

# Double free[English]

## Description

- The double free bug can fix unexpected memory locations by calling free() twice.
- If an application calls free () twice with the same argument, the memory management data structure managed by the allocator is corrupted.
  - This corruption can cause the program to crash.
- And calling malloc () twice with the same argument may return the same pointer.
  - This could allow an attacker to control the data written to the double allocated memory.
  - In other words, buffer overflow attacks are possible.

## List

Title	Creator	Modified
<a href="#">fastbin_dup_into_stack[English]</a>	<a href="#">Lazenca.0x0</a>	Jan 03, 2021
<a href="#">fastbin_dup[English]</a>	<a href="#">Lazenca.0x0</a>	Jan 03, 2021



Unknown macro: 'html'