangle\_function (work=0x7fffffffe570, mangled=<optimized out>,  declp=0x7fffffffe4f0, scan=0x7339c5 <mbuffer+5> "\_\_p\_\_.") at ../../libiberty/cplus-dem.c:2625  #3 0x00000000004dbc65 in internal\_cplus\_demangle (work=0x7fffffffe570, mangled=<optimized out>)  at ../../libiberty/cplus-dem.c:2865  #4 0x00000000004dab41 in cplus\_demangle (mangled=0x7339c0 <mbuffer> "\_Q\_\_\_\_\_p\_\_.", options=<optimized out>)  at ../../libiberty/cplus-dem.c:936  #5 0x00000000004027b9 in main (argc=<optimized out>, argv=<optimized out>) at ../../binutils/cxxfilt.c:270 |

#### libiberty/cplus-dem.c

|  |
| --- |
| 1206 for (i = 0; i < from->numb; i++)  1207 {  1208 int len = strlen (from->btypevec[i]) + 1;  1209  1210 to->btypevec[i] = xmalloc (len);  1211 memcpy (to->btypevec[i], from->btypevec[i], len);  1212 } |

#### Values

|  |
| --- |
| (gdb) p from  $36 = (struct work\_stuff \*) 0x7fffffffe570  (gdb) p from->btypevec  $37 = (char \*\*) 0x75d430  (gdb) p from->numb  $38 = 1  (gdb) p from->btypevec[0]  $39 = 0x0  (gdb) p \*from->btypevec[0]  Cannot access memory at address 0x0 |

The pointer at from->btypevec[0] points to address 0x0, which is a null pointer dereference.

### A null pointer dereference in function cplus\_demangle\_type()(cp-demangle.c:1827)

Input File: w01\_000001,sig:11,Havoc:5470:31360,src:w01\_000129

|  |
| --- |
| Program received signal SIGSEGV, Segmentation fault.  cplus\_demangle\_type (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1827  1827 ../../libiberty/cp-demangle.c: No such file or directory.  (gdb) bt  #0 cplus\_demangle\_type (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1827  #1 0x0000000000501e7b in d\_bare\_function\_type (di=0x7fffffffe4b8, has\_return\_type=0)  at ../../libiberty/cp-demangle.c:2041  #2 0x00000000004f4b4a in d\_encoding (di=0x7fffffffe4b8, top\_level=0) at ../../libiberty/cp-demangle.c:1091  #3 0x0000000000500d82 in d\_local\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2446  #4 d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1120  #5 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=0) at ../../libiberty/cp-demangle.c:1056  #6 0x0000000000500d82 in d\_local\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2446  #7 d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1120  #8 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=0) at ../../libiberty/cp-demangle.c:1056  #9 0x0000000000500d82 in d\_local\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2446  #10 d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1120  #11 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=0) at ../../libiberty/cp-demangle.c:1056  #12 0x0000000000500d82 in d\_local\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2446  #13 d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1120  #14 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=1) at ../../libiberty/cp-demangle.c:1056  #15 0x000000000050026a in cplus\_demangle\_mangled\_name (top\_level=1, di=<optimized out>)  at ../../libiberty/cp-demangle.c:980  #16 d\_demangle (mangled=0x7339c0 <mbuffer> "\_ZZZZZZdd", options=267, palc=0x7fffffffe550)  at ../../libiberty/cp-demangle.c:3853  #17 0x000000000050001c in cplus\_demangle\_v3 (mangled=0x12 <error: Cannot access memory at address 0x12>,  options=7649760) at ../../libiberty/cp-demangle.c:4011  #18 0x00000000004daa6c in cplus\_demangle (mangled=0x7339c0 <mbuffer> "\_ZZZZZZdd", options=<optimized out>)  at ../../libiberty/cplus-dem.c:921  #19 0x00000000004027b9 in main (argc=<optimized out>, argv=<optimized out>) at ../../binutils/cxxfilt.c:270 |

