京东外部威胁处理规则

编写人	**京东安全应急响应中心**
版本号	V7.0
适用范围	**通过**（http://security.jd.com，以下简称 JSRC）**反馈平台收到的所有威胁报告**
最后更新时间	2020-2-25
修订记录	V1.0 首发：2013-04-12 V2.0 修改评分标准并提高奖励力度，更新评级规范：2014-07-29 V3.0 修改评分标准并提高奖励力度；更新评级规范：2015-03-11 V4.0 更新评分标准并提高奖励力度；更新评级规范：2015-05-18 V5.0 新增和更新评分标准细则、范围等，新增 FAQ：2017-08-29 V6.0 新增和更新评分标准细则、范围等，测试业务范围及通用原则：2018-06-21 V7.0 新增和更新评分标准细则、范围等，测试范围并提高奖励力度：2020-3-31

前言

京东非常重视安全威胁信息并关注安全风险的本质，我们承诺，对每一位报告者的问题提供专人跟进、分析和处理，并及时予以答复或反馈。对于每一位恪守白帽子精神、保护人民群众安全利益、帮助京东提升安全质量的报告者，我们将给予以感谢和回馈。

京东认为，每个安全问题的处理及整个安全行业的进步，都离不开各方人士的共同推动与合作，希望企业、安全公司、安全组织和研究者一起加入到“合作式的安全报告披露与处理”中来，为建设良好的互联网安全生态而努力。

致谢：所有对该标准给出建议的安全组织、团队及个人

如果您对该流程有任何建议，欢迎发送邮件到 security@jd.com，建议一经采纳，JSRC 会送出专属礼品。

一、适用范围

京东商城：

.jd.com、.jd.hk 等;

1 号店：

.yhd.com、.yihaodian.com、*.1mall.com 等;

京东物流

*.jdwl.com ， *.jclps.com

京东海外

.joybuy.com、.jd.ru 、*.jd.co.th 、*.jd.id 等;

京东医药

.healthjd.com、.yiyaojd.com 等;

7fresh：

*.7fresh.com 等;

京东金融：

.jr.jd.com、.baitiao.com *.jdpay.com *.chinabank.com.cn *.wangyin.com 等;

京东云：

.jcloud.com、.jdcloud.com 等;

京东安联：

.jdallianz.com、.allianz.cn

京东云配：

.yunpei.com、.yunxiu.com

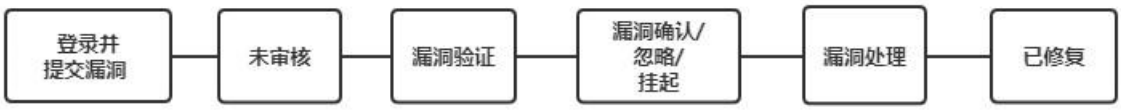
京东 App 重点关注：

拍拍二手，7Fresh，1 号店 ，京东阅读，手机京东，TOPLIFE，京东微联，JD.id（印尼版本），JOYBUY（俄罗斯版本）等

IOT 业务范围：

核心产品：京鱼座 AI 音箱，京东云路由宝路由器

二、威胁反馈与处理流程



【提交阶段】

报告者访问 JSRC 平台(https://security.jd.com/) 注册并提交漏洞，内容包括但不限于：漏洞域名、潜在危害、复现步骤、建议修复措施等。

【处理阶段】

1) 一个工作日内 JSRC 工作人员确认报告并评估，非工作日内严重或高危漏洞报告由值班人员 24 小时内确认并评估（状态：漏洞验证——漏洞确认/忽略）。

2) 漏洞确认后三个工作日内 JSRC 工作人员处理并计分（状态：已评分/漏洞处理）。必要时会与报告者沟通确认，请报告者予以协助。

【挂起阶段】（非必须）若审核时漏洞描述不清晰或者证据不充分等问题，在【处理阶段】审核人员会将漏洞设置为挂起状态，请提交者尽快补充详情，7 天后仍未补充细节，报告将超时被忽略，若确认报告问题仍然存在，可以重新提交。

