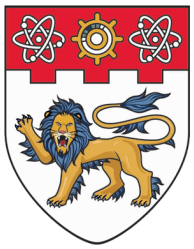


NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

CZ4062 Assignment

Fuzzing Report

Group 35

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

1 CONTENTS

2 Observations of Fuzzing Process 3
2.1 cxxfilt_1542666721080 3
2.1.1 Execution Speed 3
2.1.2 Paths Info 3
2.1.3 Abnormal Info 4
2.1.4 Findings of Mutation Operators 4
2.2 strings_1542666723047 5
2.2.1 Execution Speed 5
2.2.2 Paths Info 5
2.2.3 Abnormal Info 6
2.2.4 Findings of Mutation Operators 6
3 Crash Analysis 7
3.1 GNU c++filt 2.15 7
3.1.1 A null pointer dereference in function work_stuff_copy_to_from()(cplus-dem.c:1208) 7
3.1.2 A null pointer dereference in function cplus_demangle_type()(cp-demangle.c:1827) 7
3.1.3 A read invalid address in function d_name()(cp-demangle.c:1167) 8
3.1.4 A null pointer dereference in function do_type()(cplus-dem.c:3760) 9
3.1.5 A read invalid address in function d_substitution()(cp-demangle.c:2589) 10
3.2 GNU strings 2.15 11
3.2.1 A null pointer dereference in function bfd_section_from_shdr()(elf.c:1657) 11
3.2.2 A null pointer dereference in function bfd_section_from_shdr()(elf.c:1652) 11
3.2.3 A null pointer dereference in function bfd_hash_lookup()(hash.c:374) 12
3.2.4 A read invalid address in function bfd_alloc()(opncls.c:652) 12
3.2.5 A null pointer dereference in _bfd_elf_make_section_from_shdr bfd_alloc()(elf.c:746) 13

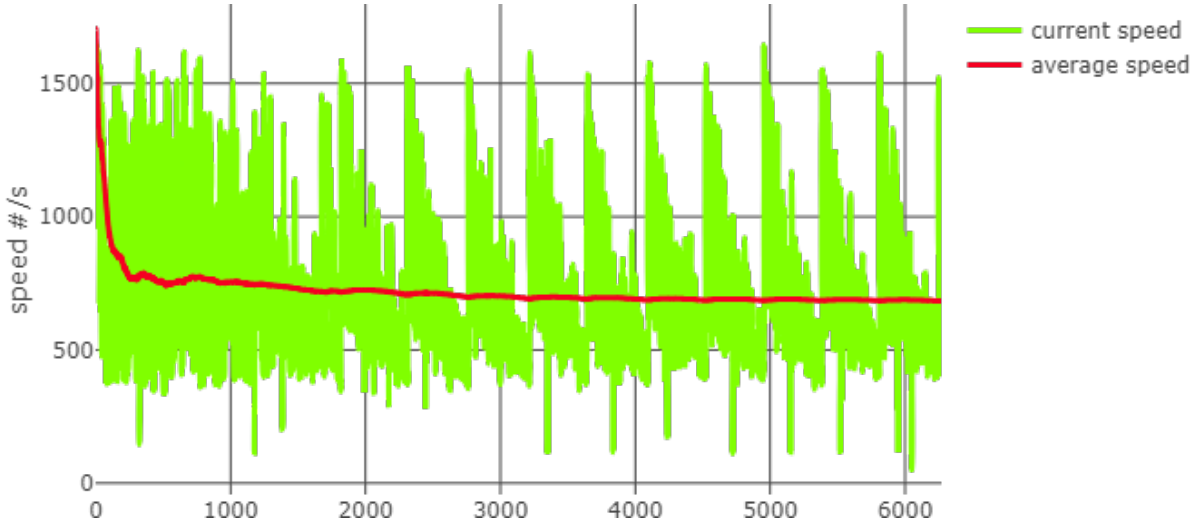
2 OBSERVATIONS OF FUZZING PROCESS

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.

