字节跳动
安全中心

字节跳动安全中心安全报告处置规则 V3.0

版本号	修订内容	发布日期
V3.0	评分标准、业务等级、情报标准等	2020.7.21
V2.1	等级判断标准、业务等级说明	2020.1.13
V2.0	评分细则、业务等级、情报收取范围等	2019.12.24
V1.1	更新中危、低危漏洞的定义	2018.6.20
V1.0	网站正式版本	2018.6.01

第一章 基本原则

1、字节跳动非常重视产品及业务的安全问题，字节跳动安全中心（ByteDance Security Center）（以下称“我们”）作为连接平台，期待白帽子、安全组织、研究者（以下称“您”）等能够一起加入，完成“合作式安全报告披露与处置”，为共建良好互联网安全生态而努力。

2、我们将对您提交的每一份报告指定专人跟进、分析和处理，并及时予以反馈。对于每一位恪守白帽子精神、帮助字节跳动发现安全风险的报告者，我们将给予以感谢和丰厚回馈。

3、以漏洞测试为借口，利用漏洞进行损害用户利益、影响业务运作、盗取用户数据等行为的，或以漏洞作为要挟或进行贿赂行为的，我们将不予奖励，并保留进一步追究法律责任的权利。

4、未经允许任何人不得对外披露漏洞细节，或利用漏洞非法获利。如您泄露了漏洞信息或利用漏洞非法获利，我们将不给予奖励，已给予的奖励有权收回，并对情节严重者保留进一步追究法律责任的权利。

5、字节跳动员工不得参与或通过朋友参与漏洞奖励计划。如经查发现是字节跳动员工参与本奖励规则所述的活动，我们有权不给予奖励，已给予的奖励有权收回，并将保留进一步内部处理的权利。

6、您在“字节跳动安全中心”平台获得奖励所产生的个税，将由平台统一承担。您应知悉我们为您代扣代缴的个税，属于综合所得的部分，则将体现在个人所得税年度汇算中。

7、当您在“字节跳动安全中心”平台进行礼品兑换时，我们将收集您的姓名、通信地址、联系方式、身份证号码等信息。这些信息是我们向您寄送礼品和个税登记扣缴所必须的信息，如果您拒绝提供，我们将无法完成礼品发放。

8、当您在“字节跳动安全中心”平台领取现金奖励时，我们还将进一步收集您的的银行账号（用于汇款）及身份证号码（用于个税登记和扣缴）。如果您拒绝提供，将无法完成相关款项支付。

9、本评分规则将进行不定期修订，通过“字节跳动安全中心”平台发布即生效，发布之后会以醒目方式将新规则供您查阅。

10、如果您对本流程有任何意见建议，通过 QQ:3472473732 向我们反馈，您的建议一经采纳，我们将送出精美的礼品作为答谢。

第二章 平台奖励

请您在 security.bytedance.com 上提交完整详尽的安全报告，完整规范的报告模板详见漏洞报告规范书写模版。

字节跳动安全中心奖励目前由**报告质量奖励、漏洞/情报奖励、特殊漏洞/情报贡献奖、平台特色奖励** 4 个版块构成，将依据行业情况、用户需求不断升级完善。平台日常奖励将以积分形式奖励。

2.1 报告质量奖励

完整清晰的安全报告是获得奖励的基础，有助于快速定位问题，完成审核，**漏洞报告的详细程度会影响最终得分，**因此请白帽子提交的安全报告务必包含「漏洞标题」「漏洞描述」「复现过程」等信息，否则将被做忽略处理。详见漏洞报告规范书写模版。

- 对于书写特别规范、清晰、详尽的报告，或漏洞利用思路新颖，审核同学将给予 5-50 分的附加分奖励。我们保留对附加分奖励规则的最终解释权。
- **漏洞报告内容需包含**
  - 【漏洞标题】包含漏洞题目、影响域名、漏洞类型等
  - 【漏洞描述】包含漏洞的入口、涉及的 URL、参数、应用版本等
  - 【复现过程】按步骤对漏洞进行复现，并在过程中体现漏洞的影响和危害，一般以文字截图形式，若使用工具，请提供工具名称
  - 【修复方案】请提供可执行的修复建议，如代码修复建议或防护策略

