TSRC 漏洞处理和评分标准

编写人	**腾讯安全应急响应中心（TSRC）**
版本号	**3.2**
最后更新日期	**2023-04-24**

致谢

感谢 7DScan、alert7、cnhawk、Dragon、DragonEgg、guimaizi、hj@topsec、iceyes、instruder、沦沦、买不起的牌子、MythHack、nforest、papaya、PiaCa、PP、pytho1n、钱途、扫地僧、Sowhat、SuperHei、TK、WooYun.org、xsjswt、天道筑基、tzrj、upme4、月神（根据 ID 首字母排序）等安全专家为本标准所作出的贡献。

如果您对本标准有任何的建议，欢迎通过 TSRC 官方邮箱（security@tencent.com）或者微信公众号（tsrc_team）的方式向我们反馈。

适用范围

本标准适用于腾讯威胁情报反馈平台（https://security.tencent.com/）所收到的所有情报。

实施日期

本标准自 2023 年 5 月 4 日起施行。

修订记录

V1.0 2012-10-30　发布第一版
V1.1 2012-12-05　更新评分标准的通用型漏洞定义；更新奖励发放原则；更新 FAQ
V1.2 2013-01-16　更新评分标准；更新奖品发放流程；更新 FAQ
V1.3 2013-03-22　更新奖品发放流程；更新评分标准
V1.4 2013-08-12　更新争议解决办法流程；更新 Discuz!产品的评分标准
V1.5 2013-09-01　更新客户端产品奖励标准；更新评分标准
V1.6 2014-02-12　更新评分标准；更新奖励发放原则
V1.7 2014-05-05　更新客户端产品奖励标准；更新评分标准
V1.8 2014-06-04　更新奖励评分标准；更新评分标准通用原则；更新 FAQ
V1.9 2014-11-10　更新奖励评分标准；更新评分标准通用原则
V2.0 2015-04-16　更新奖励评分标准；更新评分标准通用原则；更新 FAQ
V2.1 2015-10-15　更新奖励评分范围及标准；更新评分标准通用原则；更新 FAQ
V3.0 2020-05-21　每个章节均有不同程度的更新
V3.1 2021-11-17　更新基本原则补充需遵守《TSRC 安全测试规范》；更新第三方软件通用漏洞接收说明
V3.2 2023-04-24　更新评分及奖励标准

目录

基本原则

1）腾讯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）腾讯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，腾讯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提供有效帮助的报告者，腾讯也会酌情给予相应的奖励。

3）腾讯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，帮助腾讯提升安全质量的用户，我们将给予感谢和回馈。

4）腾讯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）腾讯反对和谴责一切利用安全漏洞恐吓用户、攻击竞争对手的行为。

6）腾讯认为每个安全漏洞的处理和整个安全行业的进步，都离不开各方的共同合作。希望企业、安全公司、安全组织、安全研究者一起加入到“负责任的漏洞披露”过程中来，一起为建设安全健康的互联网而努力。

7）请报告者严格遵守《SRC 行业安全测试规范》(https://security.tencent.com/index.php/announcement/msg/180)和《TSRC 安全测试规范》(https://security.tencent.com/index.php/announcement/msg/266)。

评分标准通用原则

1）评分标准仅针对对腾讯产品和业务有影响的威胁情报。域名包括但不限于*.qq.com、*.tencent.com、*.tenpay.com，服务器包括腾讯运营的服务器，产品为腾讯发布的客户端产品。对腾讯业务安全无影响的威胁情报，不计分。(注：易迅、拍拍等业务已移交给京东)。

2）由于业务调整，不再更新的客户端产品（包括但不限于 QQ 影像、QQ 安卓 HD 版、企业邮箱 IOS 版、朋友网安卓版、QQ 便民、手机 QQ 浏览器国际版、QQ 旋风等）将不予计分。

3）对于非腾讯直接发布的产品和业务或是腾讯开放平台的第三方应用威胁情报（域名包括但不限于是*.qzoneapp.com, *.myqcloud.com，*.tgovcloud.com、*.qqopenapp.com、*.saas.g-proxy.com、*.dothework.cn 等），均不计分。

