京东
JD.COM
多·快·好·省

浅谈互联网应急响应中心建设与运营

ID：Himan

京东商城-安全管理部

李学庆

京东安全第一人

Weibo：http://weibo.com/himan0

负责：安全测试中心、安全响应中心

让购物变得简单、快乐！

国内安全响应中心

JD.COM 京东

安全

响应

中心

安全响应中心建设初衷：

1、投递无门的企业入口

2、兑换等价的安全漏洞

3、回收未知的外界风险

4、招纳贤人的专业平台


梳理业务
定义级别
评分标准
响应流程
业务自检

梳理业务：

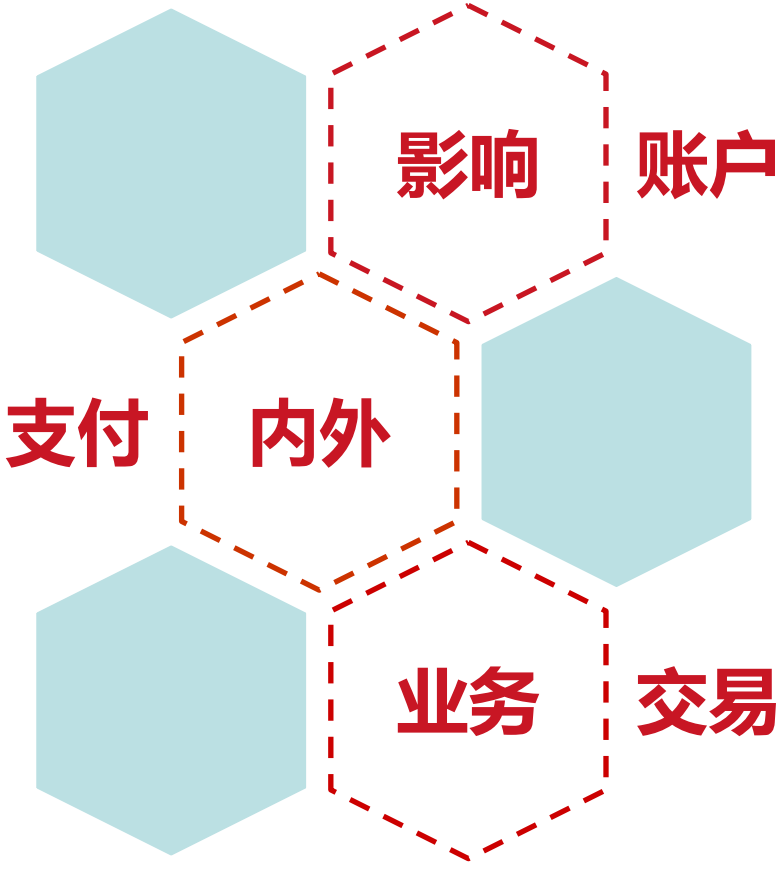
1、梳理所有域名列表---内外、部门、负责人

2、梳理所有IP列表---内外、端口、部门、负责人

3、确定安全接口人员---业务线划分

4、确定业务安全接口人员---业务部门接口人

定义级别：



评分标准：

2015年 JSRC积分进行第三次更新改革！

【第三次新积分革命】：

京东安全响应中心评分标准升级至“新积分”标准

JSRC 积分改革-评分

JD.COM 京东

严重	分值9~10分	【系数 90】	4050 ~ 4500元
高危	分值6~8 分	【系数 45】	1350 ~ 1800元
中危	分值3~5 分	【系数 12 】	180 ~ 300 元
低危	分值1~2 分	【系数 6 】	30 ~ 60 元

新积分

漏洞危害数 * 系数 = 最终积分

例：严重漏洞 10 分 系数 90 =900 积分=4500元*

新积分标准duang~~~duang~~~ duang~~~

目 录

响应流程：

研发系统研发管理体系（JDMS） / 研发系统研发管理体系（JDMS） / 京东安全管理体系（JDSec）

安全事件处理及应急响应规范v1 0

Created by 杨婷婷 on 十二月 30, 2014

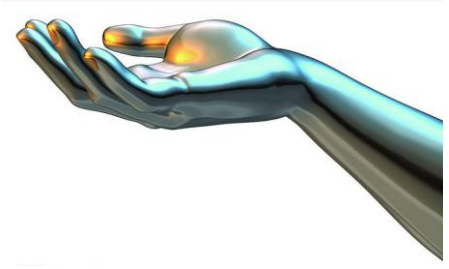
版本号：V1.0
受控状态：受控

北京京东信息技术有限公司
安全事件处理及应急响应规范

- **漏洞名称：** [redacted]
- **影响范围：** [redacted]
- **发现时间：2015.5.12**
- **漏洞安全联系人：**
- **漏洞描述：**
  [redacted]
- **漏洞证明：**
  [redacted]

