BIGO SRC 漏洞处理和评分标准

编写人	BIGO 安全响应中心
版本号	V1.0
发布日期	2021 年 6 月 30 日

（一）基本原则

1. BIGO SRC 非常重视自身产品和业务的安全问题，我们承诺对每一位报告者反馈的问题都有专人进行跟进、分析和处理，并及时给予答复。

2. BIGO SRC 在跟进报告者反馈的问题时可能需要报告者的帮助，为了有效的跟进问题可能需要报告者协助一同复现问题，BIGO SRC 反对和谴责一切遮掩漏洞细节或抗拒协助的报告行为。对于提交高质量报告并在报告、反馈和积极响应跟进等过程中供有效帮助的报告者，BIGO SRC 也会酌情给予相应的奖励。

3. BIGO SRC 支持负责任的漏洞披露和处理过程，我们承诺，对于每位恪守白帽子精神，保护用户利益，帮助 BIGO 提升安全质量的用户，我们将给予感谢和回馈。

4. BIGO SRC 反对和谴责一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益的黑客行为，包括但不限于利用漏洞盗取用户隐私及虚拟财产、入侵业务系统、窃取用户数据、恶意传播漏洞等。

5. BIGO SRC 严禁一切利用安全漏洞恐吓用户、攻击竞争对手的行为。

6. 提交到 BIGO SRC 的漏洞禁止以任何形式公开，禁止重复提交到其它第三方漏洞平台，一经发现取消此用户漏洞奖励和其他各种特殊奖励。

7. 请报告者严格遵守《SRC 行业安全测试规范》。

（二）安全漏洞奖励标准

1. 报告者提交的报告，应当详细具体，写清步骤，否则可能无法获得奖励。
2. 每个报告仅提交一个漏洞，除非漏洞之间有较强关联性。
3. 如果有多个人报告了同一个漏洞，那么通常第一个成功提交报告的人将获取奖励，如有例外，将视实际情况决定。
4. 由一个潜在问题引起的多个漏洞，可能会被授予一笔奖励。
5. 不要在你不拥有或无权访问或控制的用户账户上测试漏洞。
6. 对于每一个漏洞，我们将结合实际场景中漏洞的影响、危害等综合因素给予相应的奖励。

对应的安全币奖励范围如下：

漏洞危害 / 业务类型	严重	高危	中危	低危	无影响
核心业务	500-800	250-500	50-150	0-20	0
一般业务	150-300	50-150	20-50	0-10	0

（三）安全漏洞相关评分标准

业务范围：
核心业务：Bigo Live、Likee、Imo
*目前超出以上范围且确实属于 BIGO 公司业务的漏洞或情报，视报告严重影响程度给予降级确认或忽略。

根据漏洞的危害程度将漏洞等级分为【严重】、【高危】、【中危】、【低危】、【无影响】五个等级。由 BIGO SRC 结合利用场景中漏洞的严重程度、利用难度等综合因素给予相应分值的安全币和漏洞定级，部分边缘业务的安全漏洞根据具体情况可能进行降级或忽略。每种等级包含的评分标准及漏洞类型如下：

[严重]
1. 直接获取核心系统权限的漏洞（WEB 服务器权限、APP 客户端权限）。包括但不限于远程命令执行、任意代码执行、上传并成功执行 WebShell、SQL 注入获取系统权限等。
2. 严重的敏感信息泄漏，包括但不限于大量用户敏感信息泄露，公司内部核心数据泄露等。
3. 严重的逻辑设计缺陷和流程缺陷，包括但不限于通过核心业务接口无限制任意账号资金消费、批量修改任意帐号密码漏洞等。

[高危]
1. 越权访问重要应用系统，包括但不限于绕过认证直接访问管理后台，后台系统弱口令等。
2. 影响一定范围用户账号或资金安全，包括但不限于：非核心 DBSQL 注入，核心页面或可造成自动传播的存储型 XSS，涉及交易、资金、密码的 CSRF，可导致用户账号安全的应用系统漏洞或业务逻辑缺陷等。
3. 敏感信息泄漏包括但不仅限于非核心 DB SQL 注入、源代码压缩包泄漏、服

务器应用加密可逆或明文、移动 API 访问摘要、硬编码等问题引起的敏感信息泄露。
4. 大范围影响用户的其他漏洞。包括但不限于可造成自动传播的重要页面的存储型 XSS（包括存储型 DOM-XSS）和涉及交易、资金、密码的 CSRF。