2.1 CXXFILT_1542666721080

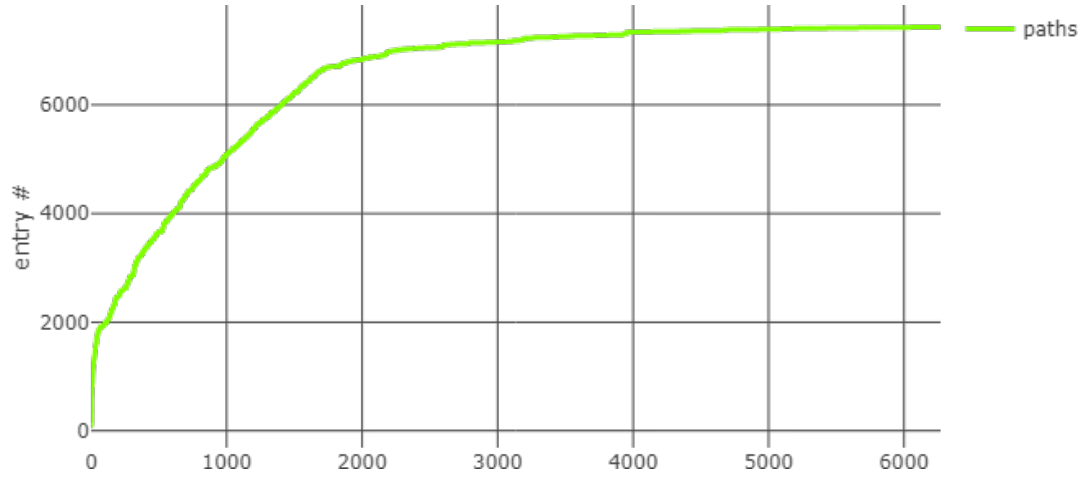
Fuzzing for GNU c++filt 2.15 started at 20/11/2018 6:32:01 and ended at 21/11/2018 8:39:30.

2.1.1 Execution Speed



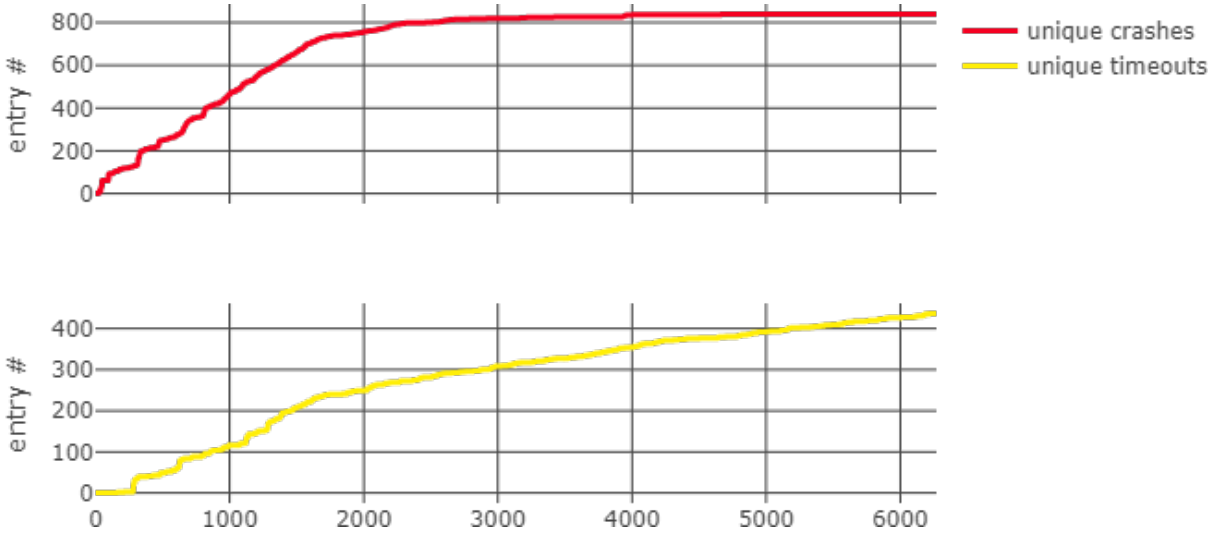
The average execution speed was around 700 per second, with a higher average speed of more than 1500 at the start and stabilizing at slightly less than 700. There is a clear pattern of the current speed throughout the fuzzing, showing the start and end of different stages.