#### libiberty/cp-demangle.c

|  |
| --- |
| 1819 switch (peek)  1820 {  1821 case 'a': case 'b': case 'c': case 'd': case 'e': case 'f': case 'g':  1822 case 'h': case 'i': case 'j': case 'l': case 'm': case 'n':  1823 case 'o': case 's': case 't':  1824 case 'v': case 'w': case 'x': case 'y': case 'z':  1825 ret = d\_make\_builtin\_type (di,  1826 &cplus\_demangle\_builtin\_types[peek - 'a']);  1827 di->expansion += ret->u.s\_builtin.type->len;  1828 can\_subst = 0;  1829 d\_advance (di, 1);  1830 break; |

#### Values

|  |
| --- |
| (gdb) p ret  $1 = (struct demangle\_component \*) 0x0  (gdb) p ret->u.s\_builtin.type  Cannot access memory at address 0x8 |

The pointer at ret points to address 0x0, which is a null pointer dereference.

### A read invalid address in function d\_name()(cp-demangle.c:1167)

Input File: w01\_000015,sig:11,Havoc:1323:30080,src:w01\_000270

|  |
| --- |
| Program received signal SIGSEGV, Segmentation fault.  0x0000000000500ff7 in d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1167  1167 ../../libiberty/cp-demangle.c: No such file or directory.  (gdb) bt  #0 0x0000000000500ff7 in d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1167  #1 0x00000000004f62a3 in d\_class\_enum\_type (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2082  #2 cplus\_demangle\_type (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1846  #3 0x0000000000501e7b in d\_bare\_function\_type (di=0x7fffffffe4b8, has\_return\_type=0)  at ../../libiberty/cp-demangle.c:2041  #4 0x00000000004f4b4a in d\_encoding (di=0x7fffffffe4b8, top\_level=0) at ../../libiberty/cp-demangle.c:1091  #5 0x0000000000500d82 in d\_local\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2446  #6 d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1120  #7 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=0) at ../../libiberty/cp-demangle.c:1056  #8 0x0000000000500d82 in d\_local\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2446  #9 d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1120  #10 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=0) at ../../libiberty/cp-demangle.c:1056  #11 0x0000000000500d82 in d\_local\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2446  #12 d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1120  #13 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=0) at ../../libiberty/cp-demangle.c:1056  #14 0x0000000000500d82 in d\_local\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2446  #15 d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1120  #16 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=0) at ../../libiberty/cp-demangle.c:1056  #17 0x0000000000500d82 in d\_local\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2446  #18 d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1120  #19 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=1) at ../../libiberty/cp-demangle.c:1056  #20 0x000000000050026a in cplus\_demangle\_mangled\_name (top\_level=1, di=<optimized out>)  at ../../libiberty/cp-demangle.c:980  #21 d\_demangle (mangled=0x7339c0 <mbuffer> "\_ZZZZZZZ", options=267, palc=0x7fffffffe550)  at ../../libiberty/cp-demangle.c:3853  #22 0x000000000050001c in cplus\_demangle\_v3 (mangled=0x7fffffffe4b8 "\300\071s", options=-7376)  at ../../libiberty/cp-demangle.c:4011  #23 0x00000000004daa6c in cplus\_demangle (mangled=0x7339c0 <mbuffer> "\_ZZZZZZZ", options=<optimized out>)  at ../../libiberty/cplus-dem.c:921  #24 0x00000000004027b9 in main (argc=<optimized out>, argv=<optimized out>) at ../../binutils/cxxfilt.c:270 |

#### libiberty/cp-demangle.c

|  |
| --- |
| 1111 char peek = d\_peek\_char (di);  1112 struct demangle\_component \*dc;  1113  1114 switch (peek)  1115 {  ...  1165 default:  1166 dc = d\_unqualified\_name (di);  1167 if (d\_peek\_char (di) == 'I') |

#### Values

|  |
| --- |
| (gdb) p peek  $2 = <optimized out>  (gdb) p di  $3 = (struct d\_info \*) 0x7fffffffe4b8 |

The pointer to di is not 0x0, so this is not a null pointer dereference bug. The d\_peek\_char() function probably tried to read an invalid address. We are unable to confirm this as d\_peek\_char() is not part of the package.