[中危]
1. 需交互方可影响用户的漏洞，包括但不限于影响非全量用户或非核心页面的存储型 XSS、敏感信息的 JSONP 劫持、重要操作 CSRF。
2. 普通越权操作包括但不限于不正确的直接对象引用，影响业务运行的
3. 普通信息泄漏，包括但不仅限于客户端明文存储密码、客户端密码明文传输以及 web 路径遍历、系统路径遍历。
4. 远程拒绝服务漏洞，包括但不仅限于客户端远程拒绝服务（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（默认配置情况下）。
5. 业务范围中的子域名劫持。
6. 需点击链接进行交互的 OAuth 登录或绑定劫持。
7. 能直接访问 BIGO 内网但无回显的 SSRF 漏洞需证明该漏洞点确实可以访问内网，且不得对内网服务进行扫描。

[低危]
1. 只在特定浏览器 (如低于 IE 11) 或客户端环境下才能执行，且影响较小的漏洞，包括但不限于反射型 XSS、非关键业务的存储型 XSS 等。
2. 难以利用但又可能存在安全隐患的问题。包括但不限于可能引起传播和利用的 Self-XSS、非重要敏感操作的 CSRF、短信炸弹、未猜解到用户口令的暴力破解、JSONP 漏洞。
3. 低敏感度信息泄漏包括但不限于路径泄漏、非核心代码 SVN 文件泄漏、phpinfo 以及 GitHub 泄露的非敏感系统源码及密码等。
4. 根据设备、系统、软件或框架的官方告警正在修复的漏洞。
5、反射 XSS 需要获取用户敏感 cookie，如果只是 alert(document.domain) 可能意义不大。

[无影响]
1. 无关安全的 bug，包括但不限于网页乱码、网页无法打开、某功能无法用。
2. 无法利用的“漏洞”。包括但不限于没有实际意义的扫描器漏洞报告(如 Web Server 低版本等)、Self-XSS、无敏感信息的 JSON Hijacking、无敏感操作的 CSRF、无意义的源码泄漏、内网 IP 地址/域名泄漏、401 基础认证钓鱼、程序路径信任问题、无敏感信息的 logcat 信息泄漏。
3. 无任何证据的猜测。包括但不限于自己账号被盗就表示有漏洞。

（四）威胁情报评分标准
威胁情报是指 BIGO 的产品和业务漏洞相关的情报，包括但不限于漏洞线索、攻击线索、攻击者相关信息、攻击方式、攻击技术等。由于情报分析调查的时间较

长，因此确认周期相比漏洞的时长较长，请耐心等待。

（五）威胁情报奖励标准

对应奖励如下安全币

威胁评级	严重	高危	中危	低危	无影响
完整	600	200-300	50-100	5-30	0
不完整	100-150	50-100	10-30	0-5	0

（六）威胁情报评分标准

威胁情报评分由 BIGO SRC 结合业务等级、实际影响和情报线索完整度等综合因素给予相应的情报奖金。依据情报危害程度，情报等级分为【严重】、【高危】、【中危】、【低危】、【无影响】五个等级。

【严重】

1. 核心业务服务器被入侵并且提供了相关行为特征方便快速定位确认问题点。
2. 核心业务数据库被拖取并且提供了数据库名或数据库文件、时间相关等线索。
3. 重大 0Day 漏洞。如核心服务器软件、系统等未公开或半公开漏洞，核心办公软件等未公开或半公开的漏洞等。
4. 对核心业务造成重大影响的威胁组织活动情报。如大规模盗取 BIGO 核心业务账号。

【高危】

1. 非核心业务系统的入侵线索。
2. 对核心业务造成较大影响的威胁组织活动情报，如 DDoS 攻击者的情报等。
3. 可造成重大影响的新型病毒、木马、蠕虫。如因重要业务的存储 XSS 漏洞导致的大规模蠕虫事件等。

【中危】

1. 新型可利用的工具、方法。如：如绕过策略可以扫号的工具等；（工具类需要提供攻击原理，可参考的修复方案。）
2. 一般风险的业务安全问题，如活动作弊、业务规则绕过；
3. 威胁组织基础信息，包括但不限于威胁组织相关人员、架构、规模、地域、活动情况等信息、交流及销售渠道、使用的工具和平台、造成的相关影响、行业动态等；