2.2 漏洞奖励

1、漏洞计分规则

漏洞/情报得分= 基础积分 * 业务系数

基础积分依据 **严重、高危、中危、低危、无影响（忽略）**五个等级进行判断，

等级规则详见 2.2-2

业务系数依据 **高系数类、中系数类、低系数类** 三个等级及**威胁等级**进行判断，

业务系数详见 2.2-3

漏洞积分(分)				
	严重	高危	中危	低危
基础积分	12、10、8	9、8、7	6、5、4	3、2、1
对应系数				
高系数类	150	80	20	5
中系数类	60	30	10	3
低系数类	20	10	5	1

漏洞对应价值（元）				
	严重	高危	中危	低危
高系数类	18000、15000、12000	7200、6400、5600	1200、1000、800	150、100、50
中系数类	7200、6000、4800	2700、2400、2100	600、500、400	90、60、30
低系数类	2400、2000、1600	900、800、700	300、250、200	30、20、10

2、漏洞等级评审标准

1）严重漏洞

- 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：远程命令执行漏洞、任意代码执行漏洞、SQL 注入获取系统可执行权限、缓冲区溢出
- 泄露大量核心敏感数据的漏洞，包括但不限于：核心 DB 的 SQL 注入漏洞、用户敏感信息接口越权导致的大范围泄露
- 核心系统的严重逻辑设计缺陷或流程缺陷，包括但不限于批量修改任意账号密码漏洞、任意账号登陆、支付系统逻辑漏洞
- 客户端大量敏感信息泄露的漏洞，包括但不限于远程获取用户大量敏感信息、本地越权访问 TEE 保护的支付相关或者用户认证相关信息、TEE 任意代码执行(高权限)
- 设备端安全机制绕过，包括但不限于绕过 SELinux

- 远程系统级永久性拒绝服务攻击

2） 高危漏洞

- 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：远程命令执行漏洞、任意代码执行漏洞、上传 WebShell、SQL 注入获取系统权限、缓冲区溢出、回显 SSRF 漏洞
- 泄露大量重要敏感数据的漏洞，包括但不限于：非核心 DB 的 SQL 注入漏洞，可自动传播的存储型 XSS 漏洞，可获得重要数据操作权限的漏洞
- 重要系统敏感越权操作漏洞
- 造成客户端本地敏感信息泄露的漏洞，包括但不限于越权、命令执行的利用
- 客户端远程永久性拒绝服务
- 因字节产品导致的移动端系统级安全机制绕过(包括不限于锁屏、认证等)

3） 中危漏洞

- 普通信息泄露 ,包括但不限于包含敏感信息的完整源代码泄露、无信息回显的 SSRF 漏洞
- 普通系统越权操作漏洞
- 存储型 XSS 漏洞、敏感信息的 JSONP 劫持、重要敏感操作的 CSRF 漏洞
- 设备端保护功能绕过，如手机找回，出厂设置保护，密码保护
- 客户端远程临时性拒绝服务

4） 低危漏洞

- 轻微信息泄露漏洞 ,包括但不限于路径泄露、.git 文件泄露、Django Debug、phpinfo、服务端业务日志内容
- 频控缺陷漏洞，包括但不限于短信炸弹、用户账户密码暴力破解
- 可用于钓鱼或黑产的漏洞，包括但不限于任意 URL 跳转、反射型 XSS 漏洞
- 容易被利用的或产生较大影响的客户端不安全配置漏洞

5） 忽略

- 提交的报告书写过于简单，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
- 内部已知漏洞，包括但不限于通用平台如 Jenkins 等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
- 无法利用或无危害的报告，包括但不限于恶作剧 CSRF（对用户无实际影响）、无法影响他人的本地拒绝服务 、Self-XSS、非敏感信息泄露（内网 IP、域名）等