4）通用型漏洞或同一个漏洞源（同一组件、产品、系统）产生的多个同类问题一般计漏洞数量为一个，并根据漏洞实际报告情况给予一定的额外倍数奖励。例如同一个 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、客户端同一个第三方组件引起的多个 RCE 漏洞。

5）具有互相依赖的关系和条件的多个漏洞，按照多个漏洞共同影响下能达到最大的危害评分，如后台弱口令导致的多个漏洞最终可造成命令执行和文件读取，仅按命令执行评分；又如多个漏洞导致文件读取和 SSRF 漏洞，评分应当高于 SSRF 漏洞低于命令执行漏洞评分。

6）对于缺乏关键因素（文字描述、图片证明、测试过程、风险接口和参数等），报告排版混乱，无法稳定复现的报告，仅提供请求不解释请求来源复现步骤的，仅提供敏感信息（密码密钥等）无法解释来源或来源违反 TSRC 相关规范的将做降级/忽略处理；任何漏洞需要提供可稳定复现的 exploit，未提供的评分不超过【中】；需要爆破难度较大的字段，例如 6 位及以上的验证码等，如不能在短时间内稳定复现，会降级或者忽略处理。以上降级/忽略处置自报告起至评分后 5 个工作日内解释说明、补充证明的不予降级，逾期解释不接受调整评分。

7）如果提交相关基础组件 nday 漏洞，提交的漏洞已公开，时间在 3 个月内且内部知晓该漏洞正在推修中，则忽略/驳回。例如同一产品的 chromium 内核漏洞，在修复周期内，重复报告其他问题不计分。

8）对于第三方库（比如 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。

9）对于移动终端系统导致的通用型漏洞，比如 webkit 的 uxss、代码执行等，仅给首个漏洞报告者计分，对于其它产品的同个漏洞报告，均不再另外计分。

10）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 TSRC 无法按原定时间内 给出结论，请各位白帽子理解。因此请各位白帽子在反馈漏洞时提供 poc/exploit 与验证视频，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。

11）如果同一时间周期内提交同一客户端的多个漏洞，请报告者在反馈漏洞时明确给出导致漏洞和触发漏洞的关键代码，以帮助快速确认是否为相同漏洞，加快漏洞确认时间。

12）对于第三方通用型漏洞导致的安全问题，依据通用漏洞奖励标准。

13）威胁情报报告者复查安全问题时如果发现安全问题仍然存在或未修复好，当作新威胁情报继续计分。

14）同一条威胁情报，第一个报告者得分，其他报告者不得分；提交网上已公开的威胁情报不计分。

15）拒绝无实际危害证明的扫描器结果。

16）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、盗取用户数据等行为的，将不会计分，同时腾讯保留采取进一步法律行动的权利。

17）禁止未经腾讯授权，私自公开漏洞的行为，一旦发现严肃处理，包括奖励取消、账户禁用等。

18）本标准所有内容最终解释权归 TSRC 所有。

威胁情报反馈与处理流程

[预报告阶段]
威胁情报报告者授权腾讯威胁情报反馈平台(https://security.tencent.com/index.php/report)生成帐号。

[报告阶段]
威胁情报报告者登陆腾讯威胁情报反馈平台，提单反馈威胁情报（状态：待审核）。

[处理阶段]
1）一个工作日内，腾讯安全应急响应中心（以下简称 TSRC）工作人员会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）。

2）RCE、SQL 注入、全回显 SSRF、任意文件读取等严重/高危漏洞在 3 个工作日跟进处理问题，给出结论并计分。

3）核心业务漏洞在 3 个工作日跟进处理问题，给出结论并计分。

4）其余漏洞在 7 个工作日内完成评分，如报告者认为属于紧急情况可以联系审核 QQ 加急处理。

[修复阶段]
1）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（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。

2）威胁情报报告者复查安全问题是否修复（状态：已复查/复查异议）。

[完成阶段]
1）TSRC 每月发布上月威胁情报处理公告，向上月的威胁情报报告者致谢并公布威胁情报处理情况。

2）威胁情报报告者可以使用安全币在虚拟市场置换现金或礼品，置换完成后，TSRC 为威胁情报报告者发出现金或礼品；同时不定期也会有奖励及线下活动。

3）在得到威胁情报报告者许可的情况下，TSRC 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 TSRC 官网。