【低危】

1. 低风险业务安全问题。如恶意注册、刷评论等；
2. 伪造 BIGO 业务的钓鱼网站等。

【无影响】

1. 不能证实、或人为制造的虚假或无效情报等。
2. BIGO 内部已知情报等。
3. 无法还原报告情报信息或未提供有效信息等

（七）安全漏洞及威胁情报处理流程

[报告阶段]
报告者通过注册平台账户或第三方登录（如：谷歌账号）登陆 BIGO 安全响应中心平台，提交安全漏洞/威胁情报（状态：待审核）。

[处理阶段]
1. 一个工作日内，BIGO 安全响应中心（以下简称 BIGO SRC）工作人员会确认收到的 安全漏洞/威胁情报 报告并跟进开始评估问题（状态：审核中）。

2. 三个工作日内，BIGO SRC 工作人员处理问题、给出结论及评级并发放相应数量的安全币（状态：已确认/已忽略）。必要时会与报告者沟通确认，请报告者予以协助。

[修复阶段]
3. 业务部门修复 安全漏洞/威胁情报 中反馈的问题并安排更新上线（状态：已修复）。修复时间根据问题的严重程度及修复难度而定，一般来说，严重和高风险问题 24 小时内，中风险 3 个工作日内，低风险 7 个工作日内。客户端安全问题受版本发布限制，修复时间根据实际情况确定。

（八）奖励发放原则

兑换时间：白帽子在每月的最后一个工作日前完成现金兑换，逢节假日等特殊情况会另外公告通知；
打款处理：为保障广大白帽子们的利益，BIGO SRC 将于每月的第一个工作日统计上月兑换现金的人员信息，提交指定第三方负责报税及打款，逢节假日等特殊情况会另外公告通知。
到账时间：最终金额到账时间以银行为准，请大家耐心等待，感谢理解。

（九）严格禁止行为

1. 以安全测试为借口，利用情报信息进行损害用户利益、影响业务正常运作、修复前公开、恶意宣扬炒作、盗取用户数据等行为的均将不计安全币。

2. 禁止利用安全漏洞/威胁情报获取大量敏感数据，包括但不限于：
a. 账号类数据：获取 50 条以上账号信息或者用户私人信息
b. 订单类数据：获取 50 条以上包含公民信息或银行卡 cvv 等敏感字段
c. 数据库数据：获取 50 条以上数据库表字段内容

3. 禁止在测试过程中影响业务正常运行，包括但不限于：
a. 执行操作可直接影响主机/网站文件，例如 rm、mv、篡改 ssh 的 authorized_keys 等
b. 直接写入大量脏数据影响业务正常用户使用的
c. 直接在主机/网站中植入恶意后门、木马、挖矿、DDoS 等文件的

4. 禁止保存、分享通过安全漏洞/威胁情报获取到的数据信息，包括但不限于：
a. 禁止 Fork 、下载存留、分享 GIT 等途径泄露的信息文件（需在验证敏感性完成后及时进行删除操作）。

5. 发现在测试中存在以上严格禁止行为的相关处置方法：
a. 第一次，涉及的安全漏洞/威胁情报将不计安全币
b. 第二次，除不计安全币外，涉及的白帽子账号（安全币）冻结三个月
c. 第三次，除不计安全币，外涉及的白帽子账号（安全币冻结）六个月
d. 超过三次，除不计安全币外，涉及的白帽子账号作封号处理，并且安全币清零。

6、禁止对内部员工发起钓鱼邮件。

7. 特别注意：对于恶意利用安全漏洞、威胁情报，窃取敏感数据、影响业务正常运行等违规操作，除上述第五点处置外，BIGO SRC 将依照法律法规，对此类行为进行惩处。

（十）特别提醒

1. BIGO SRC 已联合 BIGO 内审部对内部员工的违规行为进行监控并纳入威胁情报收录范围内，如发现利用内部资源参与黑产活动、违规操作、收受贿赂等，还请各位白帽子对我们进行监督及反馈。

2. 在收到我司的明确书面授权之前，请不要公开披露或提供关于我司产品或服务安全漏洞的任何细节信息，不得进行任何漏洞负面炒作和公关。

FAQ

Q：BIGO SRC 会“忽略”漏洞后再偷偷修复情况？
A：绝对不会。提交的“漏洞”一旦进入“忽略”状态，审核会在备注中说明具体的忽略理由。当然也有可能因为业务本身的变动导致漏洞不再存在，但无论如何，BIGO SRC 都不会“偷偷”修复。

Q：如果对报告存在争议怎么办？
漏洞处理过程中，如果报告者对流程处理、漏洞定级、漏洞评分等有异议的，可以通过邮件、漏洞详情页面的留言板功能与 BIGO SRC 负责人员沟通。邮箱：security@bigo.sg 。

Q：BIGO SRC 一个安全币价值多少？
A：当前 BIGO SRC 平台 1 个安全币相当于 10 元人民币。