### A null pointer dereference in function do\_type()(cplus-dem.c:3760)

Input File: w01\_000200,sig:11,Havoc:287:368,src:w01\_001883

|  |
| --- |
| Program received signal SIGSEGV, Segmentation fault.  0x00000000004d5e8a in do\_type (work=0x7fffffffe570, mangled=0x7fffffffe4e8, result=0x7fffffffe340)  at ../../libiberty/cplus-dem.c:3760  3760 ../../libiberty/cplus-dem.c: No such file or directory.  (gdb) bt  #0 0x00000000004d5e8a in do\_type (work=0x7fffffffe570, mangled=0x7fffffffe4e8, result=0x7fffffffe340)  at ../../libiberty/cplus-dem.c:3760  #1 0x00000000004dfe9a in demangle\_signature (work=0x7fffffffe570, mangled=0x7fffffffe4e8, declp=0x7fffffffe4f0)  at ../../libiberty/cplus-dem.c:1436  #2 0x00000000004ef7d0 in iterate\_demangle\_function (work=0x7fffffffe570, mangled=<optimized out>,  declp=0x7fffffffe4f0, scan=0x7339c4 <mbuffer+4> "\_\_B3333333333\_s") at ../../libiberty/cplus-dem.c:2636  #3 0x00000000004dbc65 in internal\_cplus\_demangle (work=0x7fffffffe570, mangled=<optimized out>)  at ../../libiberty/cplus-dem.c:2865  #4 0x00000000004dab41 in cplus\_demangle (mangled=0x7339c0 <mbuffer> "a\_\_m\_\_B3333333333\_s", options=<optimized out>)  at ../../libiberty/cplus-dem.c:936  #5 0x00000000004027b9 in main (argc=<optimized out>, argv=<optimized out>) at ../../binutils/cxxfilt.c:270 |

#### libiberty/cplus-dem.c

|  |
| --- |
| 3754 /\* A back reference to a previously seen squangled type \*/  3755 case 'B':  3756 (\*mangled)++;  3757 if (!get\_count (mangled, &n) || n >= work -> numb)  3758 success = 0;  3759 else  3760 string\_append (result, work->btypevec[n]);  3761 break; |

#### Values

|  |
| --- |
| (gdb) p work  $6 = (struct work\_stuff \*) 0x7fffffffe570  (gdb) p work->btypevec  $7 = (char \*\*) 0x0 |

The pointer at work-> btypevec points to address 0x0, which is a null pointer dereference.