2.1.2 Paths Info



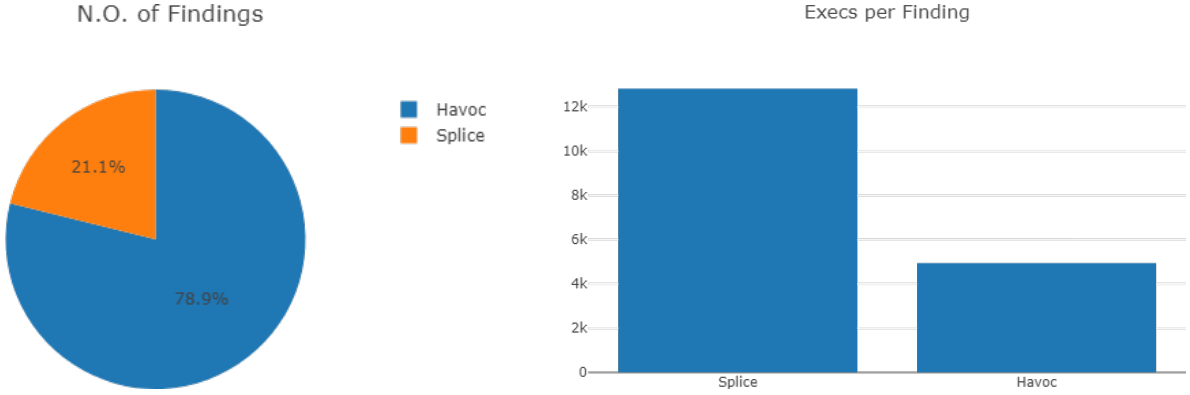
The fuzzing tool tested a total of 7429 paths, with lesser new paths found after about 8 hours.

2.1.3 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.

