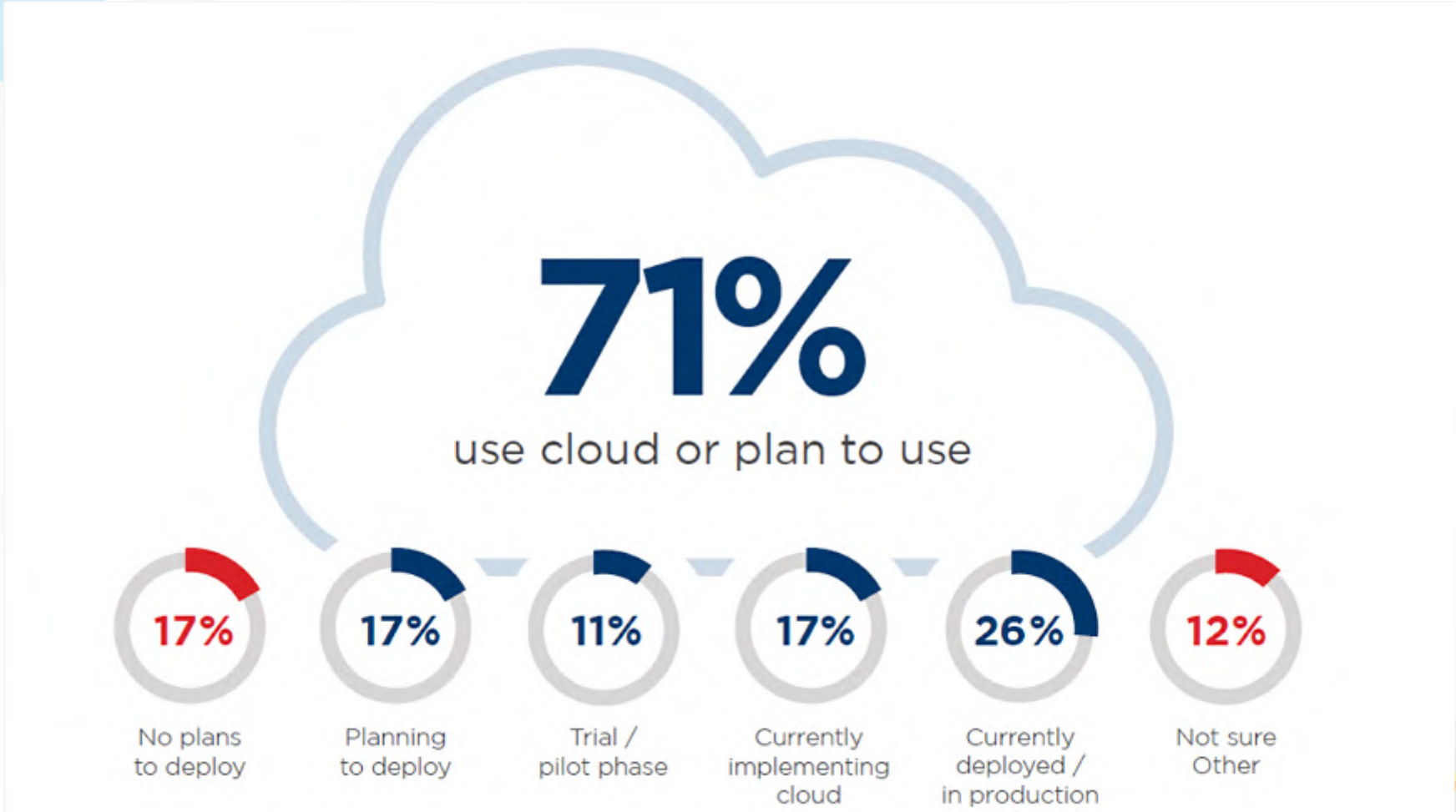
云平台安全架构剖析

主讲人：李纪峰

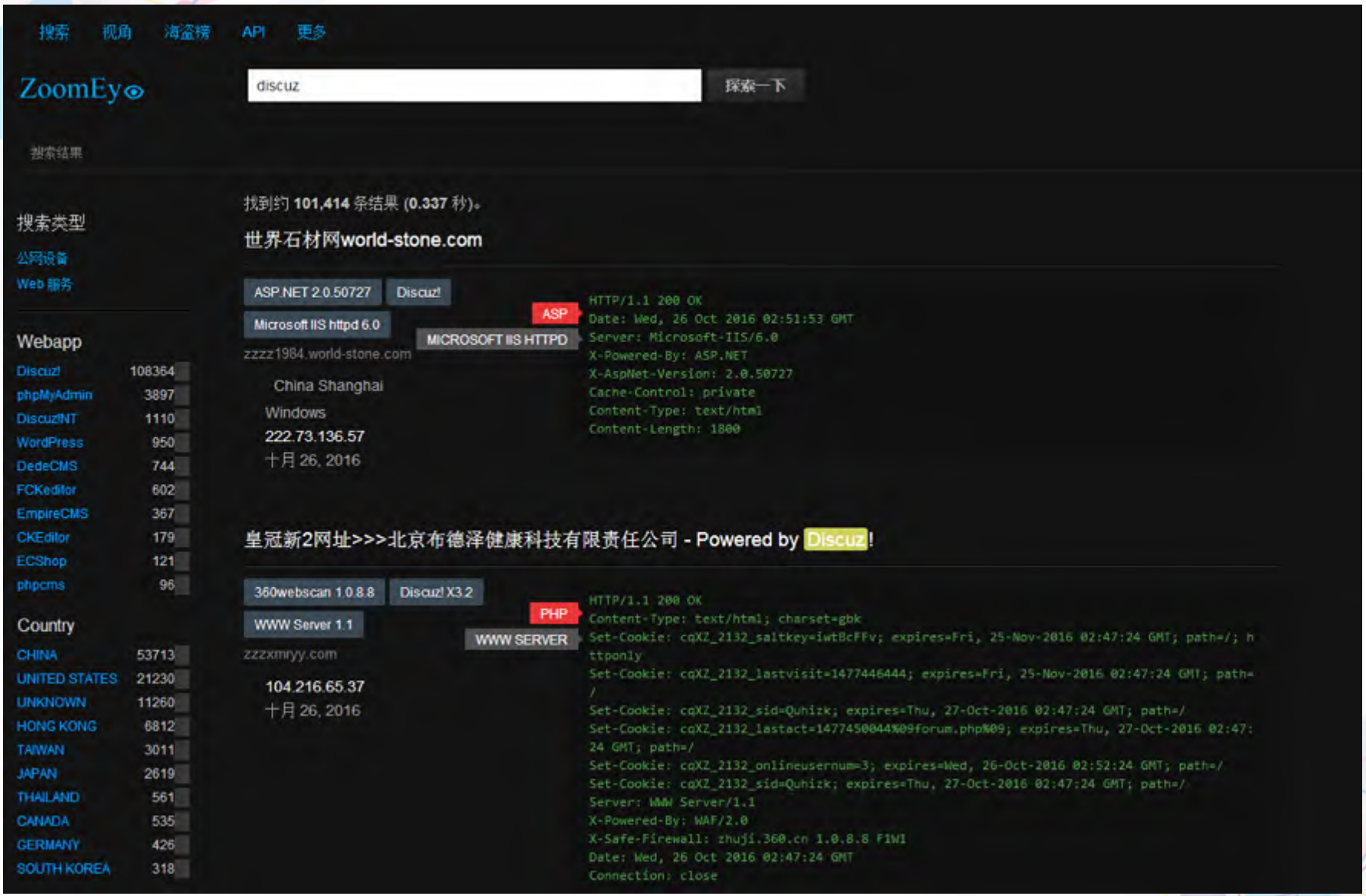
用户积极拥抱云计算


71%
use cloud or plan to use
17%
No plans to deploy
17%
Planning to deploy
11%
Trial / pilot phase
17%
Currently implementing cloud
26%
Currently deployed / in production
12%
Not sure Other

黑客攻击手段的新特点

- 基于大数据的攻击方式
- 攻击手段自动化
- 攻击形式多样(wifi,iot)

基于网站指纹的全网数据



自动化工具

3389全自动抓鸡工具- 百度
speed.m.baidu.com/pu=sz@1325_1325/s?st=111001...3389全自动抓鸡工具...
全自动Http3389抓鸡工具(rar文件.419.95KB.免1积分) 赞助商链接下载信息载入中... 下载说明: 1、推荐使用WinRAR v3.10 以上版本解压本站资源。 2、本站.

全自动3389端口检测.zip百度云资源- 百度网盘搜索- 叫我雷锋网
www.jiaowoleifeng.com/file_detail_s119302358591426963938641999 86.html
全自动3389端口检测.zip由百度云用户临时分享，网盘搜索，上叫我雷锋网.

全自动ftp扫描工具_HACK80
www.hack80.com/thread-4732-1-1.html
2013年8月6日 - 9 个帖子 - 9 个作者
print u" 欢迎使用FTP-webshell权限查找器sqlite-0.1——BY：落雪"sqlite0.1运行close_open.exe会自动注册成服务启动服务名称ftp-Server显示 ...