### A read invalid address in function d\_substitution()(cp-demangle.c:2589)

Input File: w01\_000400,sig:11,Havoc:182:532,src:w01\_003608

|  |
| --- |
| Program received signal SIGSEGV, Segmentation fault.  0x00000000004f830b in d\_substitution (di=0x7fffffffe4b8, prefix=<optimized out>) at ../../libiberty/cp-demangle.c:2589  2589 in ../../libiberty/cp-demangle.c  (gdb) bt  #0 0x00000000004f830b in d\_substitution (di=0x7fffffffe4b8, prefix=<optimized out>) at ../../libiberty/cp-demangle.c:2589  #1 0x000000000050134d in d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1128  #2 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=0) at ../../libiberty/cp-demangle.c:1056  #3 0x0000000000500d82 in d\_local\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:2446  #4 d\_name (di=0x7fffffffe4b8) at ../../libiberty/cp-demangle.c:1120  #5 0x00000000004f46ee in d\_encoding (di=0x7fffffffe4b8, top\_level=1) at ../../libiberty/cp-demangle.c:1056  #6 0x000000000050026a in cplus\_demangle\_mangled\_name (top\_level=1, di=<optimized out>) at ../../libiberty/cp-demangle.c:980  #7 d\_demangle (mangled=0x7339c0 <mbuffer> "\_ZZS", 'Z' <repeats 13 times>, "MZZZZZZZGZZZ\_S\_\_\_\_\_\_\_\_\_\_O\_\_\_\_", options=267, palc=0x7fffffffe550) at ../../libiberty/cp-demangle.c:3853  #8 0x000000000050001c in cplus\_demangle\_v3 (mangled=0x7fffffffe4b8 "\300\071s", options=-1364035264) at ../../libiberty/cp-demangle.c:4011  #9 0x00000000004daa6c in cplus\_demangle (mangled=0x7339c0 <mbuffer> "\_ZZS", 'Z' <repeats 13 times>, "MZZZZZZZGZZZ\_S\_\_\_\_\_\_\_\_\_\_O\_\_\_\_", options=<optimized out>)  at ../../libiberty/cplus-dem.c:921  #10 0x00000000004027b9 in main (argc=<optimized out>, argv=<optimized out>) at ../../binutils/cxxfilt.c:270 |

#### libiberty/cp-demangle.c

|  |
| --- |
| 2562 if (c == '\_' || IS\_DIGIT (c) || IS\_UPPER (c))  2563 {  2564 int id;  2565  2566 id = 0;  ...  2584 if (id >= di->next\_sub)  2585 return NULL;  2587 ++di->did\_subs;  2588  2589 return di->subs[id];  2590 } |

#### Values

|  |
| --- |
| (gdb) p di  $24 = (struct d\_info \*) 0x7fffffffe4b8  (gdb) p di->next\_sub  $26 = 0  (gdb) p di->subs  $27 = (struct demangle\_component \*\*) 0x7fffffffdaa0  (gdb) p di->subs[0]  $30 = (struct demangle\_component \*) 0x7fffffffe4b8 |

The pointer at di and di->subs[0] both point to the same address 0x7fffffffe4b8, which will likely result in a read invalid address when accessing other pointers in the struct.

## GNU strings 2.15

The source of GNU strings 2.15 was obtained from <http://ftp.gnu.org/gnu/binutils/binutils-2.15.tar.bz2>.

### A null pointer dereference in function bfd\_section\_from\_shdr()(elf.c:1657)

Input File: 01\_000000,sig:11,Havoc:34:18304,src:w00\_000000

|  |
| --- |
| Program received signal SIGSEGV, Segmentation fault.  0x0000000000431c39 in bfd\_section\_from\_shdr (abfd=0x71c080, shindex=515) at ../../bfd/elf.c:1657  1657 ../../bfd/elf.c: No such file or directory.  (gdb) bt  #0 0x0000000000431c39 in bfd\_section\_from\_shdr (abfd=0x71c080, shindex=515) at ../../bfd/elf.c:1657  #1 0x0000000000477dbb in bfd\_elf32\_object\_p (abfd=0x71c080) at ../../bfd/elfcode.h:689  #2 0x0000000000408d91 in bfd\_check\_format\_matches (abfd=0x71c080, format=<optimized out>, matching=0x0)  at ../../bfd/format.c:228  #3 0x000000000040298f in strings\_object\_file (file=<optimized out>) at ../../binutils/strings.c:350  #4 strings\_file (file=<optimized out>) at ../../binutils/strings.c:380  #5 main (argc=2, argv=0x7fffffffe6d8) at ../../binutils/strings.c:298 |

#### bfd/elf.c

|  |
| --- |
| 1652 Elf\_Internal\_Shdr \*hdr = elf\_elfsections (abfd)[shindex];  1653 Elf\_Internal\_Ehdr \*ehdr = elf\_elfheader (abfd);  1654 const struct elf\_backend\_data \*bed = get\_elf\_backend\_data (abfd);  1655 const char \*name;  1656  1657 name = elf\_string\_from\_elf\_strtab (abfd, hdr->sh\_name); |

#### Values

|  |
| --- |
| (gdb) p abfd  $1 = (bfd \*) 0x71c080  (gdb) p hdr  $3 = (Elf\_Internal\_Shdr \*) 0x0  (gdb) p hdr->sh\_name  Cannot access memory at address 0x0 |

The pointer at hdr points to address 0x0, which is a null pointer dereference.