2.1.4 Findings of Mutation Operators

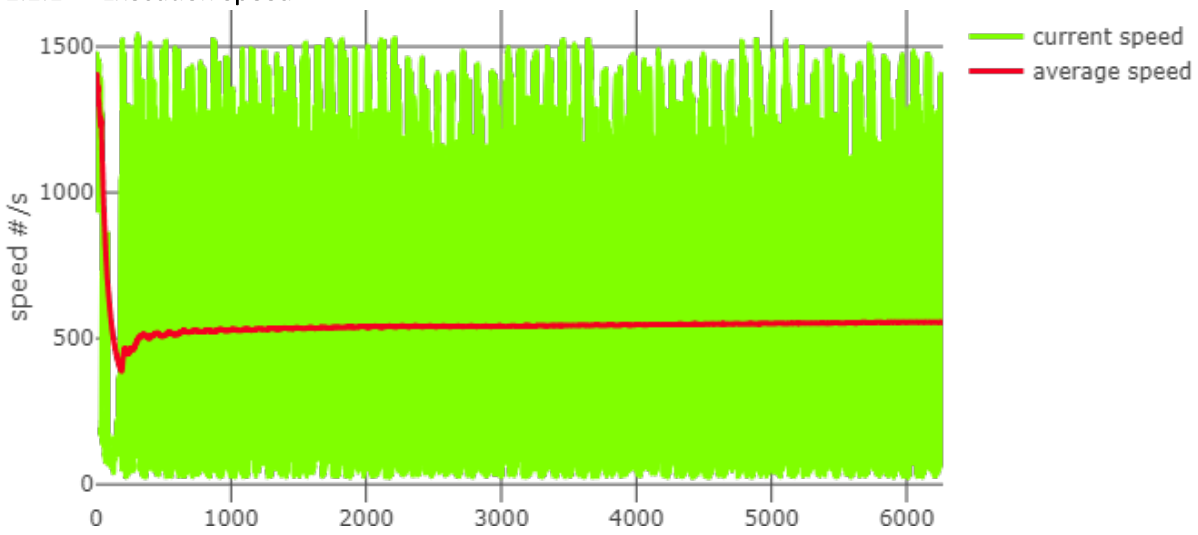


The Havoc mutation operator is more prevalent than Splice in the fuzzing of the program.

2.2 STRINGS_1542666723047

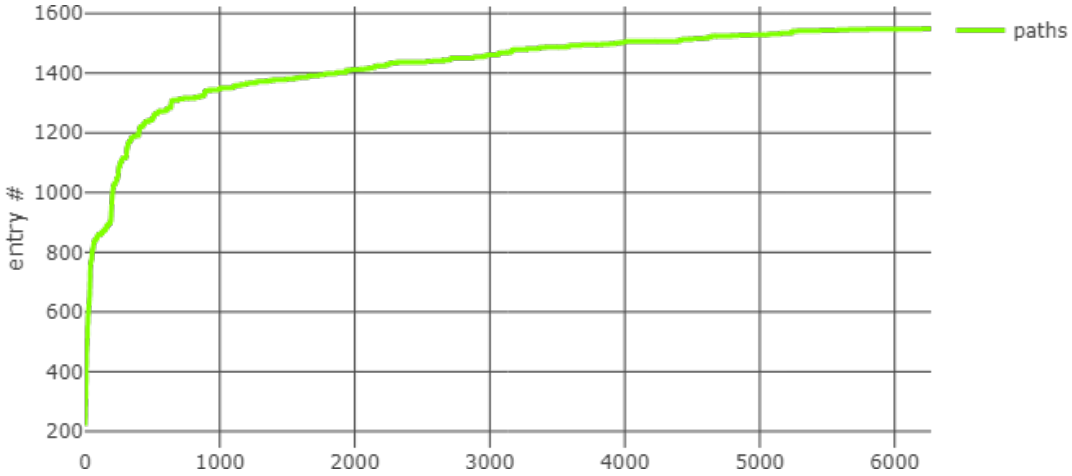
Fuzzing for GNU strings 2.15 started at 20/11/2018 6:32:03 and ended at 21/11/2018 8:39:31.

2.2.1 Execution Speed



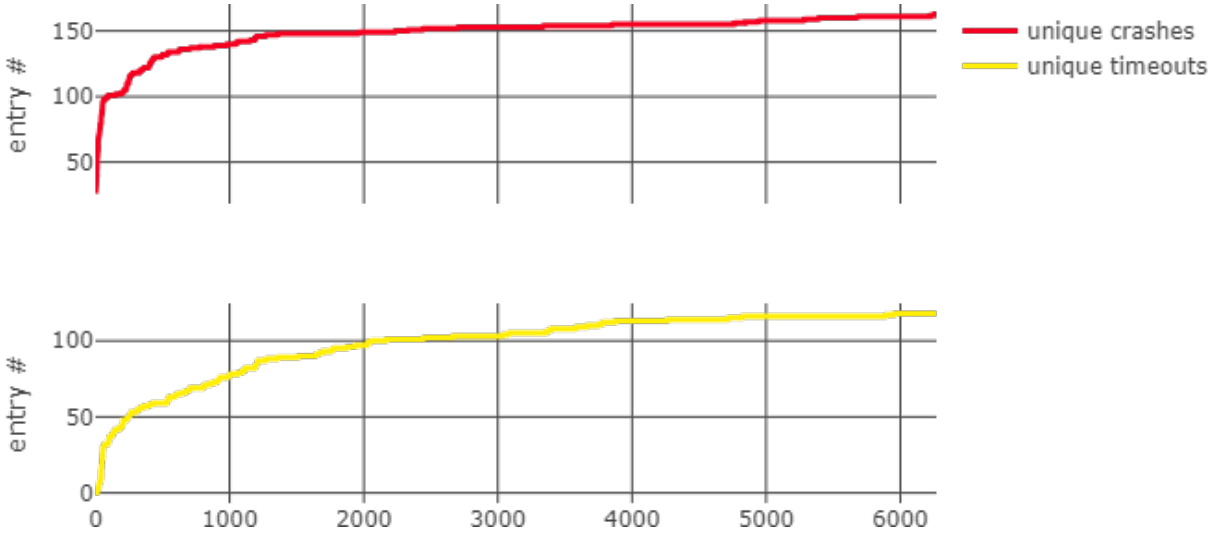
The average execution speed was around 550 per second, with a higher average speed of more than 1400 at the start and stabilizing at around 550.

