BILISRC 漏洞处理和评分标准

撰写	哔哩哔哩安全应急响应中心
文档版本	1.4
更新日期	2021-04-29
联系邮箱	security@bilibili.com

修订记录

2017-07-10 上线 BILISRC 安全应急响应中心白帽子协议

2018-03-05 修订、优化威胁情报处理流程

2018-03-14 拟订 BILISRC 漏洞处理和评分标准 V1.0

2019-02-20 评分标准：舆情、威胁情报、远程 Crash 类更新

2019-03-05 增加严格禁止行为的相关要求和处置措施

2019-04-16 提升针对提交严重、高危安全漏洞的安全币奖励

2020-09-28 修正个别漏洞评分，重新定义安全情报评分标准

2021-04-29 更新漏洞评分标准，更新业务情报接收范围，更新通用原则及禁止行为

适用范围

该评分标准仅用于对哔哩哔哩产品和业务有影响的威胁情报和安全问题。域名包括但不限于 *.bilibili.com、*.biligame.com、*.bilibiligame.net、*.acg.tv、*.hdslb.net，服务器包括哔哩哔哩运营的服务器，哔哩哔哩办公网络，产品为哔哩哔哩发布的客户端产品。注：对哔哩哔哩业务安全无实际影响的报告将不计分。

实施日期

本标准自文档发布之日起执行。

致谢

感谢 oiram、bug2048、TSRC、2233（排名不分先后）为此报告流程所做出的贡献。

（一）威胁情报反馈与处理流程

1. 报告阶段

威胁情报报告者登录哔哩哔哩安全应急响应中心，提交反馈安全问题（状态：待审核）

2. 处理阶段

根据白帽子反馈的不同威胁等级，哔哩哔哩安全应急响应中心（以下简称 BILISRC）工作人员会在一到三个工作日内，确认收到的威胁情报报告并跟进开始评估问题（状态：审核中），后续的一到三个工作日内，BILISRC 工作人员处理问题、给出结论并给予安全币（状态：已确认/已忽略）。

报告在 BILISRC 工作人员给出确认或忽略的结论后，白帽子可以在 BILISRC 前台对结论做出评判认可，若对处理结论存在较大争议可重新发起评估，提供更多细节后方便工作人员给出更好的评判结论。

3. 修复阶段

业务部门修复威胁情报中反馈的安全问题并安排更新上线。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，中风险三个工作日内，低风险七个工作日内。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。（状态：已修复）

4. 完成阶段

BILISRC 会根据威胁情报的危害等级为威胁情报报告者发出额外积分或礼品。在得到威胁情报报告者许可的情况下，BILISRC 会不定期挑选有代表意义的威胁情报进行分析，分析文章将发表在 BILISRC 官网。

（二）安全币的计算方法

安全币约合人民币 1:10 汇率。

（三）漏洞相关评分标准

根据漏洞的危害程度将漏洞等级分为【严重】、【高危】、【中危】、【低危】、【无效】五个等级。每个漏洞基础经验值最高为 10，由 BILISRC 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经验值、安全币和漏洞定级。

边缘业务的安全漏洞根据具体情况进行降级或忽略。边缘业务范围依据公司发展情况不定期调整，主要包括但不限于：

1. 测试环境的业务
2. 哔哩哔哩相关公众号
3. 与哔哩哔哩合作的产品和业务，如哔哩哔哩漫画、音频、猫耳、客服系统、我的世界中文论坛、轻视频等

每种等级包含的评分标准及漏洞类型如下：

【严重】经验值 9~10 / 安全币 500~1000

1. 直接获取核心系统权限的漏洞（服务器权限、PC 客户端权限）。包括但不仅限于远程命令执行、任意代码执行、上传获取 Webshell、SQL 注入获取系统权限、缓冲区溢出。
2. 严重的敏感信息泄漏。包括但不仅限于核心 DB（资金、身份、交易相关）的 SQL 注入，可获取大量核心用户的身份信息、订单详细信息、银行卡详细信息等接口问题引起的核心敏感信息泄露。
3. 严重的逻辑设计缺陷和流程缺陷。包括但不仅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、

