携程安全应急响应中心漏洞评分标准和奖励细则 V7.0

版本号	V7.0
编写人	CSRC
最后更新日期	2023-02-17
适用范围	本标准适用于携程安全应急响应中心 所收到的所有漏洞和威胁情报
更改内容	1. 优化漏洞评分标准和提高漏洞奖励价格； 2. 正式将去哪儿全网域名纳进收录范围，统一按照 CSRC 评分标准评判漏洞等级和奖励
实施日期	2023-02-24

修订记录：

V3.0　发布日期：2015-06-16

V4.0　发布日期：2018-05-15

V5.0　发布日期：2019-01-13

V6.0　发布日期：2020-11-13

V7.0　发布日期：2023-02-24

目录

一. 基本原则

1.携程安全应急响应中心欢迎外部同仁反馈携程旅行网以及去哪儿旅行网站的安全漏洞，以帮助我们不断提升和完善自身产品和业务的安全性，我们承诺：对每一位报告者反馈的问题都及时跟进，分析并处理，对待争议问题抱以公平公正的态度。

2. 本流程适用于携程安全应急响应中心收到的所有安全漏洞报告以及威胁情报。

3. 评分标准针对于携程以及去哪儿产品和业务，域名包括但不限于*.ctrip.com，*.trip.com，*.occpay.com，*.qunar.com 服务器包括携程及去哪儿运营的服务器，产品为携程及去哪儿发布的客户端产品（APP），与携程及去哪儿完全无关的漏洞，不计币。

4. 通用型漏洞（如同一个漏洞源产生的多个漏洞）一般计漏洞数量为一个，例如同一个发布系统引起的多个页面的 XSS 漏洞、同一个应用不同接口使用相同的鉴权逻辑并存在越权、由同一框架导致多站点存在相同类型漏洞等，通用型漏洞视漏洞危害性定级，第一位提交者得币，后面提交者不得币。

5. **同一个漏洞，不能同时提交多个平台。**第一个报告者在第一时间内提交到 CSRC 平台上可得币，其他报告者或在其他平台上重复提交过该漏洞不得币，例如白帽子在别的平台上（包括去哪儿 SRC）提交了该漏洞，又重复提交到 CSRC 平台，则该漏洞不计携程币；提交网上已公开的漏洞不计币，若网上披露漏洞细节，恶意拖取用户数据，内网扫描探测等造成携程以及去哪儿业务影响及危害，我们将保留追究法律责任的权利。

6. 漏洞描述请尽量详细，提供测试功能点截图，请求数据包等信息，对于描述过于简单的漏洞，会适当降级或者忽略处理。(比如暴力破解漏洞，漏洞描述只有一个登陆页面)。

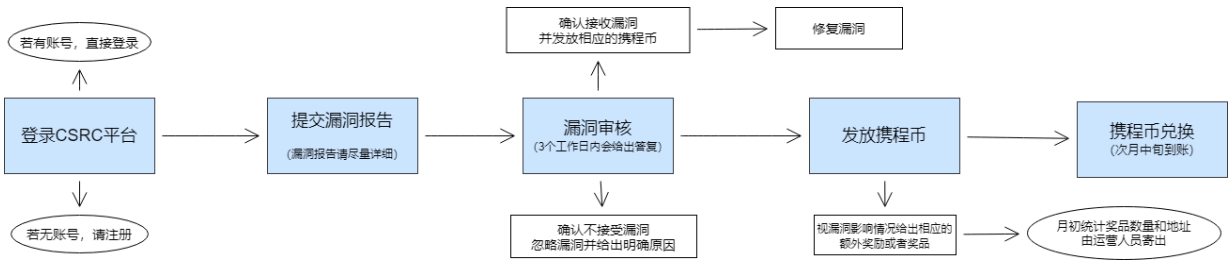
7. 如果同一个系统中短时间发现了大量的同类型漏洞（如 SQL 注入、命令执行、XSS 等），则可能判定该系统几乎没有做任何防护，正常审核前三个该类型漏洞，其他同系统同类型漏洞均不再收取。

8. 以漏洞测试为借口，利用漏洞进行损害用户利益、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，同时携程保留采取进一步法律行动的权利。请严格遵守 SRC 行业安全测试规范。