漏洞概要

关注数(279) 关注此漏洞

缺陷编号： **WooYun-2015-108465**

漏洞标题： 看我如何用wifi万能钥匙物理撸穿京东漫游内网

相关厂商： **京东商城**

漏洞作者： **杀器王子**

提交时间： 2015-04-16 21:15

公开时间： 2015-06-05 09:50

漏洞类型： 重要敏感信息泄露

危害等级： 高

自评Rank： 20

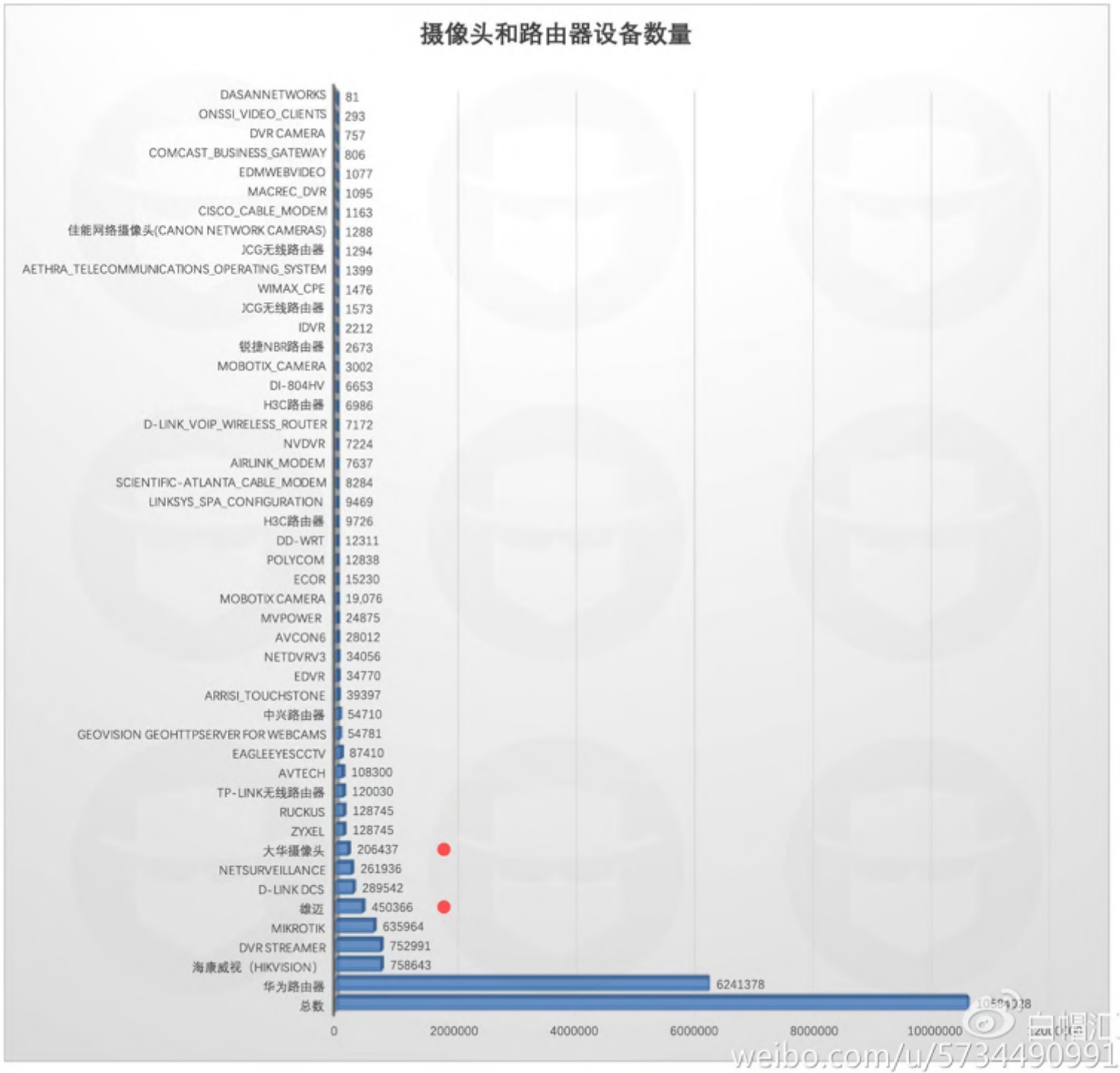
漏洞状态： 厂商已经确认

漏洞来源： **http://www.wooyun.org**，如有疑问或需要帮助请联系 help@wooyun.org

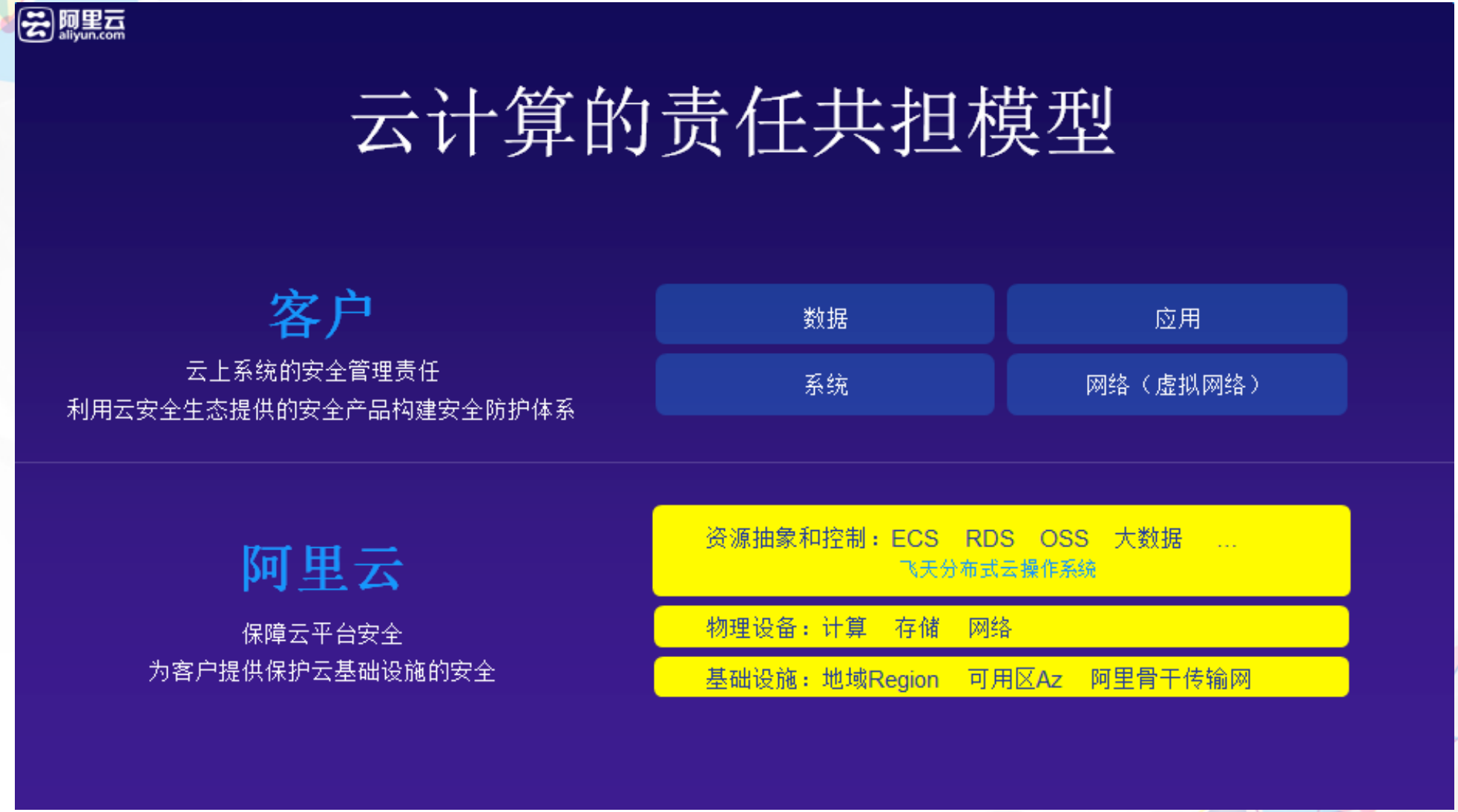
Tags标签： 无

分享漏洞： 分享到 0

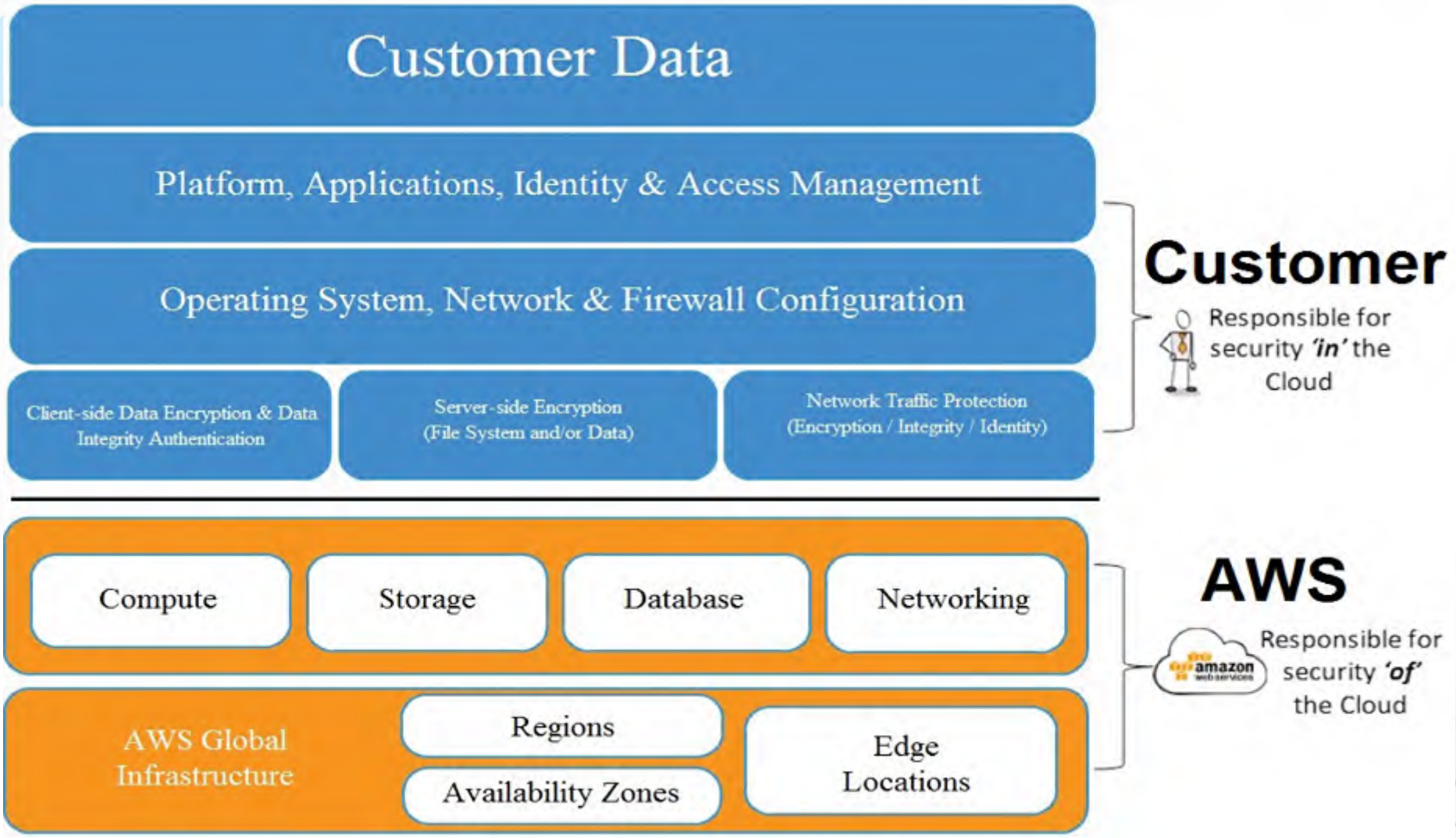
50人收藏 收藏



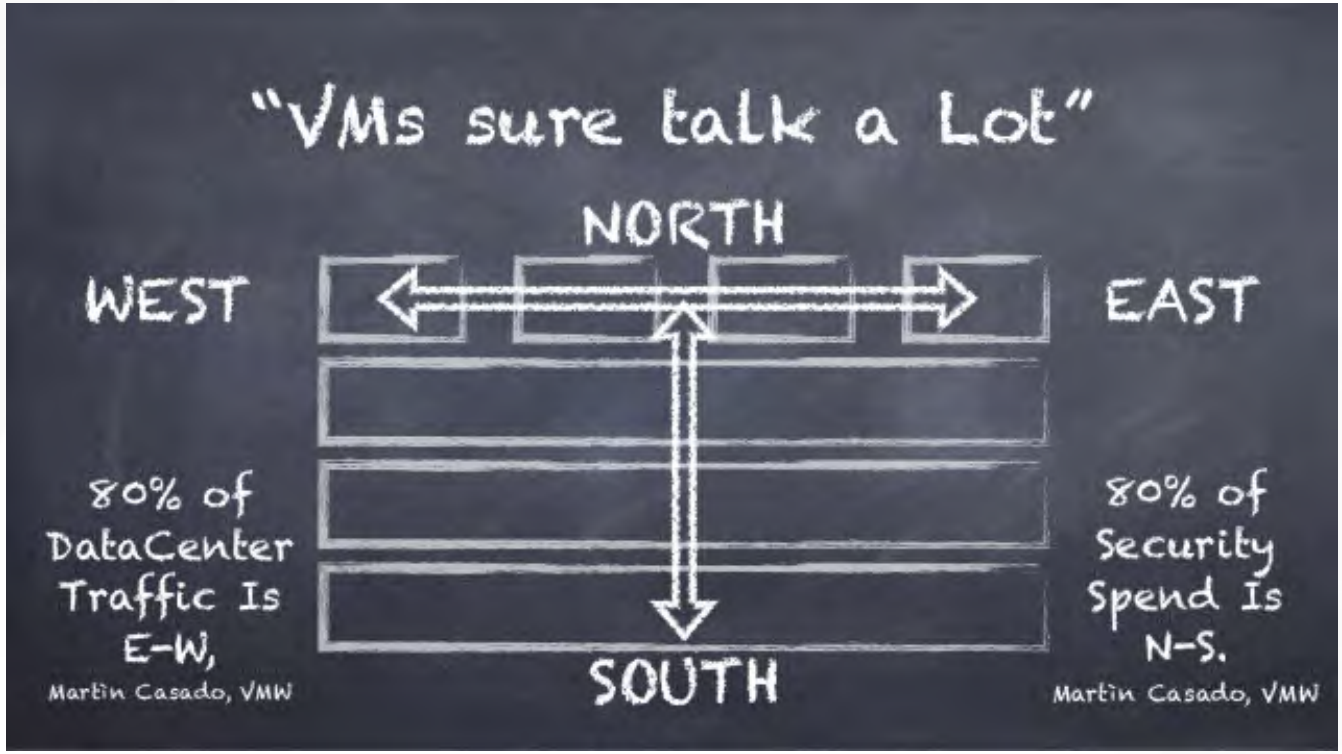
云服务商



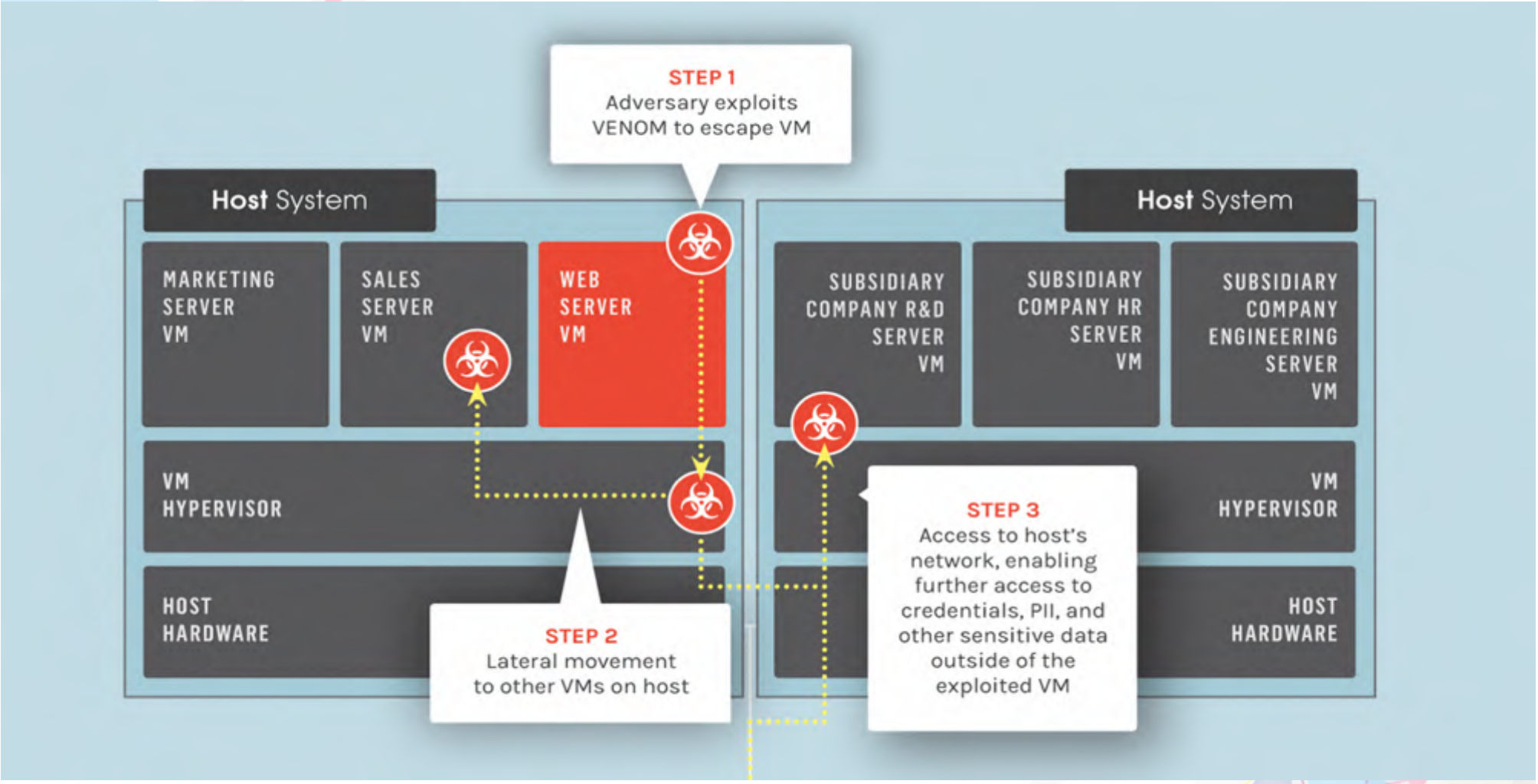
AWS责任共担模型


Customer Data
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side Data Encryption & Data Integrity Authentication
Server-side Encryption (File System and/or Data)