【修复阶段】业务部门修复所报告的问题并安排修复上线（状态：已修复），修复时间根据问题严重程度、修复难度和业务情况而定。

一般严重报告的修复时间为 24 小时内，高危为 3 天内，中危 7 个工作日内，低危 14 个工作日内，客户端和特殊业务因发版及其他限制因素，修复时间稍有变化。 白帽子可对状态为已修复的问题进行复查，若问题仍存在，可再次提交反馈。JSRC 审核人员会对该问题审查确认，并再次计分或处理（JSRC 已确认漏洞，3 个月后若复查问题仍然存在，无论漏洞当前状态，均可再次提交）。

三、 有效漏洞/情报基础奖励标准

3.1 安全威胁评分说明

JSRC 威胁报告主要包含 web/客户端漏洞、威胁情报、通用组件和插件漏洞四个报告内容，下面会对每个部分的规则做评分说明。

根据威胁对业务产生的安全风险，威胁分为严重、高危、中危、低危、无影响（忽略）五个等级。

京东相关业务，根据业务重要程度分为：核心业务、一般业务、边缘业务

【核心业务】：涉及京东支付系统、京东账户系统、京东用户敏感信息、订单详细信息的相关平台或网站。

【一般业务】：涉及京东运营数据、物流统计信息数据及商家业务数据的网站。

【边缘业务】：涉及合作商家网站、商家营销后台，及非支付功能的网站/平台。

3.1.1 京东云业务收取原则：

京东云业务系统按京东相关业务漏洞标准收取；

如下第三方业务及 SaaS 类业务评分上可能根据对京东的影响做【降分或降级】，等级不超过边缘【中】处理。：云市场、教育云、产业云、城市云、县域之窗；

京东云租户只收取涉及京东及京东商家，涉及京东数据的漏洞；

所有威胁报告将结合漏洞实际利用危害及业务重要程度进行评估最终报告得分（注：1 积分=5 人民币）

表 2-1 积分范围参考

类型\等级	严重	高危	中危	低危
核心业务	1600-2200	600-1000	60-120	12~24
一般业务	900-1200	300-500	36-80	8~16
边缘业务	135-150	48-64	9~15	1~2

特殊现金奖励漏洞：核心业务涉及重要数据和影响巨大的安全问题（可以是漏洞、情报或者通用组件或插件漏洞），由 JSRC 评定后会奖励 1-50 万人民币，该奖励会不定期做评定和发布

漏洞报告打赏：对于漏洞描述详细、报告内容完整、思路清晰的漏洞报告，审核人员将对报告者进行奖励（奖励分数范围 10-100，加分项请参考 3.6 威胁报告质量评判标准）

3.2 Web/客户端漏洞报告评审标准

严重漏洞：

1) 直接获取核心系统权限（服务器端权限、客户端权限）的漏洞。包括但不限于：命令注入、远程命令执行、上传获取 WebShell、SQL 注入获取核心系统权限、缓冲区溢出（包括可利用的 ActiveX 缓冲区溢出）。
2) 直接导致核心业务拒绝服务的漏洞。包括通过该远程拒绝服务漏洞直接导致线上核心应用、系统、服务器无法继续提供服务的漏洞。
3) 核心业务的严重逻辑设计缺陷和流程缺陷。包括但不限于任意账号登录和密码修改、任意账号资金消费、特大量订单详细泄露、核心支付系统支付交易流程的漏洞。
4) 严重级别的敏感信息泄露。包括但不限于核心 DB 的 SQL 注入漏洞、包含公司、用户敏感数据的接口引发的信息泄露。

高危漏洞

1) 直接获取一般系统权限（服务器端权限、客户端权限）的漏洞。包括但不限于：命令注入、远程命令执行、上传获取 WebShell、SQL 注入获取系统权限、缓冲区溢出（包括可利用的 ActiveX 缓冲区溢出）。
2) 核心系统越权执行敏感操作。包括但不限于绕过认证直接访问管理后台可操作、核心业务未授权访问、 核心业务后台弱密码，增删查改任意用户敏感信息或状态等核心交互的越权行为。
3) 敏感信息泄漏漏洞。包括但不限于源代码压缩包泄漏、越权或者直接获取大量用户、员工信息。
4) 涉及京东账号系统的暴力破解漏洞。
5) 可远程获取客户端权限的漏洞。包括但不限于远程任意命令执行、可进内网获取数据的 SSRF、远程缓冲区溢出及其它逻辑问题导致的客户端漏洞。核心系统重要页面的存储型 XSS（包括存储型 DOM-XSS）以及可获取核心 cookie 等敏感信息且具有传播性的各种 XSS。

