GOPS 2016 Shenzhen

GOPS

2016 全球运维大会 深圳站

会议时间：3月25日-3月26日

会议地点：深圳 • 南山区 圣淘沙酒店(翡翠店)

主办单位：开放运维联盟 OOPSA Open OPS Alliance　高效运维社区 GreatOPS Community

指导单位：数据中心联盟 Data Center Alliance

协办单位：中国新一代IT产业推进联盟

GOPS2016 Shenzhen

GOPS

2016 全球运维大会 深圳站

高效安全运维服务平台的构建

章华鹏，乌云

关于我

- 独立思考的白帽子黑客，boooooom
- 前百度高级安全工程师
- 乌云，唐朝安全巡航产品负责人
- http://www.tangscan.com

企业安全的核心是什么

- 数据
- 如何保护数据的安全

如何保护数据的安全

- 数据在哪？
- 业务是数据的载体
- 企业IT资产是业务的载体
- 运维的核心对象即是企业IT资产
- 那么安全运维应该是运维的一项基础要求

如何高效的进行安全运维

- 了解问题：运维安全问题在哪？
- 明确核心目标
- 安全运维服务平台的构建

运维安全问题在哪？

- 网络
- 系统&服务
- 应用配置

网络

- 内外网隔离
- 网络边界安全
- 黑客漫游内网

典型网络边界问题

- 服务器同时部署内网&外网业务
- SSRF 漏洞
- IDC与办公网互通
- 未授权代理配置
- IDC服务器被入侵

缺陷编号： **WooYun-2013-26212**

漏洞标题： 我是如何漫游腾讯内部网络的

相关厂商： **腾讯**

漏洞作者： **结界师**

提交时间： 2013-06-18 13:35

公开时间： 2013-08-02 13:36

漏洞类型： 设计缺陷/逻辑错误

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**


首页 厂商列表 白帽子 乌云榜 团队 漏洞列表 提交漏洞 乌云招聘 乌云集市
当前位置：WooYun >> 搜索结果
搜索关键字： 内网漫游 (共 413 条纪录) 将未公开漏洞纳入搜索结果
第一视频集团内网漫游(60台Linux已root/780w游戏用户/获取www主站权限)
第一视频集团旗下v1.cn，中国足彩网，彩票365，第一游戏网 奇虎360某工程师中枪...1.入口 http://mail.v1
邮箱进行fuzzing，得到弱口令用户，然后登录邮箱脱出所有用户名再一次进行fuzz，得到如下结果 code 区
jie@123 zhangjiaquan zhangjiaquan@123 jinlijing ji...
提交日期：2016-01-02 作者：hecate
新浪员工账户体系控制不严可入内网漫游（可OA系统ganji商渠道系统防垃圾系
新浪乐居 新年快乐...http://broker2.esf.leju.com/statnew/agentreal 若密码 登陆 大量经纪人信息 客户信息
信息 店铺统计信息 ...修改密码 若密码 新年快乐2
提交日期：2016-01-02 作者：雷

系统&服务

- 系统基础依赖组件漏洞
- 基础服务漏洞

典型系统&服务问题

- Openssl 心脏滴血
- Shellshock bash 远程命令执行
- Redis 未授权访问
- 各种服务默认账号密码

漏洞概要

缺陷编号： **WooYun-2014-55932**

漏洞标题： 淘宝主站运维不当导致可以登录随机用户并且获取服务器敏感信息

相关厂商： **淘宝网**

漏洞作者： **insight-labs**

提交时间： 2014-04-08 15:36

公开时间： 2014-05-23 15:37

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： 内部源码泄漏


WooYun.org
加关注
16.7万
首页
厂商列表
白帽子
乌云榜
团队
漏洞列表
提交漏洞
乌云招聘
当前位置：WooYun >> 搜索结果
搜索关键字： redis (共 396 条纪录)
将未公开漏洞纳入搜索结果
e袋洗elaticsearch未授权访问可访问全部文件
“e袋洗”是荣昌服务2013年11月28日感恩节当天推出的互联网洗衣...redis:x:497:498:Redis Ser
口不要随便开放
提交日期： 2015-07-28 作者： silence-white
共 396 条记录
新浪某服务器Redis未授权访问
RT...ip:115.182.85.224 新浪公司微游戏 Redis未授权访问 ...ip:115.182.85.224 新浪公司微游戏