二. 漏洞提交及处理流程

2.1 漏洞提交流程如下：



2.2 漏洞争议解决办法：

在安全漏洞处理过程中，如果报告者对处理流程、漏洞评级、漏洞评分等存在异议，可采取以下措施：

1. 可通过在 CSRC 平台上的漏洞详情下进行评论，将联系方式留言给审核人员，会有对应的运营人员联系您答疑，解决争议问题。

2. 发送邮件至携程安全应急响应中心官方邮箱：**CSRC.security@trip.com**，携程安全应急响应中心将根据漏洞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。

三. 安全漏洞评分标准

Ø 携程根据漏洞的危害程度将漏洞等级分为**【严重】、【高】、【中】、【低】、【无】**五个等级；应用系统重要性分级为：**核心应用、一般应用、边缘应用/合作公司。**

Ø 每个漏洞所得携程币=系统重要性系数*漏洞严重性系数。**CSRC 采用携程币作为货币单位，1 携程币=1RMB。**

Ø 安全漏洞最终评分会根据具体漏洞类型、业务重要性评定。根据对应的漏洞所获得的携程币对应表如下：

系统重要性*漏洞严重性	严重漏洞 (500-800)	高危漏洞 (200-500)	中危漏洞 (40-80)	低危漏洞 (10-30)
核心应用 (10)	5000-8000	2000-5000	400-800	100-300
一般应用 (5)	2500-4000	1000-2500	200-400	50-150
边缘应用/合作公司 (1)	500-800	200-500	40-80	10-30

Ø 携程应用系统重要性分级标准：

1. 核心应用（系数 10）：*.ctrip.com 和*.trip.com 主页面的入口（包括会员资金交易），程付通*.occpay.com 相关支付业务以及去哪儿主站*.qunar.com，主页面入口如下截图。

2. 一般应用（系数 5）：除核心应用外，是*.ctrip.com 和*.trip.com 以及*.qunar.com 的域名，且具有业务属性或业务用户数据相关的应用。

3. 边缘应用/合作公司（系数 1）：属于携程及去哪儿应用或携程合作公司如永安等，域名不限，且非业务属性和非业务用户数据相关的应用。

【补充说明】业务属性：携程系统服务对象属于外部用户，包括 to B 或 to C；服务于携程集团员工或关联公司的系统属于非业务属性。

域名举例如下：

核心应用 （主页面入口）	国内站点	*.ctrip.com
	国际站点	*.trip.com
	程付通	*.occpay.com
	去哪儿网	*.qunar.com
一般应用（举例）	酒店赫程	ebooking.ctrip.com
	酒店赫程	*.easytrip.com
	酒店赫程	*.toptown.cn
	携程通	b.ctrip.com
	携程旅游供应商系统	vbooking.ctrip.com
	…	…
边缘应用（域名不限的携程应用）及合作公司（举例）	招商合作	go.ctrip.com
	CSRC 平台	sec.ctrip.com
	开放平台	http://u.ctrip.com/alliance/#/index
	技术中心招聘网站	techshow.ctrip.com/
	铁友	*.tiexiaoer.com
	永安	*.wingontravel.com
	…	…

Ø 安全漏洞类型评级标准：

漏洞等级	漏洞详情
【严重漏洞】	1. 直接获取系统权限的漏洞。包括但不仅限于命令执行、代码执行、获取 Webshell、SQL 注入获取系统权限等。
	2. 严重的大量敏感信息泄漏，至少包含三个维度及以上的明文敏感信息，包括但不仅限于：手机号、银行卡信息、身份证信息、订单信息、邮箱，邮寄地址等。
	3. 严重的逻辑设计缺陷和流程缺陷，包括但不仅限于：任意用户登录、任意资金消费等。