中危漏洞

1) 普通信息泄露。包括但不限于未涉及敏感数据的 SQL 注入、影响数据量有限或者敏感程度有限的越权、源代码或系统日志等信息泄露。
2) 需受害者交互或其他前置条件才能获取用户身份信息的漏洞。包括但不限于包含用户、网站敏感数据的 JSON Hijacking、重要业务操作（如支付类操作、修改个人账号敏感信息类操作）的 CSRF、一般业务存储型 XSS。
3) 普通的逻辑缺陷和越权。包括但不限于一般业务系统的越权行为和设计缺陷，以及对经济价值影响较小的漏洞(如少量返利/京豆等)。
4) 可攻击管理后台的 XSS 类攻击（需提供前台攻击位置，定位风险）。

低危漏洞

1) 轻微信息泄露，包括但不限于路径、SVN 信息泄露、PHPinfo、异常和含有少量敏感字段的调试信息，本地 SQL 注入、日志打印及配置等泄露情况。
2) 只在特定情况之下才能获取用户信息的漏洞，包括但不限于反射 XSS（包括 DOM 型）、边缘业务的存储 XSS。

3） 利用场景有限的漏洞，包括但不限于短信、邮箱炸弹，URL 跳转，非京东账户系统的可撞库接口等。包括不涉及京东账号系统的暴力破解漏洞或涉及京东账户系统的可撞库接口

4） 利用有难度但存在安全隐患的漏洞，包括但不限于可引起传播的 Self-XSS，登录接口缺陷，敏感操作但利用条件苛刻的 CSRF。

无危害（忽略）：

1) 无法利用/无实际危害的漏洞。包括但不限于 不可利用的 Self-XSS(无法分享给其他账号访问/未收到后台记录）、非重要交互（如查询类操作）的 CSRF、静态文件目录遍历、401 认证钓鱼、内网 IP/域名、无敏感信息（如用户昵称、用户个人公开的信息、已脱敏的敏感信息等）的 JSON Hijacking 、横向短信轰炸等；
2) 不能重现的漏洞。包括但不限于经 JSRC 审核者多次确认无法重现的漏洞；
3) 内部已知、正在处理的漏洞，包括但不限于如 Discuz!等已在其他平台公开通用的，白帽子、内部已发现的漏洞；

4) 内部存在审核机制的提交接口所涉及的 CSRF、越权提交等漏洞；
5) 非接收范围或内的漏洞，如非京东业务的安全漏洞；
6) 实际业务安全性无影响的 Bug。包括但不限于产品功能缺陷、页面乱码、样式混乱；
7) 不接收无实际意义的扫描器结果报告；
8) 无证据支持的情况，包括但不限于账号被盗即表示有漏洞；

3.3 威胁情报说明

3.3.1. 情报内容及范围说明

威胁情报漏洞提交时，应包含所提交**情报场景**所对应的**关键线索**，以便审核人员验证、追踪威胁情报。
情报关键线索

表 2-2

关键词	**示例**
关系人	可以是具体人或组织的信息，如：联系方式及团体交流渠道（如 QQ 群、社区、YY 等），论坛网址等
场景	包括但不限于盗号、数据非法贩卖、通用漏洞攻击、黑产活动，参考《情报收集场景》
步骤和流程	详细的流程步骤，实现该攻击的方式。如该一个有组织的活动秒杀情报（秒杀类情报对时间要求较高，情报过期的可能会被忽略）：攻击者收集该活动的渠道，实现秒杀行为的操作步骤及工具等。
证据/样本	贩卖非法数据/账号类情报、需提供不少于 10 条数据样本共审核人员进行情报确认。 对违法操作类情报，需提供具体软件或操作过程截图证据。