应用配置

- 应用上线流程导致的问题
  - Svn信息泄露
  - Git 信息泄露
- 各种配置不当导致安全风险
  - 任意系统文件遍历
  - 列目录
  - 数据库&源码备份
  - 。。。

一汽丰田从SVN+源码信息泄漏到WWW主站数据库沦陷（ROOT权限/跨库

一汽丰田没注册厂商，就直接提交给一汽了，反正不管一汽丰田还是...SVN信息泄漏： http://aaa.ftm

.ftms.com.cn/rav4_wljd/.svn/entries 里面没有敏感信息，然并卵 有利用价值的是源码泄漏： http://ev

漏洞存在后……给这个图片打个马赛克 泄露了数据库信息，然而mysql并不能外连 于是……送温暖的

提交日期：2016-01-17 作者：岛云首席鉴黄师

51TALK（zabbix命令执行）SVN泄漏主站源码某处撞库

，，，，，，，，，，，，，，，，好贵的英语学费。... http://116....SVN http://pms.51talk.com/.svn/en

主站相似度极高。 ... 我就不shell了毕竟权限是zabbix还要提权 看一个有意思的文件wj_user.php coc

*/ include 'init.php'; //判断ip来源 $arr_return = array(); $ip = getClientIP(); if (!in_...

提交日期：2016-01-17 作者：陆由乙

东风本田汽车WWW主站存在SQL注入+SVN信息泄漏（跨库查询/数万购车

6 7月份买车 就买日系的 看你们和广本谁降价厉害了...注入点：ht...SVN信息泄漏： http://www.dong

据本人已完全删除

问题这么多，怎么办？

解决方案

安全运维服务平台

基础资产管理

安全事件预警

持续风险监测

持续风险管理

企业资产管理

- 首先要明确目标
  - 安全的核心是数据，IT资产
  - 运维的基础核心也是IT资产
  - 首先明确保护的目标即企业资产

关于资产的定义

- 域名
- IP
- 服务
- 网站
- 应用

基础资产发现

- 内部资产梳理
  - 机器上线流程控制
- 外部
  - 子域名暴力枚举
  - DNS 数据
  - 第三方数据接口&爬虫&域传送漏洞

如何高效的做好资产管理

- 指纹识别技术
  - 服务指纹识别
    - Nmap
    - SSH，mysql，redis…
  - 应用指纹识别
    - 应用指纹:cookie,文件MD5,html…
    - Blog，cms，OA…

风险检测

- 基础服务风险检测
  - 服务通用漏洞检测
  - 配置风险
- 应用风险
  - 自研应用风险检测
  - 第三方应用通用漏洞检测

如何高效

- 核心是检测策略
  - 安全问题是随着技术的不断变化而变化的
- 依托于开放平台&社区
  - 基础引擎架构支撑+社区参与建设
  - 社区运营（激励策略）
  - 检测策略的持续更新

安全事件处理

- 安全事件处理
  - 通告
  - 处理方案建议
  - 复查
- 全球威胁情报预警
  - 威胁情报来源

如何高效

- 安全事件处理
  - 平台API对接产品生命周期管理流程
  - 安全专家全流程跟进服务
- 全球威胁情报收集
  - 威胁是动态的
  - 依托于社区&开放平台

持续风险管理

- 周期性检测
  - 对应业务迭代更新频率
  - 防止回滚导致修复失效
- 风险管理
  - 风险趋势分析
  - 指导基础安全建设

如何高效？

- 自动周期安全巡检
  - 周期可配置
- 自动化分析报告
  - 自定义策略导出
  - 自动生成周报&月报&年报

谢谢