【高危漏洞】	1. SQL 注入漏洞。
	2. 高危的敏感信息泄露，包括但不仅限于：源代码泄露，高危的用户明文敏感信息泄露等。
	3. 严重的越权敏感操作，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。
	4. 直接导致订单相关业务拒绝服务的漏洞。包括但不仅限于利用漏洞或业务逻辑漏洞直接导致系统业务不可用。
	5. 绕过认证直接访问管理后台（非供应商后台，而是管理员平台）、管理后台弱密码、获取大量内网敏感信息。
	6. 任意系统文件读取漏洞，可读取重要敏感文件。
	7. 能够访问携程及去哪儿内网且有回显内容的 SSRF 漏洞
【中危漏洞】	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，存储型 XSS 请证明可获取核心 cookie 等敏感信息以及 payload 的注入点。
	2. 普通遍历越权操作，包括但不仅限于不正确的直接对象引用、越权查看订单信息，越权修改普通用户信息等
	3. 普通信息泄漏。包括但不仅限于：有掩码的用户敏感信息、GitHub 或者百度网盘等外部托管平台上面非生产项目或者其他信息泄露等
	4. 不涉及资金、订单和用户敏感信息等普通的逻辑设计缺陷和流程缺陷。
	5. 不涉及订单业务的拒绝服务漏洞
【低危漏洞】	1. 轻微信息泄漏。包括但不仅限于 phpinfo 信息泄露、SVN 信息泄漏、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、敏感配置信息等。
	2. 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、涉及重要操作的 CSRF 漏洞等。
	3. 可导致资源滥用或造成对用户骚扰的漏洞。包括但不仅限于邮箱或短信轰炸。
	4. 暴力破解漏洞。
【无】	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、应用兼容性等问题。
	2. 无法利用的漏洞。无敏感操作的 CSRF（收藏、取消收藏、一般的资料修改等）、无意义的异常信息泄漏、内网 IP 地址/域名泄漏。
	3. 不能直接反映漏洞存在的其他问题。包括但不仅限于纯属用户猜测的问题。
	4. 反射型 XSS。
	5. URL 跳转。
	6. 普通帐户弱口令。
	7. 单纯的接口文档泄露，而不能进一步利用的漏洞。
	8. 以下为对外演示站点，不收取相关漏洞： https://standard.ctrip.com https://corpgov.ctrip.com 等类似站点

四. 威胁情报评分标准

Ø 威胁情报认定原则：

1. 威胁范围：携程网站以及去哪儿的产品和业务漏洞相关的安全情报，包括但不限于漏洞线索，流程脆弱性，攻击方式，攻击者信息等。

2. 提交相同情报者，首位提交者将被予以确认，其他不予以确认。

3. 报告的详细程度会直接关联到最后的评分，报告请尽量详细：情报类型，攻击路径，攻击方法。

4. 通用型漏洞、同一安全隐患引起的多个问题计数为一个。

5. 业界暂时无法彻底解决的业务威胁问题暂时不计分，例如众包手动领券（如果发现某活动未接入风控，依靠一些黑设备或者批量注册的账号，依然可以参与活动的。若提交情报，可帮助减少业务损失的，依然算分）。

6. 对于第三方问题导致的安全威胁，我方无法修复的暂时不计分（如航空公司客户信息泄漏造成的携程用户被欺诈）。

7. 未经允许对外披露情报内容，将不予确认，已确认的情报奖励将有权追回。

8. 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，将不计分，同时携程保留采取追究法律责任的权利。

9. 威胁情报分为三个等级：**【高危】【中危】【低危】**，依据携程应用系统重要性分级标准：**核心应用，一般应用，边缘应用。**

Ø 威胁情报奖励计划：

根据对应的情报所获得的携程币对应表如下：携程币=系统重要性*漏洞严重性

系统重要性/漏洞严重性	高危（100-300）	中危（30-80）	低危（10-25）
核心应用（10）	1000-3000	300-800	100-250
一般应用（5）	500-1500	150-400	50-125
边缘应用/合作公司（1）	100-300	30-80	10-25