威胁情报评分标准

腾讯威胁情报主要包含三大部分的内容：业务漏洞、安全情报、通用软件漏洞。

根据目前腾讯产品的重要程度和发展现状，我们将在漏洞赏金范围内的产品划分为核心产品、重点产品、其他产品，下面我们将分别描述其范围和评分标准。

核心产品范围描述

目前在漏洞奖励计划中的“核心产品”范围仅包含以下可影响腾讯绝大多数用户的核心产品功能（列表会持续更新）：

微信（Android, iOS, WinPC, Mac）
微信即时通讯功能
微信登录/票据
微信通讯录
微信朋友圈
微信公众号
微信小程序主框架 API
企业微信（Android, iOS, WinPC, Mac）
企业邮箱主域(*.exmail.qq.com)
企业微信管理后台
企业微信通讯录
企业微信即时通讯功能
QQ 邮箱主域（*.mail.qq.com）
企业微信基础核心功能（企业微信即时通信功能、企业支付、会话内容存档、微盘、微文档、融合会议、企微朋友圈）
企业微信敏感信息如：企业通讯录列表，登录/票据
微信支付功能（不包含支付引导页网格所推荐的服务）
微信钱包
微信支付自研刷脸设备
微信支付自研刷掌设备
微信支付商户平台（包括境内和境外）
微信信用卡还款
财付通
理财通
腾讯手机充值
腾讯自选股
王者荣耀手游
和平精英手游
心悦俱乐部
成长守护平台
QQ 客户端（Android, iOS, WinPC, Mac）
QQ 基础核心功能（如即时通讯功能、用户资料、登录/票据等）
QQ 钱包（不包含钱包引导页网格所推荐的服务）
腾讯文档（不包含第三方提供插件）
腾讯视频主站和移动端 APP（Android, iOS）
腾讯会议
腾讯云（计算/容器与中间件/存储/网络与 CDN/安全）（参考腾讯云产品总览-腾讯云中对应的产品 https://cloud.tencent.com/product）
电脑管家/手机管家
DNSPOD

重点产品范围描述

包含绝大部分的腾讯旗下产品和业务，例如腾讯游戏助手、腾讯乘车码小程序、QQ 音乐等产品，包括但不限于移动应用、客户端、小程序、Web 站点、硬件、IOT、服务器服务等产品模式。

其他产品范围描述

腾讯公司旗下其他业务所产生的移动应用、客户端、小程序、Web 站点、硬件等相关产品；一般表现为平台用户少于千人，平台数据实时性低于 1 天，客户端产品较长时间未更新等；也包含非腾讯进行开发、运维和运营的应用、小程序后端 API 站点、服务器等。

TSRC 贡献值体系

基于以上的产品范围描述，TSRC 针对不同产品范围的安全报告构建起 TSRC 贡献值体系，并根据该体系作为主要参考为白帽子提供奖励。

计算公式：单个漏洞贡献值 = 积分 * 贡献系数

依据该体系，当白帽子提供一个核心产品(见上述核心产品范围描述)的严重漏洞并获得最终确认时，白帽子将可能获得至少 9 * 286 = 2574 的安全币奖励。其余情况见下表：

TSRC 贡献值体系				
危害分级	积分	贡献系数		
		其他	重点	核心
低	1-2	4	12	22
中	3-5	5	18	35
高	6-8	11	90	134
严重	9-10	18	192	286

1 个安全币价值人民币 5 元，所以对应的现金奖励范围如下：

TSRC 贡献值体系				
危害分级	积分	现金奖励范围（单位：元）		
		其他	重点	核心
低	1-2	20-40	60-120	110~220
中	3-5	75-125	270-450	525~875
高	6-8	330-440	2700~3600	4020~5360
严重	9-10	810-900	8640~9600	12870~14300

漏洞报告质量奖

同时我们鼓励白帽子提供更加清晰、定位明确且能帮助业务快速跟进的漏洞报告，并为高质量报告者提供最高 5000 元人民币的现金奖励。
当白帽子为其发现的安全问题编写并提供优质报告时，白帽子就有机会在漏洞确认后直接通过额外的安全币获得该奖励。TSRC 将根据优质报告的实际情况，为不同的报告分配相应额度的漏洞报告质量奖。