情报收集场景参考（包括但不限于）

表 2-3

技术情报	**业务情报**
服务器被入侵且提供了入侵行为特征等关键线索	对有组织有规模的盗取和售卖京东账号、订单数据等行为提供关键线索
核心业务数据库被下载，并提供数据库名或文件等关键线索	对大批量的刷单、注册小号、套现等行为提供关键线索

支付业务逻辑漏洞利用、业务流程绕过等关键线索	对泄露公司内部数据、用户数据等行为提供关键线索
蠕虫传播、流量劫持等提供源链接、网络数据包样本等关键线索	对有针对性的秒杀、刷积分、绕过现有认证或者流程的事件提供关键线索
用户敏感数据大规模被窃取且提供了攻击代码、漏洞利用工具等关键线索	对业务范围内的活动恶意利用提供关键线索
能够帮助完善防御系统，新型攻击方式、技术等提供详细分析	发现并提供京东内部人员联合外部个人或组织、商户，乘工作之便窃取敏感数据、攻击京东系统以谋取个人利益的关键线索。
数据泄露、非法数据贩卖等情报信息，包含：联系人，联系方式、收款信息等	

3.3.2．情报评分标准

参考《2.1 安全威胁评分标准》结合**实际影响、业务威胁等级**和**情报线索**是否完整综合评分。

情报争议解决原则：

1. 提交者应对**情报真实性**在报告中作出证明；未能主动证明真实性的情报将被**忽略或挂起**；
2. 同一漏洞的**利用情报**原则上不会高于该漏洞的**漏洞报告评分。**
3. 同一情报来源的不同情报内容（或不同情报源的相同情报内容）原则上算作记为 1 条情报，同一第三方平台域名（或其他销售媒介）下的多个京东账号、订单信息售卖页面，记为 1 条情报。当多名白帽子提交相同情报内容时，根据提交时间进行仲裁。

JSRC 不允许白帽子为获取情报使用黑客技巧攻击第三方机构或个人，请在日常工作中保护自身安全及合法权益。

3.4Iot 设备漏洞评分标准

严重漏洞

1） 严重的逻辑可造成集团或用户较大经济损失的漏洞
2） 互联网环境下无交互远程命令执行漏洞
3） 在还联网环境未授权状态下访问受保护的数据（如声纹、口令、图像）
4） 互联网环境下控制未授权设备，执行不被期望的函数（如，篡改摄像头，监控视频等）

高危漏洞

1） 局域网内的无交互命令执行
2） 局域网内对控制未授权设备，执行不被期望的函数（如，篡改摄像头，监控视频等）
3） 在未授权状态下远程发起永久性拒绝服务攻击导致大量用户的设备无法再使用，或者需要重新刷写整个系统才可恢复
4） 能够获取大量详细敏感信息的漏洞
5） 密码可以暴力破解

中危漏洞

1） 互联网/局域网内的拒绝服务
2） 需交互造成临时性拒绝服务
3） 非重要功能的越权、逻辑漏洞等
4） 需要较苛刻环境下才能触发的危害较高的漏洞
5） 在本地获取 root 用户权限并执行任意代码、命令
6） 不安全的加密算法及密钥存储，可导致敏感信息泄露等危害（根据影响程度，可提升风险等级）

低危漏洞

1） 不安全配置（利用难度较大或无较大影响的问题将忽略）
2） 低危的信息泄露
3） 需要物理接触，危害只造成信息泄露或有安全风险类漏洞
4） 强交互后的拒绝服务类漏洞

3.5 威胁报告质量评判标准

3.5.1. 漏洞类威胁报告质量评判标准：

对于高质量的威胁报告，如新颖的绕过方式，有一定技术深度但危害较小的报告，JSRC 会综合评估因素给出超出评级规则的奖励来激励报告者；

例如此前某任意用户登录漏洞，漏洞得分 420，因为提供了优质的漏洞报告，帮助审核人员提高验证效率，审核人员评分时给白帽子额外的 60 分作为奖励分。

具体奖励标准如下：

报告内容：【标题】【漏洞描述】【复现方法】【利用证明】【修复方案】
✓ 标题：标题包含漏洞影响域名、涉及参数和漏洞类型，影响范围；
✓ 漏洞描述：内容包含漏洞描述、漏洞涉及 url、漏洞参数，需要其他完整
✓ 复现方法：对漏洞复现步骤按照逻辑顺序进行描述、若使用工具复现漏洞，应提供工具名称。

