Linux klibc(2.0.8)

https://git.kernel.org/pub/scm/libs/klibc/klibc.git

Overview

- The klibc distribution contains some of the necessary software to make early(linux) userspace useful.
- Both 'malloc' and 'calloc' implementations are vulenrable to integer overflow.

Vulnerable Code

- https://git.kernel.org/pub/scm/libs/klibc/klibc.git/tree/usr/klibc/calloc.c

- https://git.kernel.org/pub/scm/libs/klibc/klibc.git/tree/usr/klibc/malloc.c#n140

index : klibc/klibc.git

klibc main development tree

about summary refs log tree commit diff stats

path: root/usr/klibc/calloc.c

blob: 53dcc6b2f6bf63acd661c485141beb4fd635dd83 (plain)

```
1  /*
2   * calloc.c
3   */
4
5  #include <stdlib.h>
6  #include <string.h>
7
8  /* FIXME: This should look for multiplication overflow */
9
10 void *calloc(size_t nmemb, size_t size)
11 {
12         return zalloc(nmemb * size);
13 }
```

```c
void *malloc(size_t size)
{
        struct free_arena_header *fp;
        struct free_arena_header *pah;
        size_t fsize;

        if (size == 0)
                return NULL;

        /* Add the obligatory arena header, and round up */
        size = (size + 2 * sizeof(struct arena_header) - 1) & ARENA_SIZE_MASK;

        for (fp = __malloc_head.next_free; fp->a.type != ARENA_TYPE_HEAD;
             fp = fp->next_free) {
                if (fp->a.size >= size) {
                        /* Found fit -- allocate out of this block */
                        return __malloc_from_block(fp, size);
                }
        }
```