陌陌安全应急响应中心

漏洞处理流程及评分标准 2.2

编写人：陌陌安全应急响应中心

版本号：2.2 | 更新日期：2019-04-25

修订记录

版本号	修订时间	修订内容
V1.0	2017-03-14	发布第一版
V2.0	2017-10-30	更新安全漏洞评级标准、评分标准通用原则
V2.1	2017-12-29	更新安全漏洞评级标准
V2.2	2019-04-25	更新安全漏洞评级标准、评分标准通用原则

目录

我们承诺

1. 陌陌安全应急响应中心（MMSRC）诚邀各界安全研究员对陌陌科技相关业务进行安全测试，承诺会认真审查每一例漏洞上报并分配审核人员进行跟进、分析和处理，并及时给予答复；
2. 陌陌安全应急响应中心（MMSRC）支持合作式的安全漏洞/威胁情报上报和处理，对于每位恪守白帽子精神，保护用户利益，推进陌陌安全质量的用户，我们将按照此评分标准及奖励办法给予感谢和回馈；
3. 陌陌反对和谴责一切以测试漏洞为借口，利用安全漏洞进行破坏、损害用户利益或陌陌公司利益的骇客行为，同时陌陌保留采取进一步法律行动的权利。
4. 陌陌安全应急响应中心（MMSRC）认为每个安全漏洞的处理和整个安全行业的进步，都离不开各方共同合作，希望各方企业、安全公司、安全组织及安全研究者一起加入到“负责任的漏洞披露”过程中来，让更多人了解安全关注安全，从而营造出更好的安全生态，一起为建设更安全更健康的互联网环境而努力。

致谢

陌陌安全应急响应中心由衷感谢每一位安全研究员，同时 MMSRC 的成立离不开业界同仁们对“互联网安全生态”推进做出的努力。

1、安全漏洞/威胁情报反馈和处理流程

1.1、预报告阶段

漏洞提交者使用陌陌账号授权登录陌陌安全应急响应中心（https://security.immomo.com）生成账号。

1.2、报告阶段

漏洞提交者可通过陌陌安全应急响应中心反馈平台（https://security.immomo.com）提交安全漏洞/威胁情报详情和复现方式流程（状态：待审核）。

1.3、处理阶段

漏洞提交者通过陌陌安全应急响应中心（https://security.immomo.com）提交安全漏洞/威胁情报，审核人员将在第一时间着手验证修复，在三个工作日内给出结论（已确认 or 已忽略），处理过程中请勿外泄任何有关漏洞的信息，必要时审核人员会与提交者沟通确认，届时请提交者予以协助。

1.4、忽略阶段

如果审核人员无法通过现有漏洞详情内容确定漏洞有效性，可要求漏洞提交者补充安全漏洞/威胁情报详情内容，补充阶段状态为“挂起”，漏洞提交者可在三日内对挂起状态漏洞进行编辑，逾期自动忽略。对于经验证后无影响或无效的漏洞，审核人员可主动选择忽略（需注明忽略理由），所忽略漏洞不计奖励。

1.5、修复阶段

审核人员复现并确认漏洞提交者上报的漏洞之后则会进入修复阶段，修复时间根据漏洞严重程度及修复难度而定，一般来说，严重和高风险漏洞 24 小时内，中风险三个工作日内，低风险七个工作日内。客户端漏洞受版本发布限制,修复时间根据实际情况确定。

1.6、复测阶段

漏洞确认修复之后会将漏洞状态更改为已修复，届时会邀请漏洞提交者协助复测该漏洞是否已成功修复或修复方案能否被 Bypass，如未成功修复或被 Bypass，陌陌安全应急响应中心应给予额外奖励。

1.7、奖励办法

陌陌安全应急响应中心感谢每位提交漏洞的漏洞提交者，每个漏洞已于确认之后会按照评分标准给予相应积分奖励，积分可在陌陌安全应急响应中心（https://security.immomo.com）兑换礼品，此外陌陌安全应急响应中心会不定期举办相应线上/线下活动，会优先邀请平台核心安全研究员参加。

2、贡献值和积分值计算方式

2.1、贡献值对应表

贡献值由漏洞对应危害程度以及业务重要程度决定
贡献值计算公式：贡献值 = 基础贡献值 * 业务系数

基础贡献值 / 业务系数	严重漏洞 (9~10)	高危漏洞 (6~8)	中危漏洞 (3~5)	低危漏洞 (1~2)
核心业务（10）	90~100	60~80	30~50	10~20
一般业务（5）	45~50	30~40	15~25	5~10
边缘业务（1）	9~10	6~8	3~5	1~2