### A null pointer dereference in function bfd\_section\_from\_shdr()(elf.c:1652)

Input File: w01\_000026,sig:11,Splice:1:16,src:w01\_000093

|  |
| --- |
| Program received signal SIGSEGV, Segmentation fault.  0x0000000000431c2a in bfd\_section\_from\_shdr (abfd=0x71c080, shindex=924872556) at ../../bfd/elf.c:1652  1652 in ../../bfd/elf.c  (gdb) bt  #0 0x0000000000431c2a in bfd\_section\_from\_shdr (abfd=0x71c080, shindex=924872556) at ../../bfd/elf.c:1652  #1 0x0000000000432875 in bfd\_section\_from\_shdr (abfd=0x71c080, shindex=3) at ../../bfd/elf.c:1751  #2 0x0000000000477dbb in bfd\_elf32\_object\_p (abfd=0x71c080) at ../../bfd/elfcode.h:689  #3 0x0000000000408d91 in bfd\_check\_format\_matches (abfd=0x71c080, format=<optimized out>, matching=0x0)  at ../../bfd/format.c:228  #4 0x000000000040298f in strings\_object\_file (file=<optimized out>) at ../../binutils/strings.c:350  #5 strings\_file (file=<optimized out>) at ../../binutils/strings.c:380  #6 main (argc=2, argv=0x7fffffffe6e8) at ../../binutils/strings.c:298 |

#### bfd/elf.c

|  |
| --- |
| 1652 Elf\_Internal\_Shdr \*hdr = elf\_elfsections (abfd)[shindex];  1653 Elf\_Internal\_Ehdr \*ehdr = elf\_elfheader (abfd);  1654 const struct elf\_backend\_data \*bed = get\_elf\_backend\_data (abfd);  1655 const char \*name;  1656  1657 name = elf\_string\_from\_elf\_strtab (abfd, hdr->sh\_name); |

#### Values

|  |
| --- |
| (gdb) p abfd  $4 = (bfd \*) 0x71c080  (gdb) p shindex  $5 = 924872556  (gdb) p \*abfd  $6 = {id = 0, filename = 0x7fffffffe8e8 "out\_20181119\_22\_32\_03/crash/w01\_000026,sig:11,Splice:1:16,src:w01\_000093",  xvec = 0x4e4828 <bfd\_elf32\_little\_generic\_vec>, iostream = 0x71e1d0, cacheable = 1, target\_defaulted = 1,  lru\_prev = 0x71c080, lru\_next = 0x71c080, where = 3439329535, opened\_once = 0, mtime\_set = 0, mtime = 0, ifd = 0,  format = bfd\_object, direction = read\_direction, flags = 256, origin = 0, output\_has\_begun = 0, section\_htab = {  table = 0x720430, size = 4051, newfunc = 0x40d330 <bfd\_section\_hash\_newfunc>, memory = 0x71f410}, sections = 0x0,  section\_tail = 0x71c110, section\_count = 0, start\_address = 4278222956, symcount = 0, outsymbols = 0x0,  dynsymcount = 0, arch\_info = 0x4d5820 <bfd\_default\_arch\_struct>, arelt\_data = 0x0, my\_archive = 0x0, next = 0x0,  archive\_head = 0x0, has\_armap = 0, link\_next = 0x0, archive\_pass = 0, tdata = {aout\_data = 0x71c1e0,  aout\_ar\_data = 0x71c1e0, oasys\_obj\_data = 0x71c1e0, oasys\_ar\_data = 0x71c1e0, coff\_obj\_data = 0x71c1e0,  pe\_obj\_data = 0x71c1e0, xcoff\_obj\_data = 0x71c1e0, ecoff\_obj\_data = 0x71c1e0, ieee\_data = 0x71c1e0,  ieee\_ar\_data = 0x71c1e0, srec\_data = 0x71c1e0, ihex\_data = 0x71c1e0, tekhex\_data = 0x71c1e0,  elf\_obj\_data = 0x71c1e0, nlm\_obj\_data = 0x71c1e0, bout\_data = 0x71c1e0, mmo\_data = 0x71c1e0,  sun\_core\_data = 0x71c1e0, sco5\_core\_data = 0x71c1e0, trad\_core\_data = 0x71c1e0, som\_data = 0x71c1e0,  hpux\_core\_data = 0x71c1e0, hppabsd\_core\_data = 0x71c1e0, sgi\_core\_data = 0x71c1e0, lynx\_core\_data = 0x71c1e0,  osf\_core\_data = 0x71c1e0, cisco\_core\_data = 0x71c1e0, versados\_data = 0x71c1e0, netbsd\_core\_data = 0x71c1e0,  mach\_o\_data = 0x71c1e0, mach\_o\_fat\_data = 0x71c1e0, pef\_data = 0x71c1e0, pef\_xlib\_data = 0x71c1e0,  sym\_data = 0x71c1e0, any = 0x71c1e0}, usrdata = 0x0, memory = 0x71c1b0} |

