Sorav Bansal <bsorav@gmail.com>

Bugs in memchr,memrchr,memccpy

Abhishek Rose <abhishek.rose@cse.iitd.ac.in> Wed, Apr 29, 2020 at 6:25 PM
To: dietlibc@fefe.de

Hi,

I am writing to report bugs in memchr, memrchr and memccpy functions of dietlibc.

The bugs are in the C implementation of the respective functions as located in lib/ and x86_64/ directories of dietlibc repository. All three bugs are related to missing type casts.

Please find detailed report below.

memchr() and memrchr()

Linux[0] and OpenBSD[1] manpages for memchr() and memrchr() specify that input argument `c' must be converted to `unsigned char' before performing the check. Dietlibc's implementation does not follow this and thus gives wrong output when `c' is greater than 256.

An example input is:

```
const char a[] = { 255, 128 };
if (!memchr(a, ~0x0, 2))
    printf("BUG!");
if (!memrchr(a, 128, 2))
    printf("BUG!");
```

memccpy()
----

memccpy() also misses the necessary type cast to `unsigned char' as specified in the OpenBSD manpage[2]. This bug is also present in the x86_64 implementation (x86_64/memccpy.c).

An example input is:

```
const char src[] = { 255, 128 };
char dst[2] = { 'A', 'B' };
memccpy(dst, src, 255, 2);
if (dst[1] != 'B')
  printf("BUG!");
```

0: https://linux.die.net/man/3/memchr
1: https://man.openbsd.org/memchr
2: https://man.openbsd.org/memccpy

Patch which adds the necessary type casts can be obtained from http://www.cse.iitd.ernet.in/~abhir/tmp/dietfixes.diff

Thanks,
Abhishek