【高危】经验值 6~8 / 安全币 200~400

1. 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。
2. 敏感信息越权访问。包括但不仅限于绕过认证直接访问管理后台、后台弱密码、获取大量内网敏感信息的 SSRF。
3. 直接导致业务拒绝服务的漏洞。包括但不仅限于直接导致移动网关业务 API 业务拒绝服务、网站应用拒绝服务等造成较高影响的远程拒绝服务漏洞。
4. 越权敏感操作。包括但不仅限于账号越权修改重要信息、进行订单普通操作、重要业务配置修改等较为重要的越权行为。
5. 大范围影响用户的其他漏洞。包括但不仅限于核心系统重要页面（如主站首页、分区首页、直播间首页）的存储型 XSS（包括存储型 DOM-XSS）和涉及交易、资金、密码的 CSRF。
6. 直接获取系统权限的漏洞。包括但不仅限于远程命令执行、任意代码执行等。

【中危】经验值 3~5 / 安全币 30~100

1. 需交互或其他前置条件才能影响用户的漏洞。包括但不仅限于一般页面的存储型 XSS、敏感信息的 JSONP 劫持、重要操作（如支付类操作、修改个人账号敏感信息类操作）的 CSRF。
2. 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）
3. 普通越权操作。包括但不仅限于不正确的直接对象引用。影响业务运行的 Broadcast 消息伪造等 Android 组件权限漏洞等。
4. 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。
5. 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）。
6. 普通的逻辑设计缺陷和流程缺陷。

【低危】经验值 1~2 / 安全币 10~20

1. 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（默认配置情况下）。

2. 轻微信息泄漏。包括但不仅限于路径信息泄漏、SVN 信息泄漏、PHPinfo、异常信息泄露，以及客户端应用本地 SQL 注入（仅泄漏数据库名称、字段名、cache 内容）、日志打印、配置信息、异常信息等。
3. 利用场景有限的漏洞，包括但不限于短信、邮箱炸弹，URL 跳转等。
4. 难以利用但存在安全隐患的漏洞。包括但不仅限于难以利用的 SQL 注入点、可引起传播和能够利用的 Self-XSS、URL 跳转、反射型 XSS 漏洞。

【无效】经验值 0 / 安全币 0

1. 提交的报告书写过于简单（如报告未指明业务路径、未证明漏洞危害），无法根据报告内容复现，包括但不限于和漏洞审核员反复沟通均无法复现的漏洞。
2. 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、弹幕无法显示等问题。
3. 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 的低版本）、Self-XSS、无敏感信息的 JSON Hijacking、无敏感操作的 CSRF (如添加购物车、非重要业务的订阅、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、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。
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. 无任何证据的猜测：包括但不仅限于纯属用户猜测的问题。
6. 内部已知漏洞，包括但不限于已在网络上公开的漏洞、内部安全人员已经发现的漏洞、已有其他白帽子优先提交的漏洞。

（四）安全情报评分标准

安全情报是指哔哩哔哩的产品漏洞和业务相关的情报，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（由于威胁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），主要包括漏洞情报和业务情报两大类。

1、漏洞情报评分规则

漏洞情报的综合评分（即情报经验值）由情报对应的威胁等级和情报完整度决定，漏洞情报评分对应表：

	严重	高危	中危	低危
高完整度	9～10	7～8	4～5	2
中完整度	6～8	4～6	2～3	1
低完整度	5	3	1	1

2、业务情报评分规则

业务情报的经验与同等级漏洞经验相同，金币奖励约为同等级漏洞奖励的 1/3

3、威胁等级说明

【严重】 本等级包括：对核心业务、系统、办公网络造成重大影响，或对哔哩哔哩公司造成大量资金损失的威胁情报。如主站某服务器被上传 webshell。

【高危】 本等级包括：对核心业务、系统、办公网络造成较大影响，或对哔哩哔哩公司造成较大资金损失的威胁情报。如利用其他站点泄露的他人账号密码在哔哩哔哩成功登录窃取大量账号。

【中危】 本等级包括：对核心业务、系统、办公网络造成一定影响，或对哔哩哔哩公司造成一定资金损失的威胁情报。如因业务规则漏洞问题导致被一定量用户恶意利用薅羊毛行为。

【低危】 本等级包括： 对业务、系统、办公网络造成轻微影响的威胁情报。如伪冒哔哩哔哩的钓鱼网站、盗版网站、盗版 APP、黑产交易网站、用户较多的黑产工具等。

3、情报收取范围

1）漏洞情报

1. 提供野外被利用的未知漏洞相关线索
2. 服务器或办公网被入侵且提供了入侵行为方式等相关线索
3. 重要业务数据库被拖取且提供了数据库名或数据库文件等相关线索
4. 支付业务逻辑漏洞利用、业务流程绕过等关键线索
5. 蠕虫传播且提供了蠕虫传播的链接等相关线索
6. 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
7. 能通过技术手段或其他手段影响排序机制的工具、方法等，需要有相关例子作为证明
8. 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

