张帆组

漏洞编号：CVE-2013-2072

链接：<http://cve.scap.org.cn/CVE-2013-2072.html>

补丁：<http://seclists.org/oss-sec/2013/q2/att-353/xsa56.patch>

说明：

这是一个关于VCPU的漏洞。XenControl库中的xc\_vcpu\_setaffinity()函数存在缓冲区溢出漏洞。要研究这个漏洞，首先要了解XenControl库的功能，以及如何发挥作用，进行什么操作才能调用xc\_vcpu\_setaffinity()函数。

XenControl is a collection of tools designed to make it easy to run and use a Xen server for colo hosting purposes. Administrators can easily create new domUs, and allow the users to control them, while giving the users as little access to the system as possible.

姚牧阳组

漏洞编号：CVE-2013-1432

链接：<http://cve.scap.org.cn/CVE-2013-1432.html>

补丁：<http://seclists.org/oss-sec/2013/q2/att-618/xsa58-unstable.patch>

说明：

这是关于Xen内存管理的一个漏洞。大概是通过访问已经释放的内存页造成Crash。需要了解Xen内存管理的机制。

李曙华组

漏洞编号：CVE-2013-4329

链接：<http://cve.scap.org.cn/CVE-2013-4329.html>

补丁：<http://seclists.org/oss-sec/2013/q3/att-578/xsa61-4_2-unstable.patch>

说明：

这是libxenlight (libxl) 组件中存在的漏洞。当使用IOMMU（输入输出内存管理单元）时，在IOMMU设置完成之前，程序提供总线管理功能PCI passthrough设备的访问权限。本地HVM访客域可通过DMA指令利用该漏洞获得权限或造成拒绝服务。研究这个漏洞首先要了解libxl组件功能与工作机制。