2.2、积分值对应表

积分值由漏洞对应危害程度以及业务重要程度决定
积分值计算公式：积分值 = 基础积分值 * 业务系数
（注：积分兑换比例为 1：10）

基础积分值 / 业务系数	严重漏洞(90~100)	高危漏洞(50~80)	中危漏洞 (5~10)	低危漏洞 (1~2)
核心业务（10）	900~1000	500~800	50~100	10~20
一般业务（5）	450~500	250~400	25~50	5~10
边缘业务（1）	90~100	50~80	5~10	1~2

3、安全漏洞评级标准

陌陌安全应急响应中心（https://security.immomo.com）根据该评分标准（以下）将安全漏洞分为五个等级，分别为：严重、高危、中危、低危、无影响。每个已确认漏洞基础贡献值最高为 10，基础积分值为 100。由陌陌安全应急响应中心结合利用场景和危害程度及业务的重要程度等综合因素给予相应分值和漏洞评级，积分值

将用于礼品奖励的兑换。

3.1、严重漏洞

【基础贡献值：9 ~ 10，基础积分：90 ~ 100】

1. 直接获取系统权限（服务器端权限、客户端权限）的漏洞。包括但不仅限于命令注入、远程命令执行、上传获取 WebShell、SQL 注入获取系统权限等；
2. 严重的逻辑设计缺陷。包括但不仅限于任意账号登陆、任意账号密码修改、任意账号资金消费、交易支付方面的严重问题等；
3. 严重级别的信息泄漏。包括但不限于核心 DB 的 SQL 注入漏洞、可获得大量用户敏感信息等；
4. 直接导致核心业务拒绝服务的漏洞。包括但不仅限于远程拒绝服务漏洞等；
5. 移动客户端涉及支付相关漏洞，例如严重的逻辑错误，能够造成直接大量获取利益相关的公司或用户损失的漏洞。

3.2、高危漏洞

【基础贡献值：6 ~ 8，基础积分：50 ~ 80】

1. 越权访问，包括但不仅限于绕过认证直接访问管理后台可操作、核心业务非授权访问、核心业务后台弱密码等；
2. 能直接盗取 IM、直播等关键业务的用户身份信息的漏洞。包括但不限于存储型 XSS 漏洞、非核心的 SQL 注入漏洞等；
3. 高风险的信息泄漏漏洞。包括但不限于源代码泄漏等；
4. 移动客户端业务的逻辑漏洞包括但不限于：严重的逻辑错误，能够造成直接大量获取非利益相关的公司或用户损失的漏洞。(如获取用户真实姓名)；
5. 移动客户端业务，第三方应用可以跨应用调用移动客户端产品的功能完成一些高危操作，包括但不仅限于远程命令执行等。

3.3、中危漏洞

【基础贡献值：3 ~ 5，基础积分：5 ~ 10】

1. 普通信息泄露。包括但不仅限于客户端明文密码存储等；
2. 需交互才能获取用户身份信息的漏洞，包括但不限于反射型 / DOM XSS、JSON Hijacking、CSRF 等；
3. 非敏感功能越权操作；
4. 移动客户端普通信息泄漏漏洞。包括但不限于客户端明文存储密码、密码明文传输等；
5. 移动客户端逻辑漏洞、敏感信息泄露、可获取敏感信息或者执行敏感操作的漏洞。

3.4、低危漏洞

【基础贡献值：1 ~2，基础积分：1 ~ 2】

1. 轻微信息泄露。包括但不仅限于路径信息泄露、svn 信息泄露、phpinfo、异常信息泄露等；
2. URL 跳转；
3. 本地拒绝服务漏洞。包括但不仅限于客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃），由 Android 组件权限暴露、普通应用权限引起的问题等；
4. 移动客户端本地拒绝服务漏洞。包括但不仅限于跨应用调用、远程浏览网页、组件权限导致的本地拒绝服

