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	1.2
更新日期	2019-04-16
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

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

威胁情报报告者登陆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，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、任意账号登录漏洞等。

【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。
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. 需交互方可影响用户的漏洞。包括但不仅限于一般页面的存储型 XSS、反射型 XSS（包括反射型 DOM-XSS）、重要操作 CSRF、URL 跳转漏洞。
2. 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。
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. 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. 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、需构造部分参数且有一定影响的 CSRF。

【无效】经验值 0 / 安全币 0

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、弹幕无法显示等问题。
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 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。
3. 无任何证据的猜测：包括但不仅限于纯属用户猜测的问题。

（四）威胁情报评分标准

威胁情报是指哔哩哔哩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），接收范围如下：

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. 蠕虫传播且提供了蠕虫传播的链接等相关线索
5. 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
6. 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
7. 更多根据业务情况进行判断存在较大影响的安全线索

无效的威胁情报范围：

1. 炒信的信息，且未提供具体有效内容的
2. 通过社工等手段诱导客服进行相关操作的
3. 虚假、捏造或人为制造情报信息
4. 已发现或失效情报的

（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. 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
5. 同一条威胁情报，第一个报告者得分，其他报告者不得分
6. 提交网上已公开的威胁情报不计分
7. 非核心业务的情报等级将结合情报影响程度作降级判定
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. 禁止利用安全缺陷/问题/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的敏感字段
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 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
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
6. **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。