Heap Pwn Cheat Sheet

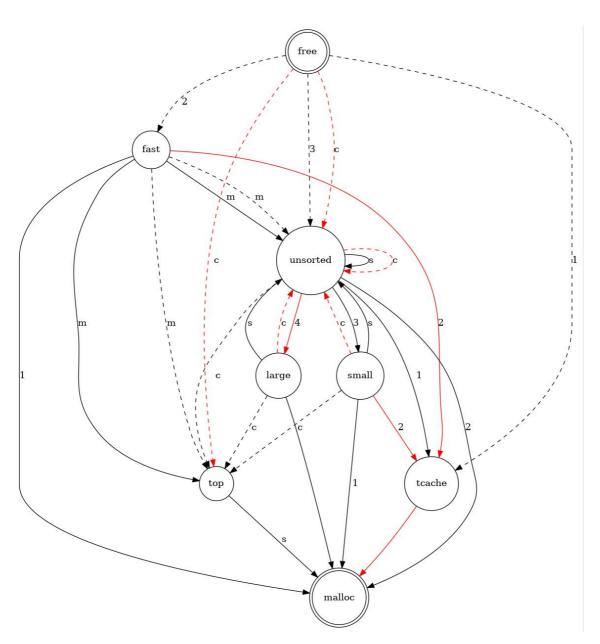
Glibc version

commit f94f6d8a3572840d3ba42ab9ace3ea522c99c0c2 (HEAD, tag: glibc-2.35)

Author: Carlos O'Donell <carlos@redhat.com>
Date: Thu Feb 3 00:27:54 2022 -0500

Create ChangeLog.old/ChangeLog.24.

Transition



symbol	description
arrow	malloc
dotted arrow	free
red arrow	weak path
С	(for back)word consolidate
m	malloc consolidate
S	split the chunk
1 ~ 4	priority (1: high, 4: low)

path	method	description
fast → malloc	malloc	1st chunk in fast bin when tcache is empty
fast → tcache	malloc	2nd ~ 8th chunks in fast bin when tcache is empty
unsorted → tcache	malloc	1st ~ 7th just-fit chunks in unsorted bin when tcache is empty
unsorted → malloc	malloc	8th just-fit chunk in unsorted bin when tcache is empty
small → malloc	malloc	1st chunk in small bin when tcache is empty
small → tcache	malloc	2nd ~ 8th chunks in unsorted bin when tcache is empty

Bins

	size	type
tcache	0x20 ~ 0x410	FILO
fast	0x20 ~ 0x80	FILO
unsorted	0x20 ~	FIFO
small	0x20 ~ 0x3f0	FIFO
large	0x400 ~	FIFO

Mmap

The following conditions are required for mmap to be called.

SIZE >= mp_.mmap_threshold && SIZE > main_arena->top.size however main_arena->top.size <= main_arena->system_mem

Therefore, if you reserve a chunk with a size larger than 0x21000, mmap will be called.

variable	intial value
mpmmap_threshold	0x20000

Double Free

1st \ nth	tcahe	fast	unsorted
tcache	X	X	Х
fast	0	0	-
unsorted [0x20 ~ 0x80]	0	0	X
unsorted [0x90 ~ 0x410]	0	-	Х
unsorted [0x420 ~]	-	-	Х
small [0x20 ~ 0x80]	0	0	X
small [0x90 ~ 0x3f0]	0	-	Х
large [0x400, 0x410]	0	-	Х
large [0x420 ~]	-	-	Х

Variables

variable	trigger	memo
malloc_hook	malloc	
free_hook	free	
realloc_hook	realloc	
after_morecore_hook	sbrk	
malloc_initialize_hook	malloc (at initialization)	
memalign_hook	aligned_alloc, memalign, posix_memalign, valloc	
_dl_open_hook	dlopen, dlsym	
_rtld_globaldl_ns[0]ns_loaded	_dl_fini	_rtld_global is in ld.so
global_max_fast		
.fini_array		
printf_arginfo_table, printf_function_table	printf	
stderr, fs:[0x30], vtable == _IO_cookie_jumps	_IO_file_sync	Whether stderr is in libc or exe depends on the code. debug and

		checkmalloc_assert
exit_funcs, fs:[0x30]	run_exit_handlers	
tls_dtor_list, fs:[0x30]	call_tls_dtors	

