CVE-2017-6952

描述：Integer overflow in the cs\_winkernel\_malloc function in winkernel\_mm.c in Capstone 3.0.4 and earlier allows attackers to cause a denial of service (heap-based buffer overflow in a kernel driver) or possibly have unspecified other impact via a large value.

软件：Capstone 3.0.4

源码：windows/winkernel\_mm.c

出现位置： 66-78行

关键源码：

if (!ptr) {

return cs\_winkernel\_malloc(size);

}

new\_ptr = cs\_winkernel\_malloc(size);

if (!new\_ptr) {

return NULL;

}

current\_size = CONTAINING\_RECORD(ptr, CS\_WINKERNEL\_MEMBLOCK, data)->size;

smaller\_size = (current\_size < size) ? current\_size : size;

RtlCopyMemory(new\_ptr, ptr, smaller\_size); //buffer overflow

cs\_winkernel\_free(ptr);