9.提供泄露哔哩哔哩内部信息、用户数据等行为的关键线索，网盘、GitHub 等第三方分享或泄露哔哩哔哩相关敏感文件、重要数据等

2) 业务情报

1.提供哔哩哔哩产品批量恶意账号注册、有组织的进行薅羊毛等行为的关键线索

2.提供哔哩哔哩产品刷量/作弊行为的关键线索，如：提供刷粉、抓赞、刷播放量等违规服务的网站/工具等

3.提供哔哩哔哩产品挂机/自动化行为的关键线索，如： 提供自动领取如直播间礼物等违规服务的网站/工具

4.提供哔哩哔哩视频下载行为的关键线索，如：提供哔哩哔哩版权视频/会员视频下载等违规服务的网站/工具

5.提供哔哩哔哩破解大会员行为的关键线索，如：提供破解版 APP、破解大会员服务限制等违规服务的网站/工具

6.提供哔哩哔哩黑产交易行为的关键线索，如：提供非法买卖账号、刷点赞、出售等违规服务的网站/工具

7.提供哔哩哔哩产品相关盗播网站/盗版 APP 的关键线索，如：提供大量哔哩哔哩版权视频、直播等违规服务的网站/工具

8.提供哔哩哔哩产品相关爬虫行为的关键线索，如：提供并批量爬取哔哩哔哩网站/用户相关外露信息的网站/工具

9.提供哔哩哔哩游戏类作弊行为的关键线索，如：游戏外挂、练号打金

3) 无效情报

无效情报是指错误、无意义或根据现有信息无法调查利用的威胁情报，例如：

1. 上报虚假捏造或人为制造情报信息的

2. 上报通过社工等手段诱导客服进行相关操作的

3. 上报可能刷量、引流的 QQ 群号，且未提供其他有效信息的

4. 上报已发现或失效情报的

5.上报情报中未包含攻击路径和攻击方法说明或表述不清，逻辑不通

4、情报完整度

提交威胁情报时，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。情报报告中的各项线索得分累计，作为情报的的完整性评分。 完整性评分越高，情报的完整度越高。情报中应当包含的线索以及各项线索的权重如下表说明：

威胁来源(1~2 分)	情报涉及到的威胁人员，能够帮助 SRC 对事件溯源分析、事件扩散面分析，帮助定位到入侵者个体或组织的信息；
攻击路径(1~2 分)（必须提供项）	实施攻击的个人或组织所攻击的具体页面或接口，简述主要造成何种风险，如：数据泄露、漏洞、刷关注、刷单等；
攻击方法(1~4 分)（必须提供项）	情报所涉及的问题是如何被利用的，包括相应的流程、技术手段、工具等。 如果能提供详细的技术分析，可酌情加分，最多可以追加 10 分，视分析难 度、分析结果完整性决定；
发生时间(1 分)	攻击发生所在的时间，如从 XX 时间开始，到 XX 时间结束； 针对作弊工具，可以描述该作弊工具最早出现的时间；
损失预估(1 分)	情报所提及的事件有多大规模，比如：预估有多少人参与了某次作弊； 情报所涉及的攻击已造成的损失，比如：刷了 XX 个赞、注册了 XX 个账号，薅 取了多少金额等； 针对作弊工具，可以描述该工具在黑灰产中的使用范围，比如预计有多少黑灰 产在使用；

情报完整度对应表：

情报完整度	完整性评分
高完整度	> 6 分
中完整度	3 ~ 6 分
低完整度	2 分

注意：攻击路径、攻击方法是必要线索，提交情报时如未包含其中任何一项，平台将不予审核。故情报完整性得分最低为 2 分。

（五）评分标准通用原则

1. 对于非哔哩哔哩直接发布的产品和业务或是第三方应用威胁情报均不计分
2. 通用型漏洞（如 discuz 等的漏洞以及由同一个漏洞源产生的多个漏洞）一般计漏洞数量为一个。例如 discuz 的 XSS 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、同一域名下同一组件产生的多个 flash xss 漏洞等等