2.2.2 Paths Info



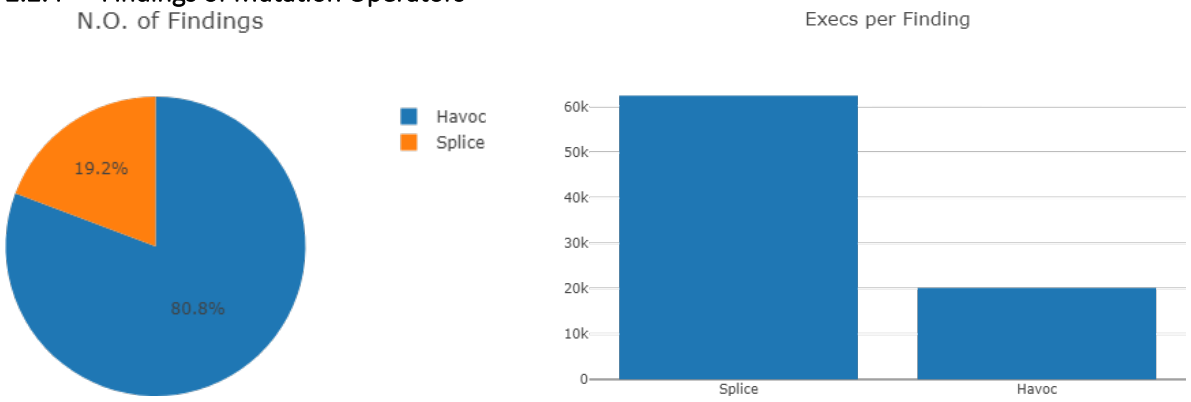
The fuzzing tool tested a total of 1549 paths, with lesser new paths found after about 4 hours.

2.2.3 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.

2.2.4 Findings of Mutation Operators



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

3 CRASH ANALYSIS

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

3.1 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.

3.1.1 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
```

3.1.1.1 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    }
```

3.1.1.2 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.

3.1.2 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
```

3.1.2.1 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;
```

3.1.2.2 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.

3.1.3 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
```

3.1.3.1 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')
```

3.1.3.2 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.

3.1.4 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
```

3.1.4.1 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;
```

3.1.4.2 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.

3.1.5 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
```

3.1.5.1 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    }
```

3.1.5.2 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.

3.2 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.

3.2.1 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
```

3.2.1.1 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);
```

3.2.1.2 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.

3.2.2 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
```

3.2.2.1 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);
```

3.2.2.2 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.

3.2.3 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  0x0000000000040daa4 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  0x00000000000477dbb 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
```

3.2.3.1 bfd/hash.c

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

3.2.3.2 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.

3.2.4 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
```

3.2.4.1 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);
```

3.2.4.2 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.

3.2.5 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
```

3.2.5.1 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      }
```

3.2.5.2 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.