务漏洞等本地或远程利用方法。

3.5、无影响

1. 不涉及安全问题的 Bug。包括但不仅限于产品功能缺陷、网页乱码、样式混乱、静态文件目录遍历、应用兼容性等问题等；
2. 不能直接反映漏洞存在的其他问题，包括但不仅限于纯属上报者猜测等问题等；
3. 包括但不限于没有实际意义的扫描器漏洞报告（如 Web Server 的低版本）、未经验证的扫描器结果（如 APK 漏洞扫描器、AWVS、IBM APPSCAN 等）、Self-XSS、无敏感信息的 JSON Hijacking、无敏感操作的 CSRF(如对话置顶、非重要业务的普通个人资料修改等)、无意义的源码泄漏、内网 IP 地址/域名泄漏、无敏感信息的 logcat；
4. 不能说明危害和利用手法或不可复现且无关紧要的“漏洞”。

4、威胁情报评级标准

陌陌安全应急响应中心（https://security.immomo.com）根据该评分标准（以下）将威胁情报分为五个等级，分别为：严重、高危、中危、低危、无影响。每个已确认的威胁情报由陌陌安全应急响应中心结合威胁情报内容详细程度及业务的重要程度等综合因素给予积分值和评级，积分值将用于礼品奖励的兑换。
注：由于威胁情报涉及内容同安全漏洞有很大差别，故给予贡献值和积分值也和安全漏洞计算方式不同，每个已确认威胁情报奖励同报告者商讨决定，对于价值较小的威胁情报不计入积分奖励，但会给予相应贡献值以表感谢。

4.1、严重情报

1. 针对陌陌相关涉及资金业务的威胁情报（如利用陌陌某功能达到刷钱或超低价购买虚拟礼物等支付类情报）；
2. 针对陌陌所属业务、系统造成严重影响的入侵事件（如控制陌陌域名或服务器等）；
3. 针对外部流传陌陌核心数据库信息（如用户数据库被拖库）。

4.2、高危情报

1. 正在发生的蠕虫传播且提供了蠕虫传播相关信息；
2. 用户身份信息大规模被窃取且提供了攻击代码等相关线索。

4.3、中危情报

1. 上报针对进行陌陌有组织的攻击行为，包括但不限于 DDOS、撞库、恶意注册等；
2. 陌陌业务中相关安全防御策略绕过；
3. 能够帮助完善防御系统以防御高风险及以上级别危害的新型攻击方式、技术等。

4.4、低危情报

1. 伪造的钓鱼站点；
2. 传播有关陌陌公司的虚假信息。

4.5、无影响

1. 无法从报告内容中获知关键信息或无意义的报告；
2. 陌陌无法解决的潜在安全威胁（包括但不限于第三方安全威胁导致陌陌受影响等，如通过其他厂商泄密数据库影响陌陌部分用户）；
3. 恶意上报虚假信息，纯属上报者猜测的“威胁情报”；
4. 上报已发现或已失效威胁情报的。

5、评分标准通用原则

奖励只针对通过陌陌安全应急响应中心（https://security.immomo.com）平台提交安全漏洞/威胁情报的安全研究员。

1. 根据报告的漏洞详细程度，分为 3 个等级：

低：报告只提供测试代码、无分析过程，无利用过程、无危害说明、无 poc，exp 的报告，评分比例 0.0~0.3
中：报告有分析过程，但无 PoC、Exploit 的报告，评分比例：0.4~0.7
高：报告完整，有测试代码，分析过程，利用方式说明，危害说明，并提供 poc，exp 的报告，评分比例 0.8~1
最终的评分按漏洞评分乘以报告质量比例评分得出；