Network Traffic Protection (Encryption / Integrity / Identity)
Customer
Responsible for security 'in' the Cloud
Compute
Storage
Database
Networking
AWS Global Infrastructure
Regions
Availability Zones
Edge Locations
AWS
Responsible for security 'of' the Cloud

东西向流量不可见


"VMs sure talk a Lot"
NORTH
WEST
EAST
SOUTH
80% of DataCenter Traffic Is E-W,
Martin Casado, VMW
80% of Security Spend Is N-S.
Martin Casado, VMW

虚拟机逃逸


STEP 1
Adversary exploits
VENOM to escape VM
Host System
MARKETING SERVER VM
SALES SERVER VM
WEB SERVER VM
VM HYPERVISOR
HOST HARDWARE
STEP 2
Lateral movement
to other VMs on host
Host System
SUBSIDIARY COMPANY R&D SERVER VM
SUBSIDIARY COMPANY HR SERVER VM
SUBSIDIARY COMPANY ENGINEERING SERVER VM
VM HYPERVISOR
HOST HARDWARE
STEP 3
Access to host's network, enabling further access to credentials, PII, and other sensitive data outside of the exploited VM

SDN权限控制不当,攻击者可以获取ROOT权限

Cisco Security Advisory

Cisco Application Policy Infrastructure Controller Access Control Vulnerability

High

Advisory ID:	cisco-sa-20150722-apic
Published:	2015 July 22 16:00 GMT
Version1.0:	Final
CVSS Score:	Base - 8.5
Workarounds:	See below
Cisco Bug IDs:	CSCuu72094 CSCuv11991

CVE-2015-4235
CWE-264

Download CVRF
Download PDF
Email

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

Cisco Application Policy Infrastructure Controller Access Control Vulnerability

Subscribe to Cisco Security Notifications

Subscribe

Summary

A vulnerability in the cluster management configuration of the Cisco Application Policy Infrastructure Controller (APIC) and the Cisco Nexus 9000 Series ACI Mode Switch could allow an authenticated, remote attacker to access the APIC as the *root* user.

The vulnerability is due to improper implementation of access controls in the APIC filesystem. An attacker could exploit this vulnerability by accessing the cluster management configuration of the APIC. An exploit could allow the attacker to gain access to the APIC as the *root* user and perform *root*-level commands.