- ✓ 利用证明：包含漏洞影响说明和漏洞利用证明，一般以截图形式提供。
- ✓ 修复方案：报告中对于所发现漏洞，提供至少一条可执行的修复建议，可以提供代码级的修复建议，也可以提供防护策略

质量评判标准：报告首次提交时上述 5 个元素是否全部包含（加分必要条件），标题明确概括漏洞情况（加分）、漏洞细节准确详细（加分），漏洞证明清晰、逻辑完整（加分），修复建议可执行性强（加分）。

3.5.2. 威胁情报类报告质量评判标准：

报告内容：【标题】【情报内容】【数据证明】【原始情报来源】

- ✓ 标题：标题简要是概括情报内容，影响；
- ✓ 情报内容：情报具体内容，威胁组织信息，漏洞利用威胁内容，情报涉及系统、数据、业务信息等。
- ✓ 数据证明：情报数据真实性证明，如贩卖账号样本，漏洞攻击 EXP、黑产工具样本（或工具截图）、被拖数据库数据样本等。
- ✓ 原始情报来源（非必填）：引用情报链接，社交群组聊天记录，网页截图等情报来源证明。

质量评判标准：报告首次提交时上述前 3 个元素是否全部包含（加分必要条件），标题准确概括情报内容（加分）、情报内容准确详细（加分），数据证明清晰、逻辑完整（加分），原始情报来源真实可靠，可溯源（加分）。

三、通用原则

1. 威胁报告禁止保存在互联网开放的云服务中（包括但不限于云盘、云笔记等），因漏洞报告内容保存于云服务导致的漏洞泄露风险一经确认，当前报告不计分；
2. 威胁报告提交后在未修复前，主动公开的报告不计分；
3. 同一威胁报告（包括情报、通用组件和插件）最早提交者得分，提交网上已公开的报告不计分。
4. 当多份威胁报告（安全漏洞、情报、通用组件和插件）有相似之处，JSRC 工作人员分析发现是由于同一处问题导致时，该情况只有最早提交者得分；
5. 同一漏洞导致的多个利用点按照级别最高的奖励执行； 同一系统只收取前三个接口产生的同类型漏洞，此条款收取漏洞时限为 3 个月。（如：同个 JS 引起的多个 XSS 漏洞、同接口多参数 xss 漏洞/sql 注入漏洞统一处理，同一个发布系统引起的多个页面的 XSS 漏洞、通用框架导致的整站问题等）；
6. 各等级漏洞的最终积分由漏洞利用难度及影响范围等综合因素决定，若触发条件非常苛刻（如：特定浏览器才可触发的 XSS 漏洞），特殊时期(如双 11 活动内传播影响大的业务逻辑漏洞)，需要特殊账号权限才能发现利用的漏洞，经审核可能跨等级调整积分；