例如：漏洞利用链复杂或需多账号多动作才可以达成利用效果的漏洞，逐步编写漏洞利用流程，并为每个动作提供如 HTTP 请求包文本、测试思路、详细的 Payload、可一键执行并复 现的 POC 脚本或已尝试的 Payload 列表和日志等信息，帮助 TSRC 和业务同事快速准确地复现、跟进和修复漏洞；满足以上情况的报告将有机会获得漏洞报告质量奖。

严重漏洞额外现金奖

对于为核心业务或重点业务提供高质量严重漏洞报告的白帽子，TSRC 将额外提供现金奖励，通过“月度奖励”形式进行发放。奖励标准如下：
核心产品的严重漏洞：税后 3 万以上人民币
重点产品的严重漏洞：税后 1～3 万人民币

业务额外奖励

“业务额外奖励”系腾讯业务团队根据每次活动设置的悬赏规则，悬赏规则于每次活动前公布，凡满足相关规则者，均可获得业务额外奖励。

年度特别奖励

根据白帽子报告所获得的贡献值评选年度特别奖励获得者。

业务漏洞评分标准

每个漏洞会根据技术维度和业务维度进行综合评估，技术维度主要包括用户交互、攻击媒介、前置条件等三个方面。

用户交互	无交互	不依赖用户交互，攻击者可自主完成整个攻击流程。或者用户100%可以触发，比如打开首页或者任意页面即可触发
	低交互	用户访问某些通用页面即可触发，比如 正常浏览产品页面，浏览某个特定页面，打开某个特定链接
	高交互	用户需完成特定交互，或者超过两步交互（含两步），比如：访问特定链接、页面后点击某个功能，浏览邮件后点击转发等等
攻击媒介	远程网络	可以通过网络远程利用的，可跨网段远程利用
	局域网	可以通过相邻的网络进行利用，比如共享的物理（蓝牙、无线）或者逻辑（本地局域网）网络，进行漏洞利用
	本地	需要在目标电脑操作系统本地完成利用的。通常需要攻击者登录本地系统，或者依赖用户交互执行恶意的本地文件来进行漏洞利用
前置条件（权限/信息）	无	攻击者可自主完成整个攻击流程，不需要前提权限或者数据。
	一定条件	需要一定权限或者数据才能完成攻击，比如：需要知道目标用户的ID、邮箱、手机号等前置条件，或者需要一定的初始权限，比如登录后台。
	较高条件	需要获得其他用户的账号控制权，或者管理员账号才能利用的。需要提前知道一些要求较高的信息，比如：完全无法猜解的物理路径、无法猜测的ID、或者需要遍历6位以上的ID等。

业务维度主要包括功能重要程度、影响数量、平台活跃度等

业务因素	功能重要程度	重要功能，例如社交类APP中的通信功能
		不重要功能
	影响条目	巨量（>100w）
		大量（>1w）
		少量（<1000）
	平台活跃度	用户基数大于1000
		用户基数小于1000

根据漏洞危害程度分为严重、高、中、低、无五个等级，每个等级评分如下，每个等级也会按照上表进行综合评判，重要程度低、影响小、需要额外条件的将在原有评分上依情况减少评分。

[严重]
1） 直接获取权限的漏洞（仅限于腾讯所属的服务器权限、核心产品客户端权限）。包括但不限于远程任意命令执行、上传 webshell 等。

2） 直接导致严重的信息泄漏漏洞，仅限于微信、QQ、王者荣耀等平台或后续产生的同体量平台，涉及的可影响用户身份信息安全的信息。

3）直接导致严重影响的逻辑漏洞。包括但不限于伪造任意 QQ、微信账号给任意用户发送可完全自定义内容的消息，任意 QQ、微信帐号密码更改漏洞。如果漏洞利用时仅可弹出骚扰无法指定可阅读的内容，则不适用于定级为严重漏洞。

4）直接影响现金的，需满足可直接提现且无利用限制，并且影响金额超过 10 万。

[高]
1）能直接盗取用户身份信息的漏洞。包括 QQ 空间、QQ 邮箱、企业邮箱、WEB 微信、微信公众号产品的存储 XSS 漏洞（低交互易传播可影响大量用户）、腾讯业务站点的可读取数据库表字段名的 SQL 注入漏洞（注：SQL 注入白帽子可读取当前表的第一个字段的前 两个字符作为佐证，不可直接利用 SQL 注入获取用户数据；存储型 XSS 漏洞不建议采取盲打、破坏页面结构等类型的 payload 语句，建议采用 console.log 方式验证）。