Cisco has released software updates that address this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150722-apic

Affected Products

Vulnerable Products

The following products are known to be affected by this vulnerability:

- Application Policy Infrastructure Controllers running software versions prior to 1.1(1j), 1.0(3o) and 1.0(4o).
- Cisco Nexus 9000 Series ACI Mode Switches running software versions prior to Release 11.1(1j) and 11.0(4o).

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability.

Details

The Cisco Application Policy Infrastructure Controller (Cisco APIC) is the unifying point of automation and management for the Application Centric Infrastructure (ACI) fabric. The Cisco APIC provides centralized access to all fabric information, optimizes the application lifecycle for scale and performance, and supports flexible application provisioning across physical and virtual resources.

A vulnerability in the cluster management configuration of the Cisco Application Policy Infrastructure Controller (APIC) and the Cisco Nexus 9000 Switch ACI Mode Switch could allow an authenticated, remote attacker to gain access to the APIC as the *root* user.

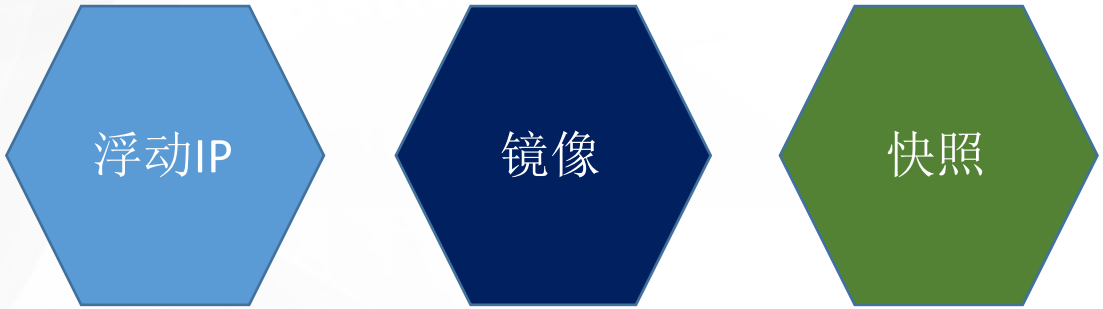
The vulnerability is due to improper implementation of access controls in the APIC filesystem. An attacker could exploit this vulnerability by accessing the cluster management configuration of the APIC. An exploit could allow the attacker to gain access to the APIC as the *root* user and perform *root*-level commands.

第三方组件给云平台带来的风险

漏洞概要

缺陷编号： **WooYun-2016-216049**
漏洞标题： 亚马逊云环境存在远程命令执行
相关厂商： **亚马逊AWS**
漏洞作者： **路人甲**
提交时间： 2016-06-04 13:57
修复时间： 2016-07-12 16:23
公开时间： 2016-07-12 16:23
漏洞类型： 命令执行
危害等级： 中
自评Rank： 10
漏洞状态： 厂商已经修复
漏洞来源： **http://www.wooyun.org**，如有疑问或需要帮助请联系 help@wooyun.org
Tags标签： 远程命令执行
分享漏洞： 分享到 0