2. 奖励机制只支持陌陌相关业务。合作方、供应商等第三方公司系统不在此奖励范围内；
3. 同一漏洞源产生的多个漏洞,按照最高级别的漏洞奖励标准执行，漏洞数量计为一。例如 Live800 的安全漏洞、同一个 JS 引起的多个 XSS 漏洞、同一个发布系统引起的多个页面的 XSS 漏洞、框架导致的整站 XSS/CSRF 漏洞、泛域名解析产生的多个 XSS 漏洞、同一个 URL 多个参数的相同问题等；
4. 各等级安全漏洞/威胁情报的最终积分由漏洞利用难度及影响范围等综合因素决定,若漏洞触发条件非常苛刻,包括但不限于特定浏览器才可触发的 XSS 漏洞,则将跨等级调整积分。 如存储型 XSS 不能获取有 HttpOnly 保护的 cookie 等；
5. 对于陌陌正在使用的第三方应用组件所曝光的 0Day 漏洞（包括但不限于第三方 CMS、开发框架、服务端组件、第三方 SDK 等）首个上报的漏洞一经确认提交者将获得**双倍积分**奖励；
6. 游戏业务分为两个等级，不包含在列表中的游戏，将不再接收对应的漏洞，分类参考如下链接 https://security.immomo.com/blog/65；
7. 依三方站点性质不同，信息泄漏类漏洞按该站点用户/网站维度收取；
8. 如果同一漏洞或同一问题漏洞的不同表现形式在漏洞修复前由多位漏洞报告者提交，在进行奖励时,我们会以最先提交并清晰表述、重现此漏洞问题的研究者为唯一受奖励者；
9. 客户端同一个问题源产生的多个漏洞记为一个漏洞，且只给第一个提交者奖励。例如漏洞触发的调用链相同,但可以根据参数跳转到不同的功能。
10. 由于客户端的特殊性，提交漏洞以当前时间最新客户端为准；
11. 陌陌公司自己开发的客户端组件导致的通用型漏洞。例如本地拒绝服务、代码执行等等，仅给首个漏洞报告者计分，对于公司其它客户端的同个漏洞报告，均不再另外计分。
12. 对于第三方库（如 libpng、zlib、libjpeg 等）导致的客户端漏洞（包括 PC 和移动端），且可以通过升级或者更换第三方库可完成修复的漏洞，仅给首个漏洞报告者计分(不区分操作系统)。同时，从 MMSRC 获取首个漏洞的反馈时间到第三方首个修复版本发布时间的日期内，对于同一类漏洞均按一个漏洞计分，危害等级取危害最大的一个漏洞来评定；
13. 对于移动终端系统导致的通用型漏洞，比如 webkit 的 UXSS、代码执行、Android 组件配置不当等等，仅

给首个漏洞报告者计分，对于陌陌其它客户端产品的同类型漏洞报告，均不再另外计分；
14. 只接收属于陌陌移动客户端产品的漏洞，不接收 Android/IOS 系统自身漏洞；
15. 由于客户端漏洞审核本身比较复杂并且涉及到其它的开发部门，审核时间可能较 WEB 漏洞长，因此请各位白帽子在反馈漏洞时提供 PoC/Exploit，并提供相应的漏洞分析，以加快管理员处理速度，对于 PoC 或 Exploit 未提供或者没有详细分析的漏洞提交将可能直接影响评分；
16. 由于一个漏洞会有不同的利用方式，产生的危害程度也不同，所以在反馈漏洞时提供的 poc/exploit 尽可能是危害程度最大的，我们将以危害程度最大的效果来评分。
17. 漏洞挖掘过程应当以不影响陌陌业务正常运作、不破坏、不传播漏洞为原则,否则陌陌安全应急响应中心有权取消漏洞奖励；
18. 在安全漏洞/威胁情报未修复之前，被公开的安全漏洞/威胁情报不计分；
19. 网上已公开的安全漏洞/威胁情报不在奖励范围内；
20. 陌陌员工不得参与或通过朋友参与本活动；
21. 白帽子未经授权不能擅自公开或部分公开提交的漏洞，否则陌陌有权取消奖励并保留追究法律责任权利。

6、奖励发放原则

[常规奖励]

漏洞提交者通过陌陌安全应急响应中心（https://security.immomo.com）提交安全漏洞/威胁情报一经确认则会给予相应积分值奖励（陌陌安全应急响应中心平台上的一种虚拟货币），积分值可累加，除非特别声明，未使用的积分值不会过期。

礼品每月邮寄两次，15 号之前兑换的当月中下旬邮寄，15 号之后兑换的次月月初邮寄。如因报告者未能完善资料导致的延误,将顺延至下个月批量寄送时寄出；如因报告者过失、快递公司问题及人力不可抗拒因素产生的奖品丢失或者损坏，MMSRC 不承担责任；京东卡可以以卡密形式兑换，卡密一旦发出去，就不受理任何错误的情况。

实物奖品兑换依照供货商库存实际情况进行发货。

[额外奖励]

为鼓励报告者提交高质量的安全漏洞/威胁情报信息，针对影响重大的安全漏洞/威胁情报、思路新颖并对陌陌业务安全或系统安全作出突出贡献的报告者，通过陌陌安全应急响应中心评审后可获得额外奖励，除特殊说明一般为即时现金奖励。

7、争议解决办法

在漏洞处理过程中，如果漏洞上报者对处理流程、漏洞等级评定、积分发放等具有争议，请通过留言或陌陌与工作人员进行沟通，陌陌安全应急响应中心将根据**漏洞上报者利益优先**的原则进行处理，必要时可引入外部人士共同协商裁定。