2）未授权访问管理平台并使用管理员功能，包括但不限于敏感管理后台登录；相关平台的活跃度、用户基数（用户不少于千人）、功能重要性、用户信息敏感度等都将作为高危漏洞的评级标准。

3）高风险的信息泄漏漏洞。包括但不限于可直接利用的敏感数据泄漏，可导致站点大量用户身份信息泄露的漏洞或直接对业务造成高风险的信息。需泄漏三个及以上的敏感信息字段，且影响数量超过一万条；如不满足，按照实际情况酌情评分（敏感信息字段是指个人真实姓名、身份证号、住址、联系方式（手机号、微信、QQ）、银行卡号，完整交易信息，医疗信息等）。

4）直接远程获取客户端权限的漏洞。包括但不限于远程任意命令执行、可利用的远程缓冲 区溢出、可利用的浏览器 use after free 漏洞、远程内核代码执行漏洞以及其它因逻辑问题导致的远程代码执行漏洞。

5）能直接访问腾讯内网且可获取回显的 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；另外 SSRF 不区分业务性质，统一按照重点业务计分。SSRF 评级：无回显 SSRF 中 3，仅图片回显 SSRF 中 4，部分回显 SSRF 高 6（例如回显字数有限制，PS：图片回显不算做此类），全回显 SSRF 高 7；SSRF 会提供 IP 和域名两种方式验证，如果可同时访问，正常评分；如果只能访问域名或 ip，则会做相应降级。（SSRF 测试域名：http://tst.qq.com/flag.html；SSRF 测试 IP：http://10.204.9.230/flag.html，使用方式详见：https://security.tencent.com/index.php/announcement/msg/212）

6）可获取敏感信息或者执行敏感操作的核心客户端产品的 XSS 漏洞。

7）越权使用他人身份进行所有功能操作。

8）在业务、产品预期之外，单用户可任意刷取具有现金价值的虚拟商品（比如：一个月及以上的会员、点券、仅单产品内的数字资产、游戏内 RMB 道具、无门槛现金优惠券、免费无限使用腾讯云服务器等等），影响现金价值超过 5000 元。
9）任意文件读写漏洞，包括业务使用的能进行全站的 COS 任意文件读写、覆盖漏洞。

[中]
1）需交互才能获取用户身份信息的漏洞。包括但不限于存储型 XSS、反射型 XSS、DOM-XSS、重要敏感操作的 CSRF。

2）远程应用拒绝服务漏洞（无交互的）、内核拒绝服务漏洞、可获取敏感信息或者执行敏感操作的客户端产品的 XSS 漏洞。

3）普通信息泄漏漏洞。包括但不限于客户端明文存储密码、QQ 密码明文传输、包含敏感信息的源代码压缩包泄漏。

4）qq.com 和 tencent.com 的子域名劫持。

5）需点击链接进行交互的 OAuth 登录或绑定劫持。

6）能直接访问腾讯内网但无回显的 SSRF 漏洞。

7）本地任意代码执行。包括但不限于本地可利用的堆栈溢出、UAF、double free、format string、本地提权(从普通用户提升到 Administrator 或 System 且客户端产品为默认设置)、文件关联的 DLL 劫持（不包括以下几种情况：加载不存在的 DLL 文件、加载正常 DL L 未校验合法性、需要管理员权限操作、需要用户大量交互以及基

于 KnownDLLs 缺陷 所导致的 DLL 劫持等）以及其它逻辑问题导致的本地代码执行漏洞。

8）微信小程序密钥泄露如未能证明可利用部分危害较大的 API，如发送客服消息、调用腾讯云 API 写操作等，评级不超过【中】。

9）非重要功能的单接口越权漏洞最高不超过中危。

[低]
1） 只在特定非流行浏览器环境下（不接收 IE 等过老浏览器的问题）才能获取用户身份信息的漏洞。包括但不限于存储型 XSS、反射型 XSS、DOM-XSS 等。