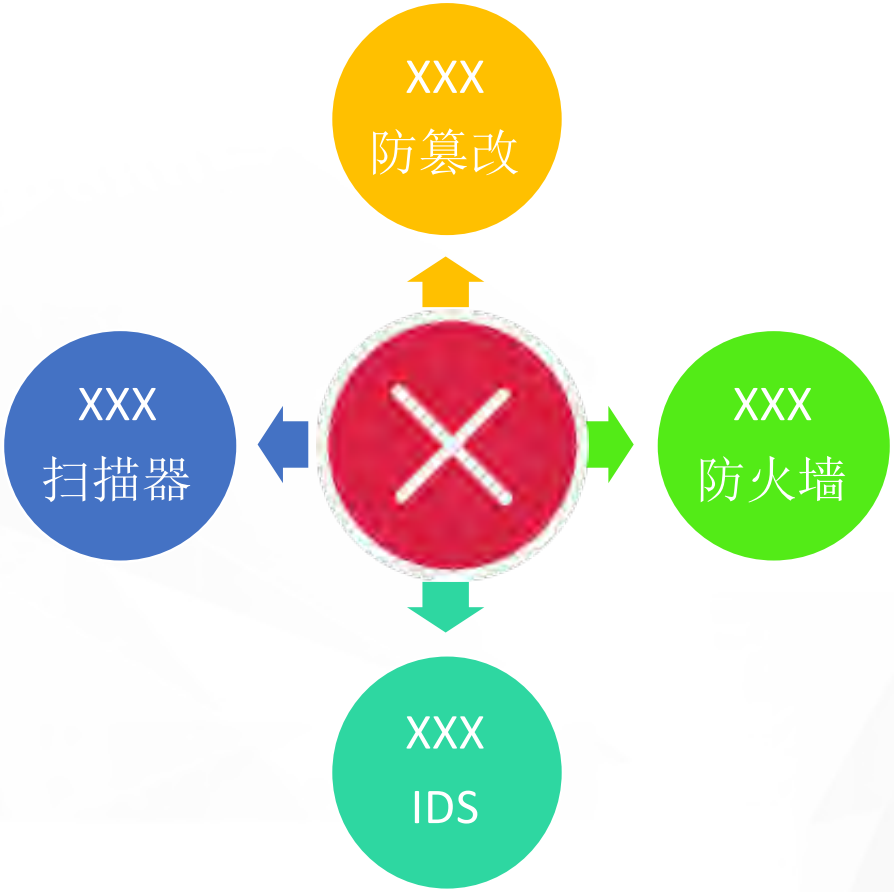
第三方组件给云平台带来的风险



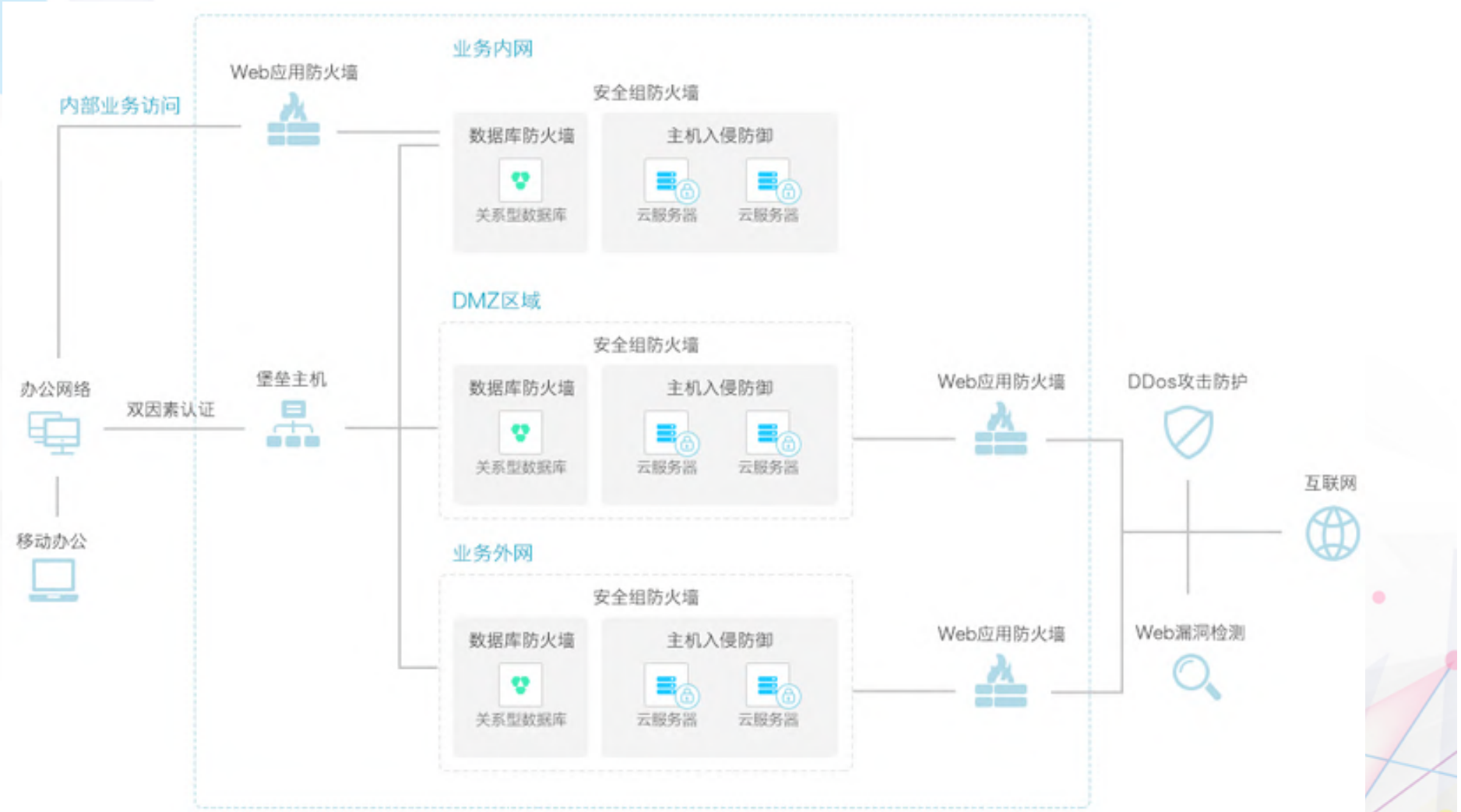
OPENSTACK 六年间共披露了 130 个漏洞,过去一年就有 21 个漏洞,其中高危 3 个

大项	分类	漏洞数量
组件安全	Nova	26
	Neutron	9
	Keystone	22
	Glance	16
	Swift	10
	Horizon	9
	Cinder	4
基础架构安全	Restful API	13
	TLS	2
	DoS	10
传统安全	XSS	8

传统厂商互相封闭



云安全网络架构


业务内网
Web应用防火墙
内部业务访问
安全组防火墙
数据库防火墙
主机入侵防御
关系型数据库
云服务器
云服务器
DMZ区域
安全组防火墙
数据库防火墙
主机入侵防御
关系型数据库
云服务器
云服务器
办公网络
双因素认证
堡垒主机
移动办公
Web应用防火墙
DDos攻击防护
互联网
业务外网
安全组防火墙
数据库防火墙
主机入侵防御
关系型数据库
云服务器
云服务器
Web应用防火墙
Web漏洞检测