7. 对于非京东商城发布的产品和业务，如京东投资公司、子公司、合资公司等，评分上【降分或降级】，等级不超过中【中】，但会参考实际危害和影响做具体评级操作，其处理和修复不能保证在预定时间内，请报告者理解；
8. 对于京东云合作业务，例如 http://cpsc.jcloud.com（虽以 jcloud.com 为域名，但从页面标题及内容可明显辨别为非京东业务），此类威胁报告可能会根据业务影响降低评分（但涉及核心业务范围内的敏感数据，JSRC 工作人员会与业务方沟通后酌情评级处理）；
9. 对于京东云租户业务漏洞处理说明：平台对云租户漏洞不会给予积分奖励，但是义务性会把漏洞通知给租户；
10. 报告者在进行渗透测试时，如在线上对业务做增删改操作时，请勿直接对正常用户数据做操作，数据添加请在标题或明显字段增加【我是测试】字样，以便于 JSRC 和业务方识别数据真实性；
11. 未经授权的情况下，不允许使用非本人账号在系统内进行安全测试，禁止使用非本人账号进行功能操作/如添加权限等。可参考【SRC 行业安全测试规范】。
12. 威胁情报的定级根据提供信息完整度及影响综合评定。对于业务侧/风控已有感知的业务情报，将结合已知信息评定/忽略。对于多人提交同一情报的情况，根据情报丰富度判断是否再次收录，即后提交者的情报信息更完整详细也将予以奖励。在提交情报时，请尽可能详细完整。
13. 以漏洞测试为借口,利用漏洞进行损害用户利益、影响业务正常运作、修复前公开、盗取用户数据等行为在溯源发现后将不会计分，同时京东保留采取进一步法律行动的权利；
14. SQL 注入测试过程中，证明危害即可，获取十条以上数据者追究更加数据情况做出相应处理（取消奖励同时京东保留采取进一步法律行动的权利）。延时函数请勿使用大数，而对业务造成影响
15. webshell 的上传，上传输出语句即可，禁止上传 webshell，或者提权等高危操作。
16. 本协议最终解释权归京东集团信息安全部所有。
17. 为方便业务修复，不同系统的漏洞建议分开提交
18. 白帽子如需在漏洞修复后将技术细节用作学习交流，需经京东同意。
19. 京东集团及京东所属公司员工不得参与漏洞奖励计划；
20. 请通过正常渠道与工作人员交流反馈问题，对于一些没有证据或使用非正当手段进行诬陷、诽谤等行为，工作人员将适用法律手段维护权益。

四、 平台奖励

1、“神兽”赋能

本季度提交 20 个高质量漏洞（除边缘业务外），获得“麒麟”神兽助力，本季度严重/高危漏洞奖励 2 倍（奖励不与活动漏洞叠加，活动漏洞只计入数据）

本季度提交 10 个高质量漏洞（除边缘业务外），获得“凤凰”神兽助力，本季度严重/高危漏洞奖励 1.5 倍（奖励不与活动漏洞叠加，活动漏洞只计入数据）

2、个人月度奖

每获得一次月度前十便可获得一个【信物】

年终累积获得 3、6、9、12 个信物可额外获得新春现金大红包+神秘礼盒，神秘礼盒将在 JSRC 微信公众号提前一个月预告。

3、个人季度奖

注：下表中的 n 为一个季度内白帽子个人的高危漏洞个数						
段位	**子段位**	**高危个数**	**积分**	**现金奖励**	**京东卡奖励**	**荣誉证书**
高危段（A）	A1	≥10	≥6000	15K	（n-10）张 1000 元京东卡	定制荣誉证书
	A2	≥6	≥4000	8K	（n-6）张 1000 元京东卡	定制荣誉证书
	A3	≥4	≥3000	5K	（n-4）张 1000 元京东卡	定制荣誉证书
	A4	≥2	≥2000	3K	（n-2）张 1000 元京东卡	定制荣誉证书
普通段	B	≥0	≥1000	1K	n 张 1000 元京东卡	定制荣誉证书

4、团队季度奖

团队奖励（团队人数限制 1-15 人）		
称号	要求（同时满足）	奖励
精英战队	1、团队总积分》5000 2、提交有效高危总个数》10	1、6000 元现金奖励 or 京东卡 2、团队季度奖定制证书 3、团队内积分最多队员可获得 600 元现金 or 京东卡
传奇战队	1、团队总积分》10000 2、提交有效高危总个数》20	1、1.8W 现金奖励 or 京东卡 2、团队季度奖定制证书 3、团队内积分最多队员可获得 1800 元现金 or 京东卡
史诗战队	1、团队总积分》15000 2、提交有效高危总个数》30	1、3W 现金奖励 or 京东卡 2、团队季度奖定制证书、奖杯 3、团队内积分最多队员可获得 3000 元现金 or 京东卡 4、获得“史诗战队”称号的团队，将受邀参加年终 JSRC 白帽盛典

