

02.Heap Exploitation

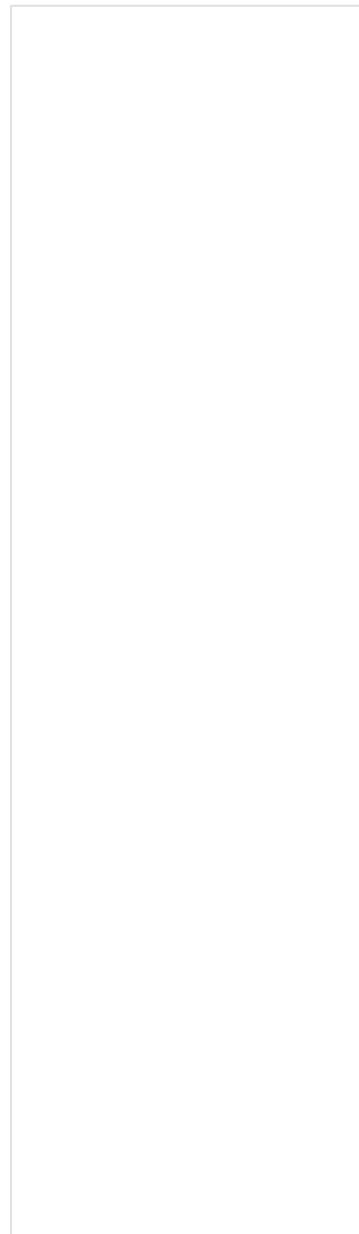
List

- [Heap Exploit](#)
- [Exploit table](#)

Heap Exploit

Description of Heap Exploitation.		
Title	Creator	Modified
House of Orange	Lazenc.a.0x0	Feb 04, 2020
Overlapping chunks	Lazenc.a.0x0	Jan 25, 2020
Poison null byte	Lazenc.a.0x0	Jan 25, 2020
unsorted bin attack	Lazenc.a.0x0	Jan 23, 2020
unsafe unlink	Lazenc.a.0x0	Oct 13, 2017
Overlapping chunks 2	Lazenc.a.0x0	Aug 09, 2017
House of einherjar	Lazenc.a.0x0	Aug 04, 2017
fastbin_dup_into_stack	Lazenc.a.0x0	Aug 04, 2017
fastbin_dup	Lazenc.a.0x0	Aug 04, 2017
first-fit(Use-After-Free)	Lazenc.a.0x0	Aug 04, 2017
The House of Lore	Lazenc.a.0x0	Aug 04, 2017
The House of Spirit	Lazenc.a.0x0	Aug 03, 2017
The House of Force	Lazenc.a.0x0	Aug 03, 2017

Exploit table



Exploit table

Exploits	Access area		Overwrite area					Free	
	Stack	Heap	Top chunk	F - size	F - bk	A - prev_size	A - size	Double Free	Free (Stack area)
First fit		○							
Fastbin dup		○						○	
Fastbindupinto stack	○					○		○	
Poison null byte		○		○ (1byte)					
Overlapping chunks		○		○					
Overlapping chunks 2		○		○					
House of einherjar	○					○	○		
The House of Force	○		○						
The House of Lore	○				○				
The House of Spirit	○								○
Unsorted bin attack	○				○				
Unsafe unlink	○					○	○		