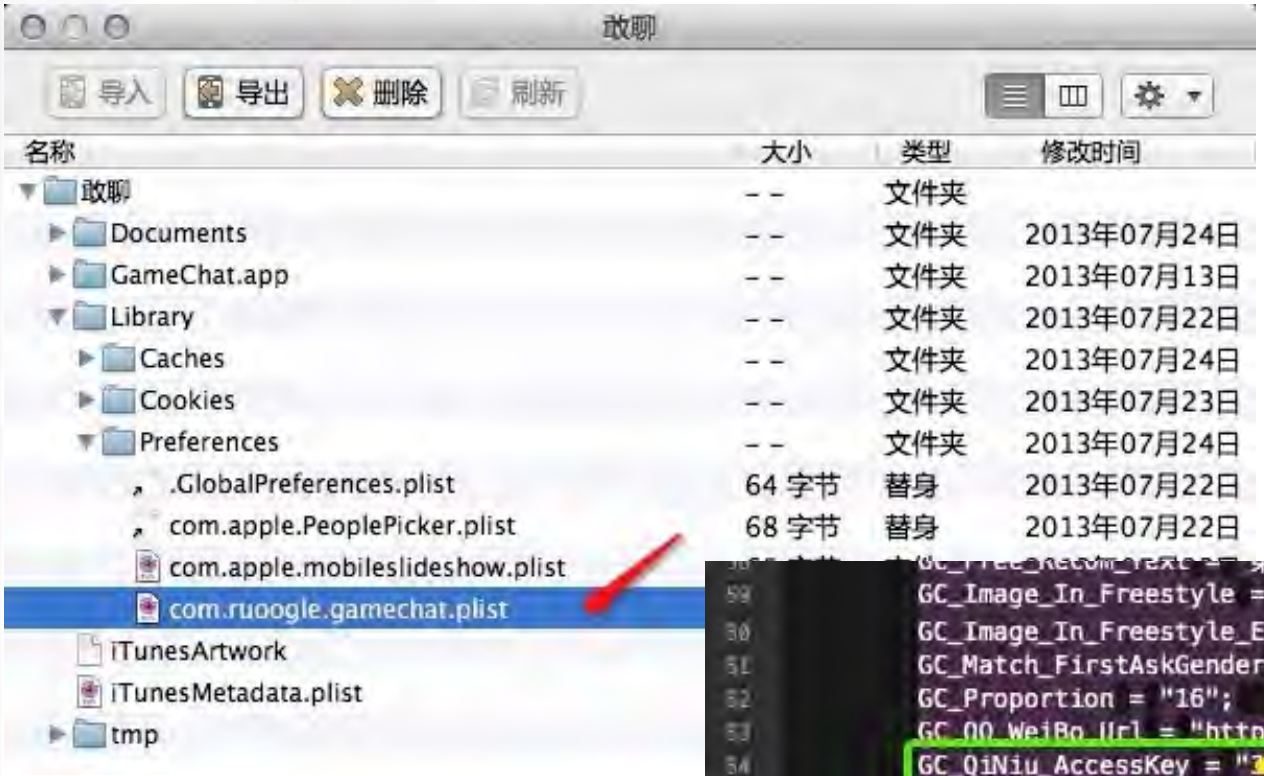
构建立体数据安全的防御体系

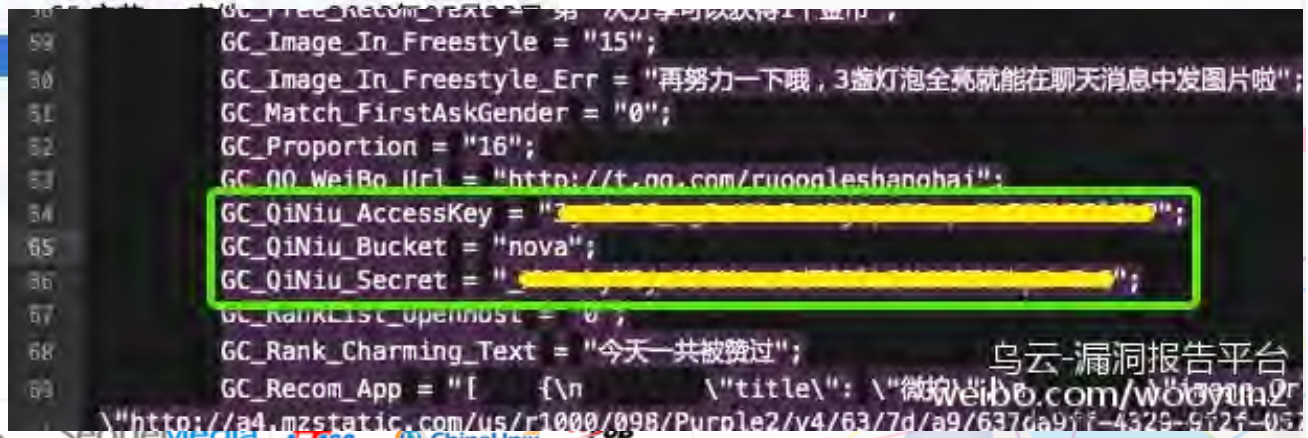
- 应用层安全(部署web防火墙,数据库防火墙,数据库审计)
- 主机层安全(密码10位以上, 只分配内网IP，只允许白名单访问,最小化权限)
- 传输层安全(数据传输SSL加密)
- 存储层安全(核心数据加密)
- 容灾备份(每周2次全量备份，每天增量备份,核心数据保留1年,每月检查一次备份的有效性)
- 数据安全管理（运维安全,开发安全,数据分级)

RUBYCHINA主站及RUBYTAOBAO数据库和配置文件泄漏

```
24  ActiveRecord::Migration.verbose = false
25  ActiveRecord::Base.raise_in_transactional_callbacks = true
26
27  # 测试的时候需要修改这个地方
28  ALIYUN_ACCESS_ID = "osOX[redacted]s3"
29  ALIYUN_ACCESS_KEY = 'm2L[redacted]
30  ALIYUN_BUCKET = "bi[redacted]-dev"
31
32  CarrierWave.configure do |config|
```

“敢聊”用户照片及语音泄漏等隐私泄露





数据分级


10.0.0.55/index.html?http://www.hao123.com/?tn=12092018_15_hao_pg
北京理工大學
校园网认证系统
上网不涉密 涉密不上网
用户登录
新用户注册
客户端下载
自服务登录
用户名:
密码:
记住密码
登录
注销
温馨提示:
系统公告
有主动进行"注销"或"断开连接"的操作。因为我校的有线和无线网络都是自动分配IP地址，设备关机或离开后释放出来的IP地址可能会分配给新接入的其他用户。如果登录后没有做退出操作，那么该IP无需登录便可继续访问外网资源，产生的流量将会记录在与该IP关联的用户帐号上。
为此，请广大用户在上网认证后，如果不再使用网络，请养成主动退出网络的习惯：使用页面登录的用户，在登录页面执行"注销"操作；使用WINDOWS客户端登录的用户，在操作面板上选择"断开连接"操作；使用命令行登录的用户，执行LOGOUT命令；或者在自服务中我的状态里，选择"下线"，确保自己的用户帐号与IP断开，不再产生流量。
祝大家使用网络愉快!
网络服务中心
2014年6月9日

构建应用 安全纵深防御体系

- 开发人员安全培训(安全意识，安全编码规范)
- 持续性风险检测(web漏洞扫描,webshell扫描,篡改检测)
- 漏洞管理(上线前安全测试，加入补天SRC,0day管理)
- 部署Web应用防火墙
- 建立DDOS防御机制
- 应用安全审计

编码规范

2012 年 8 月

OWASP
The Open Web Application Security Project

OWASP 安全编码规范
快速参考指南

构建主机安全立体防御体系

- 最小化系统(单一角色原则，精简原则)
- 恶意代码防范(病毒、木马查杀)
- 漏洞补丁管理
- 主机入侵检测
- 主机加固(账号服务加固,系统服务加固,内核参数加固)
- 账号安全(防止暴力破解，异地登陆提醒)

360云安全管理平台

纵深防御、一站式解决方案

Security is a process

THANKS

SequeMedia 盛拓传媒 | ChinaUnix | ITPUB