5、个人/团队年度奖

以年度积分为参考，JSRC 将为年度内做出杰出贡献的白帽/安全团队，发放年度奖励。

个人奖励评价标准：本年度内，个人贡献值位于个人年度荣誉榜前七，年度奖励金额以具体积分为参考

（2019 年数据仅供参考）

第 1 名 120000

第 2 名 80000

第 3 名 60000

第 4-5 名 30000

第 6-7 名 10000

团队奖励评价标准：在本年度内，团队内所有成员（人数> 3 人）的总贡献值位于团队排行榜前三名，则可获得团队年度奖励，年度奖励金额以团队积分为参考。

（2019 年数据仅供参考）

第 1 名 30000

第 2 名 20000

第 3 名 10000

五、【JSRC 礼品发放机制】

1. 漏洞提交者在收到平台发放的漏洞积分后，可在 JSRC 平台商城中进行礼品兑换，1 积分价值相当于 5 人民币。

2. 当月 15 日前兑换的非现金礼品，将于当月 16 日统一发放；15 日后兑换的非现金礼品将于次月 1 日统一发放，如遇节假日顺延至节后第一个工作日；

3. 每月 25 日前兑换现金，将于本月 26 日结算，10 个工作日内统一汇款；

4. 兑换非现金实物礼品时，需在平台提供准确的收件人信息；兑换非现金电子礼品时，需在平台提供准确的收件邮箱；兑换现金礼品时，需在平台提供准确的收款信息；如因接收信息不准确造成礼品丢失或损坏，JSRC 不承担责任。

5. 常规礼品兑换外，JSRC 会定期开展月度、季度、年度贡献值排行榜奖励、高质量漏洞奖励、热点节日关怀、线上众测等活动，具体规则将在活动前以公众号文章形式发布，奖励标准及礼品管理以活动公告为准。

6. JSRC 遵循诚信原则，如有违反诚信的行为，JSRC 有权采取相应的措施，如扣除积分、要求退还礼品。

六、 争议解决办法&FAQ

争议解决办法

在威胁处理过程中，如果报告者对处理流程、威胁评定、威胁评分等有异议的，请通过当前报告详细页即时通讯“一键沟通”按钮联系 JSRC 工作人员交流反馈，JSRC 将根据威胁报告者利益优先的原则进行处理。

FAQ

Q: JSRC 平台的 1 积分相当于多少人民币?

A: 截止目前的奖励标准，JSRC 平台 1 积分相当于 5 元人民币。

Q: JSRC 平台礼品兑换发放是不是有固定规则?

A: 是的，每月 2 次兑换，第一次是在每月的 1 号~15 号，第二次在 16 号~月底之间。

Q: 在其他平台提交的京东威胁也有效吗? 与其他安全团体关系如何?

A: 是的，有效。如在其他威胁或漏洞揭报平台提交，也会跟进处理，如该平台有对应规则（虚拟货币、积分等），JSRC 会参考该平台规则给予奖励。JSRC 提倡合作共赢，希望为整个互联网安全生态添砖加瓦，目前 JSRC 已与一些安全团体有了合作，未来会有更多。

Q: 威胁报告在被评分之后，积分是不是会有变动?

A: 是的，少数情况下会有变动。一种是 JSRC 工作人员在评分之后发现评分给少或者给多；另外一种是报告者反馈有异议后，工作人员综合情况做出的变动。JSRC 将尽力减少甚至避免此情况，给出一个客观且无争议的评级。

Q: 威胁报告的确认、处理周期会按照标准来执行吗?

A: 常规情况按照标准执行，但也会存在周期较长的情况，如 JSRC 做活动时、业务大促、客户端漏洞和安全情报等。同时也有可能由于报告者提供的内容不够详细导致确认延迟，请各位理解。因此请报告者尽可能提交详细步骤或 POC，加快工作人员处理速度。

Q: JSRC 有没有先“忽略” 之后偷偷修复情况?

A: 绝对不会。提交的“威胁”一旦进入“忽略”状态，工作人员会在备注中说明缘由，JSRC 会根据规则操作每一个报告者提交的威胁，有依有据，客观中肯。当然，中间存在因业务变动导致“威胁”不存在的可能性。但无论如何，JSRC 都不会 “偷偷” 修复。