2）轻微信息泄漏漏洞。包括但不限于 GitHub 泄露的非敏感系统源码及密码、SVN 文件泄漏、phpinfo、logcat 敏感信息泄漏、正确的内网账号密码。

3）URL 跳转。包括但不限于 qq.com 、tencent.com、wechat.com 等重要子域名下的腾讯 URL 跳转漏洞、需证明可直接跳转到 http://www.qq.com_521_qq_diao_yu_wangzhan_789. com ，如能跳转到该站点，无任何提示且未使用其他方式多次跳转或中转，则认为存在漏洞，否则不存在；如提交的报告无法证明跳转到 http://www.qq.com_521_qq_diao_yu_wangzhan_789.com，原则上不作为跳转漏洞确认。

4）无限制短信轰炸漏洞。

5）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、非重要的敏感操作 CSRF 以及需借助中间人攻击的远程代码执行漏洞并提供有效 PoC。

[无]
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 的 低版本）、Self-XSS、无敏感信息的 JSON Hijacking、无敏感操作的 CSRF(如收藏、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）部分风险过低或难以利用的问题。包括不限于 PDF XSS、邮箱轰炸、无法请求内网的 SSRF、并发请求操作某些产品中不重要的数据（如浏览量、报名人数、不重要的点赞评分功能）、无意义的 API Key 泄露、本地拒绝服务漏洞；未提供成功案例，只是说明理论可行（例如只提供 dnslog 的“log4j2 命令执行漏洞”）。

4）无任何证据的猜测。包括但不限于自己 QQ 被盗就表示有漏洞。

5）运营预期之内或无法造成资金损失的问题、符合业务预期的产品设计，包括但不限于可使用多个账号领取小额奖励的正常业务活动。

6）非腾讯业务漏洞、不涉及腾讯产品自身 BUG 且非腾讯产品直接造成的安全问题。

安全情报评分标准

安全情报是指腾讯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。

情报报告必须经过情报提供者的验证和复现并提供相关证明材料（不限于复现截图和视频）用于证明威胁情报真实有效；情报提供者需写清事实依据，同时应该反馈详细复现信息包括 但不限于复现行为开始时间，复现行为结束时间，复现结果和结果证明，复现账号和 ID 等。

根据危害及情报提供情况详细评分标准如下表：

评分级别	线索范围	描述
严重	服务器被入侵且提供了入侵行为方式等相关线索	业务服务器被入侵且提供了相关行为特征方便快速定位确认问题点
	核心业务敏感数据泄露线索	业务数据库被拖取，且提供了数据库详细信息，方便快速定位确认问题点
	重大金融逻辑漏洞线索	支付类严重的逻辑漏洞
高	蠕虫传播且提供了蠕虫传播的链接等相关线索	核心业务存储型 XSS 导致的大规模蠕虫传播
	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	因漏洞引起的大规模身份信息被窃取
	核心游戏产品外挂线索	核心游戏产品可严重影响游戏平衡的外挂线索
中	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	新型 WebShell、DDoS 等攻击方式

安全情报奖励见上述“TSRC贡献值体系”。

第三方软件通用漏洞接收说明

暂停接收第三方软件通用漏洞，建议您向软件官方以及国家相关漏洞平台报告。如果您发现腾讯业务也受到通用漏洞影响，请将漏洞及受影响业务报告给我们。感谢您为网络安全作出贡献。

英雄榜单与荣誉称号

对于每一位提交有效漏洞/情报的白帽子，都会在“英雄榜”展示出网络昵称和贡献值，以 示感谢。

在 TSRC 旧的贡献值体系下：单个漏洞贡献值 = 积分
在 TSRC 新版贡献值体系下：单个漏洞贡献值 = 积分 * 新贡献系数

旧贡献系数分别为：低危（9）、中危（15）、高危（60）、严重（120），新贡献系数见上文。

以 2020 年 5 月 21 日 0 时为节点，之前的贡献值以“积分 * 旧贡献系数”进行追溯计算，之后的贡献值以“积分 * 新贡献系数”进行计算，两者累加得出新版贡献值排行榜，包括 总排行、年排行、月排行。