The pointer at abdf->sections points to address 0x0, which is a null pointer dereference.

### A null pointer dereference in function bfd\_hash\_lookup()(hash.c:374)

Input File: w01\_000030,sig:11,Splice:6:16,src:w01\_000198

|  |
| --- |
| Program received signal SIGSEGV, Segmentation fault.  0x000000000040f8ee in bfd\_hash\_lookup (table=0x71c0f0, string=0x0, create=1, copy=0) at ../../bfd/hash.c:374  374 ../../bfd/hash.c: No such file or directory.  (gdb) bt  #0 0x000000000040f8ee in bfd\_hash\_lookup (table=0x71c0f0, string=0x0, create=1, copy=0) at ../../bfd/hash.c:374  #1 0x000000000040daa4 in bfd\_make\_section\_anyway (abfd=0x71c080, name=0x0) at ../../bfd/section.c:941  #2 0x000000000042c25c in \_bfd\_elf\_make\_section\_from\_shdr (abfd=0x71c080, hdr=0x71c790, name=0x0)  at ../../bfd/elf.c:651  #3 0x0000000000431ca7 in bfd\_section\_from\_shdr (abfd=0x71c080, shindex=<optimized out>) at ../../bfd/elf.c:1672  #4 0x0000000000477dbb in bfd\_elf32\_object\_p (abfd=0x71c080) at ../../bfd/elfcode.h:689  #5 0x0000000000408d91 in bfd\_check\_format\_matches (abfd=0x71c080, format=<optimized out>, matching=0x0)  at ../../bfd/format.c:228  #6 0x000000000040298f in strings\_object\_file (file=<optimized out>) at ../../binutils/strings.c:350  #7 strings\_file (file=<optimized out>) at ../../binutils/strings.c:380  #8 main (argc=2, argv=0x7fffffffe6e8) at ../../binutils/strings.c:298 |

#### bfd/hash.c

|  |
| --- |
| 371 hash = 0;  372 len = 0;  373 s = (const unsigned char \*) string;  374 while ((c = \*s++) != '\0') |

#### Values

|  |
| --- |
| (gdb) p s  $8 = (const unsigned char \*) 0x1 <error: Cannot access memory at address 0x1> |

The pointer at s points to address 0x1, which was 0x0 before the ++ operator, which is a null pointer dereference.

