腾讯外部威胁情报处理流程

编写人	**腾讯安全应急响应中心**
版本号	**2.1**
最后更新日期	**2015-10-15**

致谢

感谢 **7DScan**、**alert7**、**cnhawk**、**hj@topsec**、**instruder**、**MythHack**、**papaya**、**PiaCa**、**So what**、**SuperHei**、**WooYun.org**、**xsjswt**、**买不起的牌子**、**钱途**、**扫地僧**、**DragonEgg**、**ice yes**、**TK**、**nforest**、**PP**（排名不分先后）为本流程所作出的贡献

如果您对本流程有任何的建议，欢迎通过邮箱（security@tencent.com）或者微博私信（http://weibo.com/tsrcteam ）的方式向我们反馈。

适用范围

本流程适用于腾讯威胁情报反馈平台（http://security.tencent.com/index.php/report）所收到的所有情报。

实施日期

本文档自发布之日起实行

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- 1-16 更新评分标准；更新奖品发放流程；更新 FAQ
V1.3 2013- 3-22 更新奖品发放流程；更新评分标准
V1.4 2013- 8-12 更新争议解决办法流程；更新 Discuz!产品的评分标准
V1.5 2013- 9-01 更新客户端产品奖励标准；更新评分标准
V1.6 2014- 2-12 更新评分标准；更新奖励发放原则
V1.7 2014- 5-05 更新客户端产品奖励标准；更新评分标准
V1.8 2014- 6-04 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

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

3） 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

4） 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

5） 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

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（http://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） 三个工作日内，TSRC 工作人员处理问题、给出结论并计分（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]

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。

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 每月第一周内，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；严重或重大影响威胁情报会单独发布紧急安全公告

2） 威胁情报报告者可以使用积分兑换安全币，通过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：自身业务的漏洞、通用软件漏洞及安全情报。下面我们将分别描述其评分标准。

业务漏洞评分标准

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：

[严重]
分值范围 9-10，安全币 1080~1200。

额外现金奖励（人民币）：
1) 3 万~10 万：核心移动终端产品的安全问题（手机 QQ 标准版、微信及手 Q 浏览器标准版）
2) 1 万~3 万：所有 Web 类产品及核心 PC 客户端产品的安全问题（QQ 标准版）

本等级包括

1） 直接获取权限的漏洞（服务器权限、重要产品客户端权限）。包括但不限于远程任意命令执行、上传 webshell、可利用远程缓冲区溢出、可利用的 ActiveX 堆栈溢出、可利用浏览器 use after free 漏洞、可利用远程内核代码执行漏洞以及其它因逻辑问题导致的可利用的远程代码执行漏洞

2） 直接导致严重的信息泄漏漏洞。包括但不限于重要 DB 的 SQL 注入漏洞

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、微信号码发送消息漏洞，伪造任意 QQ、微信号码弹任意 TIPS 给任意用户漏洞，任意 QQ、微信帐号密码更改漏洞

[高] （兑换安全币系数：Web/服务器 60 ； PC 客户端/移动终端 60 ）
分值范围 6-8，安全币 360~480。

额外现金奖励（人民币）：
1) 1 万~3 万：核心移动终端产品的优质安全问题（手机 QQ 标准版、微信及手 Q 浏览器标准版）

本等级包括

1） 能直接盗取用户身份信息的漏洞。包括重要业务（如微信、QQ 邮箱、QQ 空间、财付通主站）的重点页面的存储型 XSS 漏洞、普通站点的 SQL 注入漏洞

2） 越权访问。包括但不限于敏感管理后台登录

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

4） 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、文件关联的 DLL 劫持（不包括加载不存在的 DLL 文件及加载正常 DLL 未校验合法性）以及其它逻辑问题导致的本地代码执行漏洞

5） 直接获取客户端权限的漏洞。包括但不限于远程任意命令执行、远程缓冲区溢出、可利用的 ActiveX 堆栈溢出、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

6） 可获取敏感信息或者执行敏感操作的重要客户端产品的 XSS 漏洞(关于重要客户端产品参见后面）

[中] （兑换安全币系数：Web/服务器 15 ； PC 客户端/移动终端 15 ）
分值范围 3-5，安全币 45~75。等级包括

1） 需交互才能获取用户身份信息的漏洞。包括但不限于反射型 XSS（包括反射型 DOM-XSS）、JSON Hijacking、重要敏感操作的 CSRF、普通业务的存储型 XSS

2） 远程应用拒绝服务漏洞、敏感信息泄露、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

[低] （兑换安全币系数：Web/服务器 9 ； PC 客户端/移动终端 9 ）
分值范围 1-2，安全币 9~18。本等级包括

1） 只在特定非流行浏览器环境下（如 IE6 等）才能获取用户身份信息的漏洞。包括但不限于反射型 XSS（包括反射型 DOM-XSS）、普通业务的存储型 XSS 等。

2） 轻微信息泄漏漏洞。包括但不限于路径泄漏、SVN 文件泄漏、phpinfo、logcat 敏感信息泄漏

3） PC 客户端及移动客户端本地拒绝服务漏洞。包括但不限于组件权限导致的本地拒绝服务漏洞。

4） 越权访问。包括但不限于绕过客户端主动防御，腾讯 URL 跳转漏洞、绕过腾讯恶意网址检测机制的第三方 URL 跳转(注：跳转到正常网站的不属于跳转漏洞，跳转测试 poc：http://www.qq.com_521_qq_diao_yu_wangzhan_789.com，如能跳转到该站点，且无任何提示，则存在漏洞，否则漏洞并不存在)