3. 对于第三方库（比如 libpng、zlib、libjpeg 等等）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。同时，从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
4. 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、同一框架导致的整站问题等）
5. 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，有时可能由于报告者提供的漏洞细节不够详尽，导致 BILISRC 无法按原定时间内给出结论，请理解。因此请各位白帽子在反馈漏洞时提供 poc/exploit，并给出相应的漏洞分析细节，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最终评分
6. 同一条威胁情报，第一个报告者得分，其他报告者不得分
7. 提交网上已公开的威胁情报不计分
8. 拒绝无实际危害证明的扫描器结果，具体参见《哔哩哔哩安全应急响应中心白帽子协议》

（六）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会计分
2. SQL 注入漏洞禁止读取表内数据，只要证明可以读取数据就行。对于 UPDATE、DELETE、INSERT 等注入类型，禁止使用自动化工具进行测试。
3. 越权漏洞禁止进行批量读取，越权读取的时候，允许读取到的真实数据不超过 5 组。
4. 测试 XSS 漏洞，证明危害即可，禁止进行获取其他用户 cookie 或用户信息等敏感操作。
5. 如果可以 shell 或者命令执行的，推荐上传一个文本证明，如纯文本的 1.php、1.jsp 等证明问题存在即可，禁止下载和读取服务器上任何源代码文件和敏感文件，禁止执行删除、写入命令，如果是上传的 webshell，请写明 shell 文件地址和连接口令。

6. 在测试未限制发送短信或邮件次数等扫号类漏洞，请使用自己的手机号或邮箱，禁止对其他用户进行轰炸测试
7. 禁止进行物理测试、社会工程学测试或任何其他非技术手段测试
8. 禁止进行内网渗透行为，如内网扫描、主机提权等行为。
9. 禁止进行可能引起业务异常运行的测试，例如：IIS 的拒绝服务等可导致拒绝服务的漏洞测试以及 DDOS 攻击。
10. 禁止保存、分享通过安全缺陷/问题/威胁情报获取到的数据信息（包括但不限于）：
    a. 禁止 Fork 、下载留存、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）
    b. 禁止未经 BILISRC 官方允许，擅自对外公布所发现的安全缺陷/问题/威胁情报细节、展示其中包含的敏感数据内容
11. 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，涉及的安全缺陷/问题/威胁情报将不计分
    b. 第二次，除不计分外涉及的白帽子账号（积分冻结）三个月
    c. 第三次，除不计分外涉及的白帽子账号（积分冻结）六个月
    d. 超过三次，除不计分外涉及的白帽子账号积分做归零处置
12. **特别注意：**对于恶意利用安全缺陷/问题/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，哔哩哔哩安全将依照法律法规，对此类行为进行惩处

（七）问题与解答

Q：什么时候发送兑换的礼物？

为方便诸位大佬能够及时和满意的兑换到 BILISRC 的礼物和奖品，现礼物兑换时间为「每月的 15 号之后～次月的 10 号之前」，统一固定发货日为：每月 15 号，如遇到节假日酌情提前或顺延到工作日。

Q：BILISRC 与其他安全团体的关系是如何的？

哔哩哔哩安全离不开业界的支持与帮助，哔哩哔哩安全应急响应中心愿意与各个安全团体深度合作，共同推动安全行业的健康发展。目前 BILISRC 已经与一些安全厂商展开了合作，未来将会有更多合作。

Q：哔哩哔哩威胁情报奖励计划是不是用奖品隐瞒安全问题？

不是。首先，我们认为，在威胁情报中的安全问题未修复前，为了保护用户群体的利益，威胁情报不应该被提前公开，这也是业界的通用做法。其次，哔哩哔哩为威胁情报报告者提供礼品等奖励是为了表达对报告者的感谢和尊重，绝对不是用奖品隐瞒威胁情报中的安全问题。

Q：哔哩哔哩会不会先『忽略』漏洞然后偷偷修复？

绝对不会。提交的报告一旦进入『忽略』状态，跟进同事会回复忽略的原因。常见情况是这个『漏洞』不认为是漏洞而被评估为一个 bug ，BILISRC 仅知会相关产品同事，是否更改这个『bug』将由产品同事决定；另外一种情况是业务本身的变动，导致问题不复存在。但是不论如何，哔哩哔哩方面都不会偷偷修复漏洞。

Q：如果对报告存在争议怎么办？

在漏洞报告处理过程中，如果报告者对流程处理、漏洞定级、漏洞评分等有异议的，可以通过漏洞详情页面的留言板、前台评判功能或者通过联系 security@bilibili.com 邮箱进行沟通。我们将按照漏洞报告者利益优先的原则处理，必要时可引入外部安全人士共同裁定。