Issue:

在BLCR restore過程中的do\_munmap會嘗試去unmap 一塊從0xffff0000開始的空間，我查證以後這裡是interrupt vector table起始位址，

但是在做do\_munmap時是在user space，所以無法使用kernel space的位址(大於0xc0000000)

Solution:

利用kernel裡exit\_mmap中處理special page的macro “arch\_exit\_mmap” 來完成unmap的動作，所以新增一個function 呼叫這個macro並且export出來

Side effect:

User mode之下可以unmap vector table

Modified File:

1. modify $linux\_src/include/linux/mm.h

                add:

                        extern void unmap\_vector(struct mm\_struct \*);

2. modify $linux\_src/mm/mmap.c

                add:

                        void unmap\_vector(struct mm\_struct \*mm)

                        {

                        arch\_exit\_mmap(mm);

                        }

                        EXPORT\_SYMBOL(unmap\_vector);

3.     modify $linux/arch/arm/mm/Kconfig

                add:

                        config HAS\_TLS\_REG

                bool

                depends on !TLS\_REG\_EMUL

                default y if SMP || CPU\_32v7