**CWE-416: Use After Free**

***定義 :*** 使用被釋放的記憶體空間，可能會導致程序崩潰、使用非預期數值、執行無關命令

***描述 :*** 這類問題有許多負面影響，輕則會使合法數據被破壞、重則可以重複執行任意指令。

常見的發生原因有兩種。1.導致程序出錯和發生異常的各種條件2.程序負責釋放記憶體空間的指令發生錯亂。有問題的記憶體空間被釋放後，如果又被合法地分配給了其他的指針，這塊記憶體位置釋放之前的指針又被重新使用並且指向了新分配的同一記憶體空間的某個區域，但該段數據已經發生變化，造成了釋放前指針對象的數據被破壞，這會導致未定義的程序行為。如果新分配的數據是例如C++中的class，那這塊堆上可能散落著各種函數指標，只要用shellcode的地址覆蓋其中一個函數指標，就能夠達成執行任意指令。

***相關問題 :***

1. CWE-1000 (Research Concepts)
2. CWE-1003 (Weaknesses for Simplified Mapping of Published Vulnerabilities)
3. CWE-699 (Development Concepts)

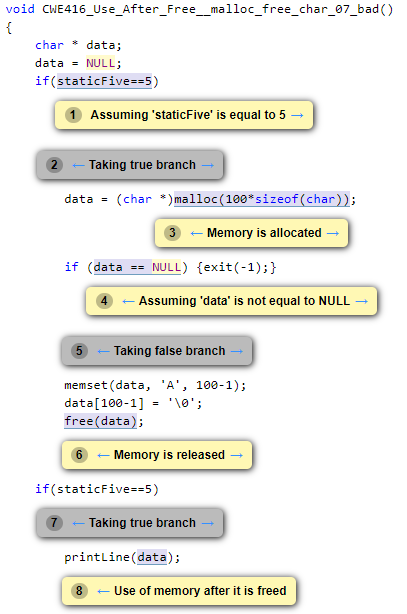
***可能會發生Use After Free的平台 :***

1. C
2. C++.

***Use After Free的常見後果 :***

1. 完整性 : 如果被釋放的問題記憶體空間被適當的分配且利用，會破壞合法數據 (Modify Memory)
2. 可用性 : 如果塊合併發生在使用被釋放的記憶體空間之後，則當將無效數據用作塊訊息時程序可能會崩潰 (DoS : Crash, Exit, Restart)
3. 保密性、完整性、可用性 : 如果在進行塊合併之前輸入了惡意數據，則可以利用write-what-where缺陷來執行任意代碼 (Execute Unauthorized Code or Commands)

***例子 :***



***漏洞成因 :***

條件式的判斷下導致後面在使用data時，data可能已經被釋放了