Dangling pointer (Use after free) A dangling pointer is a pointer that no longer points to a valid memory. This usually happens when the memory has been freed, but the address is kept inside the pointer.

```
#include <stdio.h>

#include <stdlib.h>

int main()

{

	//Allocate some memory on the heap

	int* ptr = malloc(sizeof(int));

	if(ptr == NULL)

	{

		return 0;

	}

	//Use the memory

	*ptr = 5;

	printf("%d\n", *ptr);

	free(ptr);

	//ptr is a dangling pointer now

	//The below code exhibits undefined behavior

	*ptr = 7; //Use after free

	printf("%d\n", *ptr);

}
```

Double free errors occur when free() is called more than once with the same memory address as an argument.

Mitigations... After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again.

```
free(ptr);

ptr=NULL;
```