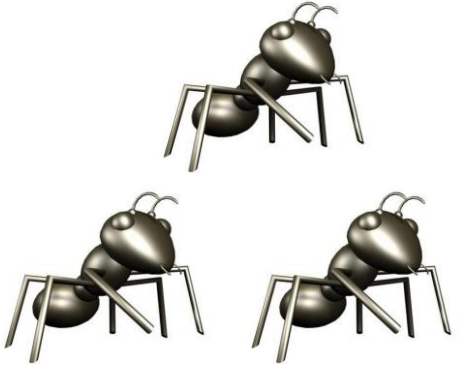
业务自检：

手工排查



工具检测

众测项目



安全响应中心运营

JD.COM 京东

7*24小时

JSRC

安全响应中心运营-及时沟通

- 第一时间联系白帽子
- 统一官方语言回复模式
- 有异议达成一致再评分
- 定期举办线上线下交流

安全响应中心运营-及时改进

JD.COM 京东

编号	漏洞名	漏洞大类型 【全部】	漏洞小类型 【全部】	漏洞等级	状态 【全部】	获得积分	提交者	提交时间	Remedy号	来源	操作
5775	[redacted]	WEB漏洞	[redacted]	高	漏洞处理	32	zhpyuan	2015-05-14 22:51:58	000000000113984	JSRC	删除/ 案例 / 详情
5774		WEB漏洞		高	漏洞处理	32	zhpyuan	2015-05-14 22:50:01	000000000113993	JSRC	删除/ 案例 / 详情
5773		WEB漏洞		高	漏洞处理	32	zhpyuan	2015-05-14 22:49:22	000000000113992	JSRC	删除/ 案例 / 详情
5772		WEB漏洞		高	漏洞处理	32	zhpyuan	2015-05-14 22:47:43	000000000113991	JSRC	删除/ 案例 / 详情
5771		WEB漏洞		高	漏洞处理	180	zhpyuan	2015-05-14 22:28:30	000000000113981	JSRC	删除/ 案例 / 详情
5770		WEB漏洞		严重	漏洞处理	180	zhpyuan	2015-05-14 21:55:28	000000000113982	JSRC	删除/ 案例 / 详情
5769		WEB漏洞		低	漏洞处理	4	zhpyuan	2015-05-14 21:48:40	000000000113983	JSRC	删除/ 案例 / 详情
5768		WEB漏洞		中	漏洞处理	24	xphad	2015-05-14 21:31:06	000000000113	JSRC	删除/ 案例 / 详

连接内部工单系统

漏洞处理

当前状态：

未处理 漏洞验证 漏洞确认 **漏洞处理** 已修复 忽略

处理信息：

处理时间	处理信息	备注说明	操作人
2015-05-14 22:52:57	感谢您提交的反馈，我已通知工作人员请耐心等待。		ROBOT-J
2015-05-15 17:08:17	您的反馈由工作人员接管，正在评估危害和影响。		weichongfeng
2015-05-15 17:08:22	漏洞得到确认，您获得积分：32。		weichongfeng
2015-05-18 11:23:27	您提交的漏洞已进入修复过程，事件号：000000000113984。		weichongfeng

漏洞处理： 已修复 ▼

安全响应中心运营-及时跟踪

JD.COM 京东

2015/6/25 (周四) 17:46

杨婷婷 <yangtingting3@jd.com>

【6月25日】JSRC整体运营情况

收件人　鞠宝松

抄送　李学庆; 曾毅; 晋亮

需后续工作。　开始时间: 2015年6月26日星期五。　到期时间: 2015年6月26日星期五。

截止今日占五月份总价值**77.95%**。当天漏洞总价值**1410元**，未超出警告基线。

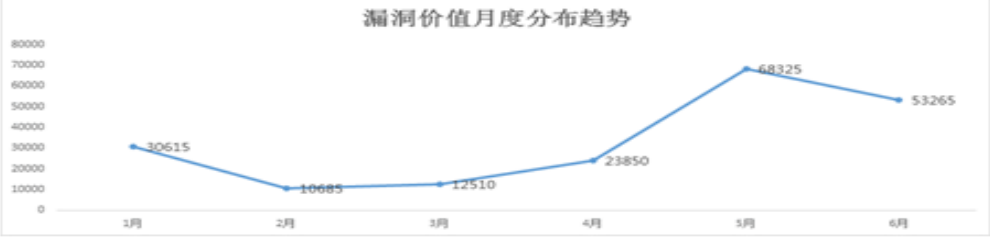
➢ 当天严重高风险漏洞表

0006为商城SQL注入漏洞 总价值占当天价值96%。请小松在最晚回复时间（19:00）回复此任务。

任务编号	任务名称	原因分析	解决方案	负责人	完成时间	审核人	审核状态
0006	京码应用中心-包裹码管理-SQL注入						

➢ 漏洞价值月度分布趋势

六月漏洞总价值**53265**元。每日的安全警告基线为**1523**元（基线值的80%）。



➢ 2015年漏洞价值趋势（单位：周）

安全响应中心运营-及时沉淀

JD.COM 京东

任务编号	任务名称	漏洞类型	原因分析	后续改进措施	负责人	当日任务进度	完成情况	归档名称	归档位置
201506160001	wap机 历	水平权限	原因分析：机票原来的逻辑结构为机票后台通过 户 pi 询系 统 ，当 用 pi 出 pi 与订 单 漏 1、 2、后端调用订单时，pin为空依旧可以调用	无			完成	机票 线 申请 完成 【邮件】	ft tı ac 严 机 答复 机票订单严重漏洞紧急上
201506120002	快 及配置	信息泄露	618 发部 部 线， 经 回 滚， 漏洞 的	1、 添加针对备份文件的检 测 名 及i 检测 检测 ".t "、 ".g	(享 及 代 (署 和 齐	已完成	未完成	弱 测【 邮件】	ft tı ac 严 漏 快车整站代
			漏洞未发现原因：漏洞	1、本周找学志明要所有网站 tre 疑 似 、 ran 验 2、 事 件 扩展添加服务器安全监	兰 鞠	1、此任务已 完 1 16 现 手工验证发现		6月24日严重高风险漏洞任务跟进情况【邮件】	ft tı aı 严 漏 /0002京东快车整站代

检测方法

防御思路

最佳实践

开发规范

安全培训

黑锅语录：

当这样平台的运营人员是幸福的，就像一个图书馆 (图书馆的威力，你们都懂的!)

JD.COM 京东

多·快·好·省

Thanks – THE END