- 与字节跳动无关的漏洞
- 和安全无关的 Bug 类问题，包括但不限于网页打开比较缓慢、样式杂乱

6）特殊说明

- 如提交的漏洞不包含于上述内容中，则字节安全中心将按照漏洞的实际危害性、影响范围、利用难度等进行等级评估和调整
- 同一漏洞源产生的多个漏洞按照一个漏洞计数，如同一个 JS 引起的多个安全漏洞、同一个发布系统引起的多个页面的安全漏洞、框架导致的整站的安全漏洞、泛域名解析产生的多个安全漏洞等
- 涉及到第三方组件漏洞，如 UC 浏览器内核、第三方库、Android 或 Chromium 的原生漏洞等，按下述方式处理：
  - 如果提交相关基础组件 nday 漏洞，提交的漏洞已公开，时间在半年内且字节跳动已知晓该漏洞，则忽略/驳回，不予记分；若字节跳动不知晓该漏洞，或者该漏洞已公开时间超过半年，字节跳动仍未修复，会根据实际攻击演示效果来评估定级，需提供 nday 具体链接及 CVE 编号，并且需提供了可利用证明（如 poc 能证明造成信息泄露、控制 pc 等）
  - 如果提交相关基础组件 0day 漏洞，且提供了可利用证明（如 poc 能证明造成信息泄露、控制 pc 等）会根据实际攻击演示效果来评估定级

3 、漏洞业务系数说明

1）高系数类

今日头条、抖音短视频、抖音火山版、西瓜视频、飞书五款产品的主营业务

2）中系数类

皮皮虾、懂车帝、Faceu 激萌、轻颜相机、剪映、巨量引擎(即*.oceanengine.com，主要有广告投放平台、穿山甲、云图、星图、即合、飞鱼、橙子建站)、清北网校、开言英语、GoGoKid、好好学习、瓜瓜龙、汤圆英语、头条百科、悟空问答、坚果品牌系列产品、图虫、东方 IC、时光相册

3）低系数类

低系数类指除以上外，属字节跳动投资、合资的公司且其业务已由字节跳动负责研发和运维。

注：业务系数将依据公司发展情况不定期调整

2.3 情报评分标准

1、 情报评分规则

情报评分根据情报线索的完整性和威胁等级计算得出，计算公式为：

情报综合得分 = 情报完整性得分 × 威胁等级

评分规则对应表：

情报评分规则				
威胁等级	严重(60~80)	高危(20~30)	中危(5~10)	低危(1)
最完整报告(15)	900~1200 分	200~450 分	75~150 分	15 分
~	~	~	~	~
最不完整报告(2)	120~160 分	40~60 分	10~20 分	2~4 分

2、 情报收取范围

1）安全情报

- 服务器被入侵且提供了入侵行为特征等关键线索
- 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
- 支付业务逻辑漏洞利用、业务流程绕过等关键线索
- 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
- 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
- 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

2）业务情报

- 提供字节跳动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
- 提供泄露字节跳动内部信息、用户数据等行为的关键线索，网盘、GitHub 等第三方分享或泄露字节跳动相关敏感文件、重要数据等
- 提供字节跳动产品刷量行为的关键线索，如：关注、分享、点赞、评论、阅读量、播放量等
- 提供字节跳动直播类作弊行为的关键线索，如：刷人气、抢红包等
- 提供字节跳动支付类作弊行为的关键线索，如：苹果 IOS 代退款
- 提供字节跳动游戏类作弊行为的关键线索，如：游戏外挂、练号打金

3 、情报完整性评分

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。

情报中应当包含的线索以及各项线索的权重如下表 4 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(1~3 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；
攻击方法(1~5 分) **（必须提供项）**	情报涉及的作弊或攻击所使用的技术手段、流程步骤或工具等； 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；
风险类型(1~2 分)	简要分析情报所涉及的主要问题，如：数据泄露、漏洞、刷关注、刷单等 ；
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(1~2 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；

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。

4 、情报特殊计分说明

- 相同情报内容，首位报告者计分，其他报告者均不计
- 报告评分与线索详细程度相关联。
- 未经允许对外披露情报内容，将不予记分，已支付的有权收回

5 、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：

- 上报虚假捏造或人为制造情报信息的

- 上报可能刷量、引流的 QQ 群号，且未提供其他有效信息的
- 上报单个或少量用户的非业务规则问题导致的刷量行为
- 上报已发现或失效情报的
- 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

2.4 特殊漏洞/情报贡献奖

当安全报告被判定为有效的高系数严重漏洞/情报时，根据漏洞/情报的实际危害，我们将对此进行二次评定，视情况评估是否再给予 **1-20W** 的额外现金奖励。我们保留对额外现金奖励规则的最终解释权。

2.5 平台特色奖励

平台将不定期推出或升级新人奖励、忠实白帽子奖励、个人/团队奖励、年度奖、活动奖励等一系列奖励计划，奖励发布详情，请关注「字节跳动安全中心」公众号或在官网公告查看。

字节跳动安全中心

2020 年 7 月 21 日