因贡献值排名体系变更，为感谢白帽子八年来的支持，TSRC 保留从 20120520 至 20200520 的旧体系排名，特设“凌烟阁”，感谢白帽子的辛勤付出。

为了更加清晰地展示出贡献巨大获得特别奖励的白帽子，TSRC 也增设“特别奖励榜”，列举 特别现金奖励信息。

当贡献值达到一定分值后，将获得相应的“荣誉称号”和安全币鼓励，荣誉称号的分值规定如下：

荣誉称号	旧榜单：积分	新榜单：贡献值（积分 * 贡献系数）
一无所有	0	0
新手上路	1	1
安全助理	10	50
民间高手	30	300
安全研究员	50	500
高级安全研究员	100	1000
资深安全研究员	150	2000
安全专家	300	5000
高级安全专家	1000	20000
资深安全专家	2500	50000
权威专家	5000	200000

奖励发放原则

[常规奖励]
奖品使用安全币（TSRC 威胁情报反馈平台上的一种虚拟货币）兑换，安全币数量由威胁情报的评分乘以相应危害等级系数而得，危害等级系数参考“威胁情报评分标准”章节（该系数会根据实际情况调整，每次调整会公告发布）。多个威胁情报产生的安全币可累加，除非特别声明，未使用的安全币不会过期。

奖品上架时有数量限制，当期上架奖品被兑换完后不再接受兑换。

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，TSRC 不承担责任。

[月度奖励]
为鼓励报告者提交高质量的威胁情报，每月会设置若干现金奖励，具体奖励名额根据当月威胁情报质量而定，无上限，也可能空缺，奖励范围如下：

1）提交核心业务或重点业务的严重漏洞报告者（奖金见上述“严重漏洞额外现金奖”）
2）思路新颖或影响范围大，对腾讯业务安全做出突出贡献的报告者（奖金为税后 5000 以上人民币）

TSRC 在每月初对上个月所有报告进行高质量评选，并发放现金奖励。

争议解决办法

在威胁情报处理过程中，如果报告者对处理流程、威胁情报评定、威胁情报评分等具有异议的，请通过当前威胁情报报告页面的评论功能或者审核人员 QQ 及时沟通。腾讯安全应急响应中心将根据威胁情报报告者利益优先的原则进行处理。

FAQ

Q：TSRC 平台的 1 个安全币相当于多少人民币？
A：根据既往奖励标准，当前 TSRC 平台 1 个安全币相当于 5 元人民币。

Q：在腾讯威胁情报反馈平台上的威胁情报会公开吗？
A：为了保护用户利益，在威胁情报反馈的安全问题修复前，威胁情报相关信息均不会公开。安全问题修复后，且经 TSRC 授权后威胁情报报告者可以公开。本着“授人以鱼不如授人以渔”的考虑，TSRC 建议威胁情报报告者将威胁情报相关技术进行归类和总结，以技术文章的方式公开，且不展示具体产品名称。

Q：TSRC 与其他安全团体的关系是如何的？
A：腾讯安全离不开业界的支持与帮助，TSRC 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 TSRC 已经与一些安全团体展开了合作，未来将有更多合作。

Q：腾讯威胁情报奖励计划是不是用奖品隐瞒安全问题？
A：不是。首先，我们认为，在威胁情报中的安全问题未修复前，为了保护用户利益，威胁情报不应该被公开，这也是业界的通用做法。其次，腾讯为威胁情报报告者提供礼品等奖励是为了表达对威胁情报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：腾讯是不是只感谢通过腾讯威胁情报反馈平台的报告者？
A：不会。腾讯尊重和感谢每一位善意的报告者。但是腾讯威胁情报奖励计划目前仅针对腾讯威胁情报反馈平台，对于通过其他渠道反馈的威胁情报，我们也会表示感谢。

Q：腾讯有没有先“忽略”漏洞然后偷偷修复？
A：绝对不会。提交的“漏洞”一旦进入“忽略”状态，跟进同事会在评论中留下忽略的原因。常见情况是这个“漏洞”不认为是漏洞而被评估为一个 bug，TSRC 仅知会相关产品同事，是否更改这个“bug”由产品同事决定；另外一种情况是业务本身的变动，导致“漏洞”不复存在。但是不论如何，腾讯方面都不会“偷偷修复漏洞”。