### A read invalid address in function bfd\_alloc()(opncls.c:652)

Input File: w01\_000080,sig:11,Havoc:47:1144,src:w01\_000725

|  |
| --- |
| Program received signal SIGSEGV, Segmentation fault.  bfd\_alloc (abfd=0x363f363636363636, size=7) at ../../bfd/opncls.c:652  652 ../../bfd/opncls.c: No such file or directory.  (gdb) bt  #0 bfd\_alloc (abfd=0x363f363636363636, size=7) at ../../bfd/opncls.c:652  #1 0x0000000000416405 in first\_phase (abfd=<optimized out>, type=<optimized out>, src=<optimized out>)  at ../../bfd/tekhex.c:458  #2 pass\_over (abfd=<optimized out>, func=<optimized out>) at ../../bfd/tekhex.c:519  #3 tekhex\_object\_p (abfd=<optimized out>) at ../../bfd/tekhex.c:588  #4 0x0000000000408d91 in bfd\_check\_format\_matches (abfd=0x71c080, format=<optimized out>, matching=0x0)  at ../../bfd/format.c:228  #5 0x000000000040298f in strings\_object\_file (file=<optimized out>) at ../../binutils/strings.c:350  #6 strings\_file (file=<optimized out>) at ../../binutils/strings.c:380  #7 main (argc=2, argv=0x7fffffffe6e8) at ../../binutils/strings.c:298 |

#### bfd/opncls.c

|  |
| --- |
| 644 void \*ret;  645  646 if (size != (unsigned long) size)  647 {  648 bfd\_set\_error (bfd\_error\_no\_memory);  649 return NULL;  650 }  651  652 ret = objalloc\_alloc (abfd->memory, (unsigned long) size); |

#### Values

|  |
| --- |
| (gdb) p abfd  $9 = (bfd \*) 0x363f363636363636  (gdb) p abfd->memory  Cannot access memory at address 0x363f36363636374e  (gdb) p \*abfd  Cannot access memory at address 0x363f363636363636  (gdb) p size  $10 = 7 |

The pointer at abfd->memory points to address 0x363f36363636374e, which is an invalid address.

### A null pointer dereference in \_bfd\_elf\_make\_section\_from\_shdr bfd\_alloc()(elf.c:746)

Input File: w01\_000130,sig:11,Havoc:603:1104,src:w01\_001202

|  |
| --- |
| Program received signal SIGSEGV, Segmentation fault.  \_bfd\_elf\_make\_section\_from\_shdr (abfd=<optimized out>, hdr=0x71c6e0, name=<optimized out>) at ../../bfd/elf.c:746  746 in ../../bfd/elf.c  (gdb) bt  #0 \_bfd\_elf\_make\_section\_from\_shdr (abfd=<optimized out>, hdr=0x71c6e0, name=<optimized out>) at ../../bfd/elf.c:746  #1 0x0000000000432bcb in bfd\_section\_from\_shdr (abfd=0x71c080, shindex=<optimized out>) at ../../bfd/elf.c:1936  #2 0x0000000000477dbb in bfd\_elf32\_object\_p (abfd=0x71c080) at ../../bfd/elfcode.h:689  #3 0x0000000000408d91 in bfd\_check\_format\_matches (abfd=0x71c080, format=<optimized out>, matching=0x0)  at ../../bfd/format.c:228  #4 0x000000000040298f in strings\_object\_file (file=<optimized out>) at ../../binutils/strings.c:350  #5 strings\_file (file=<optimized out>) at ../../binutils/strings.c:380  #6 main (argc=2, argv=0x7fffffffe6d8) at ../../binutils/strings.c:298 |

#### bfd/elf.c

|  |
| --- |
| 744 for (i = 0; i < elf\_elfheader (abfd)->e\_phnum; i++, phdr++)  745 {  746 if (phdr->p\_paddr != 0)  747 break;  748 } |

#### Values

|  |
| --- |
| (gdb) p phdr  $11 = (Elf\_Internal\_Phdr \*) 0x0  (gdb) p phdr->p\_paddr  Cannot access memory at address 0x20 |

The pointer at phdr points to address 0x0, which is a null pointer dereference.