Ø 威胁情报评级细则：

级别	线索范围	示例
高危	1. 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
	2. 绕过反爬限制，可以恶意爬取客户敏感信息的爬虫手段和技术	例如爬取客人未掩码的手机号、姓名、身份证号码、地址等等
	3. 公司最近一个月内的重要业务敏感信息泄漏的相关线索	证明最近一个月内携程网客户、订单信息批量泄漏，提供被脱库的详细信息，可快速定位确认问题点
	4. 重大金融逻辑漏洞线索	支付类严重的逻辑漏洞
	5. 业务存在严重逻辑缺陷导致业务不能正常进行的线索	绕过认证可以批量提交恶意订单的
	6. 网站价格被恶意篡改影响当前业务的线索	网站旅游价格被恶意篡改，出现“1 元”旅游的相关证明
中危	1. 公司业务存在严重脆弱性环节的漏洞	通过致电携程及去哪儿的客服，利用客服人员安全意识薄弱可以成功套取用户相关信息的相关证明
	2. 外部黑产群或论坛，流出的黑产工具，且可运行	例如某恶意自动注册账号工具、自动返现工具等
	3. 外部黑产群或论坛，传播存在风险的业务活动（众包不算）	例如某抽奖活动未接风控，恶意设备或者账号一天可以拿到 5 个免费住五星酒店的机会
	4. 绕过风控限制，可批量进行恶意业务风险操作的漏洞	例如可以通过接口发包批量登录注册、唯一的模拟器设备可以批量注册账号 100 个以上，恶意账号可以批量领券等等
	5. 绕过反爬限制，可以恶意爬取一般敏感信息的爬虫手段和技术	例如商品价格、酒店地址、库存量等等
低危	1. 发现针对携程以及去哪儿的假冒或者钓鱼网站等	提供假冒或者钓鱼网站有效链接

五. 奖励发放原则和方式

Ø 奖励发放原则：

1. 漏洞报告者通过报告有效漏洞获取携程币，**1 个携程币=1RMB，可点击携程币兑换地址进行兑换**

2. 兑换现金前请先确认个人资料是否完善，兑换的携程币到账的银行卡必须为本人实名认证的银行卡，如果因银行卡及身份证非本人实名认证的原因无法完成打款，后果请自行承担。

3. 兑换携程币的流程周期为 15-30 天，次月的中旬（10-15 号）会到账，如果有问题可以随时联系运营人员，若需要联系运营人员请在 CSRC 平台上进行留言，或者在微信公众号（携程安全应急响应中心）上进行留言。

Ø 奖励发放方式：

奖励分为**【常规奖励】和【年度奖励】**，以及不定期的**【活动奖励】**

【常规奖励】:

常规奖励即所提交的有效漏洞/威胁情报报告获得的携程币，可随时进行兑换，1 个携程币=1RMB

【年度奖励】

年度贡献榜排行**前三名**将获得 **CSRC 年度奖金，荣誉证书以及荣誉奖杯**

【活动奖励】

CSRC 会不定时推出节日福利及双倍活动，以双倍携程币的方式或礼品发放的形式进行活动，由运营人员统计获得奖品的人数，月初统一寄出一次奖品。

六. FAQ

1. Q：1 个携程币等于多少人民币?

   A： 1 个携程币相当于 1 元人民币。

2. Q：CSRC 会把我提交的漏洞先修复了，然后忽略我的漏洞吗?

A：不会，我们承诺，对待每一位报告携程网站安全漏洞的白帽子进行积极主动地跟进，每一个漏洞都会得到公平公正的处理，不会先修复后忽略。

3. Q：为什么我提交的高危漏洞被降级为中危漏洞?

A：漏洞评级依据该漏洞在实际场景中对业务的影响程度给出，对于没有出现用户敏感信息，以及对业务不会产生实质影响和危害的漏洞，会被降级处理。

4.Q：收取的 APP 隐私漏洞有范围限制吗?

A：有，提交的漏洞必须是在安卓 8.0 及以上系统版本，或 IOS12.0 及以上系统版本上发现的携程 APP 隐私漏洞

5.Q：我发起了漏洞奖金兑换，需要多久才能到账?

A：次月中旬（一般是次月 10-15 号）

6.Q：我想跟别人分享我的挖洞经验和案例，可以披露部分已修复的漏洞细节吗?

A：若有相关分享需求，请提前发送邮件至 **CSRC.security@trip.com** 说明情况，我们会第一时间进行评估并给予答复。若未经同意私自披露漏洞细节，携程将保留追究法律责任的权力。