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了有效 PoC

[无] （兑换安全币系数：Web/服务器 0 ； PC 客户端/移动终端 0 ）
分值范围 0，本等级包括

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） 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

4） 非腾讯业务漏洞

[Discuz! 产品评分标准]

由于腾讯旗下康盛公司的 Discuz!产品被各网站大量使用，如果 Discuz!产品本身出现漏洞影响会较大，故 TSRC 为 Discuz!产品制定专门的评分标准。该标准仅针对 Discuz!产品本身，不包括使用 Discuz!的站点及 Discuz!产品的非官方插件

本标准涉及的 Discuz!产品和版本如下表。“√”代表出现对应安全问题时会发布补丁，“×”代表不会发布补丁。“一般安全问题”指 TSRC 评定为“中”和“高”的，而“严重安全问题”指 TSRC 评定为“严重”的。范围如下：

Discuz!产品版本	版本维护级别	
	一般安全问题	严重安全问题
Discuz! X3.2	√	√
Discuz! X3.1	√	√
Discuz! X3.0	√	√
Discuz! X2.5	×	√
Discuz! X2	×	√

Discuz！X1.5.1	×	√
Discuz！X1.5	×	√

评分标准如下：

危害程度	漏洞危害	示例	分值范围
严重	获取服务器权限	直接/有条件的任意代码执行 直接/有条件的任意命令执行	20 ~ 30
	获取数据库内容	SQL 注入漏洞	20 ~ 25
高	直接盗取管理员/用户身份信息	存储型 XSS 漏洞	10 ~ 15
	越权访问	以管理员身份执行敏感操作	10 ~ 15
中	交互盗取用户身份信息	反射型 XSS	6 ~ 10
	伪造利用用户身份信息	造成实质危害的 CSRF	6 ~ 10
	信息泄漏漏洞	普通的信息泄漏漏洞	3 ~ 6

通用软件漏洞评分标准

1) 软用软件漏洞奖励计划适用各种常见通用软件，优先考虑以下列表：
   a) 操作系统：Linux 、iOS 、Android
   b) Web 服务器：Apache、Nginx、Tomcat
   c) 存储系统：MySQL、Memcache
   d) 开发语言：PHP、Java
   e) 云和虚拟化：Xen、Hadoop
   f) 其他重要软件： OpenSSL 、Struts
2) 漏洞危害级别为严重或高（一般是远程可以利用且危害较大），需要通过 TSRC 平台提交，定级标准按照业务漏洞评分标准执行；
3) 漏洞未在外部公开且未报告给其他机构或组织，需要提供可用的 PoC 。
4) 对于影响巨大的漏洞会给予额外的现金奖励，最高额度 50 万，并且 TSRC 会以漏洞报告者的名义向该漏洞对应的软件基金会捐赠相同额度的现金，帮助其投入更多资源改进软件安全性（如果该软件是商业软件或者不接受捐赠，TSRC 会将该费用捐献给其他公益项目）；

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。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	示例	分值范围
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	9~10
	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	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	重要业务存储型 XSS 导致的大规模蠕虫传播	6~8
	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	
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	3 ~ 5
低	攻击者相关信息	攻击者 QQ、电话等	1~2

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：搜搜、QQ 输入法等业务已移交给搜狗，易迅、拍拍等业务已移交给京东。)

2） 重要客户端产品是指 QQ、手机 QQ、微信、手机 QQ 浏览器；另外，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，原则上也不会修复

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（域名一般是*.qzoneapp.com），均不计分

4） 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

5） 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 TSRC 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

6） 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

7） 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，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

8） 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。

9） 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。

10） 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

11） 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

12） 拒绝无实际危害证明的扫描器结果

13） 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

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信息，每月会单独设置特殊奖励若干，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，奖励为价值至少 2000 元左右的礼物，最高可达 1 万元的现金奖励。奖励标准如下：

1） 提交“严重”等级威胁情报较多的报告者
2） 提交造成较大影响的通用类型威胁情报报告者
3） 思路新颖，对腾讯业务安全做出突出贡献的报告者
4） 如当月没有“严重”威胁情报或其它突出贡献者，则奖项可空缺
5） 当月已获得额外现金奖励的报告者，原则上不再参与月度奖励的评选，除现金奖励报告以外贡献仍然特别突出者除外

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页面中的“一键联系处理人员”、“联系值班人员”的按钮及时沟通。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，必要时可引入外部人士共同裁定

FAQ

Q：TSRC 平台的 1 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 安全币大约相当于 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，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

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：Google 漏洞奖励 5 万美金，为什么腾讯的奖励只有发公仔？

A：首先，腾讯目前已为多位高质量威胁情报报告者送出了包括现金、iPhone、Mac、New iPad、三星手机、小 Q 机器人在内的奖品，并不是只有公仔；其次，由于每个公司的实际情况不同，腾讯目前的奖品价值可能不会如国外的一些公司那么大，但我们后续会不断努力，更多的回馈每位负责任的威胁情报报告者

Q：是不是一个 Shell 换一个 iPad？

A：不是。腾讯威胁情报奖励计划是按照贡献度来进行奖励的，贡献度跟积分相关。具体规则请参考本文档的“奖励发放原则”章节，章节中也没有这个说法。只能说提交高质量威胁情报越多，获得高价值礼物的几率越大

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，我们会在每月公告中表示感谢，如果该渠道有相应规则（比如分发虚拟货币、分数等），我们会按照该渠道的规则给予奖励

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”。