User critical data leaked : when an attacker attacks the hypervisor, the hypervisor is compromised. The attacker can modify the EPT of VM,

The information leakage attack method: the attacker obtains the permission of the virtual machine monitor through the virtual machine escape method, and can attack the virtual machine at the runtime, and on the other hand, can change the key data in the context switching process between the virtual machine and the host, including General purpose register information, privileged registers, etc. On the other hand, the attacker changes the address mapping of the EPT of the virtual machine, causing remapping attacks and double mapping attacks.

The specific implementation is as follows. For the modification of the key data of the context switch, the attacker can obtain the access authority and address of the VMCS structure in the victim virtual machine, change the information in the VMCS, HOST\_RIP, HOST\_CR3, GUEST\_CR3, GUEST\_CR0, EPTP, etc., and change the RIP register. And writing the rest of the malicious program address will cause a control flow hijacking attack. Changing the privilege register CR0 will turn off the DEP mechanism, and changing the register CR4 will turn off the SMEP mechanism.

For the second attack mode, the dual mapping attack: the attacker first breaks through a virtual machine, and then obtains the authority of the virtual machine monitor through the escape of the virtual machine, and maliciously accesses the VMCS structure to obtain the EPTP. The attack process is as shown in FIG. 1. In this way, the EPT addresses of the attacker virtual machine VM1 and the victim virtual machine VM2 are respectively obtained, and for a certain client virtual address A in VM2, the corresponding real physical address B, VM1 is obtained. The real physical address corresponding to the client virtual address C is D, and D is changed to B. Then VM1 can access the data of VM2. This process is called address double mapping.

Remapping attack: attacker virtual machine VM1 and victim virtual machine VM2. When VM2 uses some physical page A on the host, the page will be released after use. When A is released, VM1 will remap A. So that the virtual client address E points to the physical page A, then the VM1 can access the information on the VM2, causing information leakage.

信息泄露攻击方式：攻击者通过虚拟机逃逸的方法拿到虚拟机监控器的权限，可以对运行时的虚拟机进行攻击，一方面可以更改虚拟机与宿主机上下文切换过程中的关键数据，包括通用寄存器信息，特权寄存器等。另一方面攻击者更改虚拟机的EPT的地址映射，造成重映射攻击和双映射攻击。

具体实施如下，对于上下文切换的关键数据的修改，攻击者可以获取受害虚拟机中VMCS结构体的访问权限和地址，更改VMCS中的信息，HOST\_RIP,HOST\_CR3,GUEST\_CR3,GUEST\_CR0,EPTP等,更改RIP寄存器并写入其余恶意程序地址会造成控制流劫持攻击，更改特权寄存器CR0会关闭DEP机制，更改寄存器CR4会关闭SMEP机制。

针对第二种攻击方式，双映射攻击：攻击者首先攻破一个虚拟机，然后通过虚拟机逃逸的方式拿到虚拟机监控器的权限，恶意访问VMCS结构体获得EPTP。攻击过程如图1，通过这种方式分别获取到攻击者虚拟机VM1和受害虚拟机VM2的EPT地址，针对VM2中的某一客户机虚拟地址 A，获取到其对应的真实物理地址B，VM1客户机虚拟地址C对应的真实物理地址为D,将D改为B。那么VM1就可以访问到VM2的数据。这个过程叫做地址双映射。

重映射攻击：攻击者虚拟机VM1和受害者虚拟机VM2，当VM2使用某些在宿主机上的物理页A，使用完毕后，该页会被释放，当A释放后，VM1会重新映射A，使得虚拟客户机地址E指向物理页A，那么VM1可以访问VM2上的信息，造成信息泄露。